

Exploitation

Ecoute du trafic sur un réseau local

Objectifs spécifiques

- Découvrir le plan d'adressage (clients, serveurs, éléments actifs du réseau...)
- Récupérer les objets sensibles véhiculés par les protocoles (identifiants, mots de passe...)
- Attaque passive discrète et peu coûteuse à mettre en oeuvre

Outils

- analyseurs réseau : `wireshark`, `tshark`, `tcpdump`
- Outils spécifiques : `ettercap`, `dsniff`, `webspy`...

Difficulté différente en fonction des équipements réseaux présents : Hub ou Switch.

Exploitation

Ecoute du trafic sur un réseau local

Wireshark 1.6.2 interface showing a network capture. The filter is `tcp.port==80`. The packet list shows various protocols including TCP, NetBIOS, NBSS, SMB, DNS, and HTTP. The packet details pane shows the structure of the selected packet (Frame 1516), including Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Hypertext Transfer Protocol. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
473	11.192015	192.168.10.175	192.168.10.1	TCP	78	63481 > netbios-ssn [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=0 TSval=1915949603 TSecr=
487	11.312945	192.168.10.1	192.168.10.175	TCP	60	microsoft-ds > 63480 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
488	11.314733	192.168.10.1	192.168.10.175	TCP	74	netbios-ssn > 63481 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=
489	11.314860	192.168.10.175	192.168.10.1	TCP	66	63481 > netbios-ssn [ACK] Seq=1 Ack=1 Win=524280 Len=0 TSval=1915949601 TSecr=9452023
490	11.314947	192.168.10.175	192.168.10.1	TCP	66	63481 > netbios-ssn [FIN, ACK] Seq=1 Ack=1 Win=524280 Len=0 TSval=1915949801 TSecr=94
491	11.315411	192.168.10.175	192.168.10.1	TCP	78	63482 > netbios-ssn [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=0 TSval=1915949001 TSecr=
498	11.378233	192.168.10.1	192.168.10.175	TCP	66	netbios-ssn > 63481 [ACK] Seq=1 Ack=2 Win=5888 Len=0 TSval=945202544 TSecr=1915949801
499	11.378401	192.168.10.175	192.168.10.1	TCP	66	[TCP Dup ACK 490#1] 63481 > netbios-ssn [ACK] Seq=2 Ack=1 Win=524280 Len=0 TSval=1915
500	11.387525	192.168.10.1	192.168.10.175	TCP	66	netbios-ssn > 63481 [FIN, ACK] Seq=1 Ack=2 Win=5888 Len=0 TSval=945202544 TSecr=1915
501	11.387781	192.168.10.175	192.168.10.1	TCP	66	63481 > netbios-ssn [ACK] Seq=2 Ack=2 Win=524280 Len=0 TSval=1915949871 TSecr=9452023
511	11.518005	192.168.10.1	192.168.10.175	TCP	74	netbios-ssn > 63482 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=
512	11.518089	192.168.10.175	192.168.10.1	TCP	66	63482 > netbios-ssn [ACK] Seq=1 Ack=1 Win=524280 Len=0 TSval=1915949998 TSecr=9452023
513	11.518155	192.168.10.175	192.168.10.1	NBSS	130	Session request, to MERLIN<20> from MACBOOKPRO-ADDC<00>
526	11.596538	192.168.10.1	192.168.10.175	TCP	66	netbios-ssn > 63482 [ACK] Seq=1 Ack=73 Win=5888 Len=0 TSval=945202701 TSecr=191594998
527	11.596417	192.168.10.1	192.168.10.175	NBSS	70	Positive session response
528	11.596457	192.168.10.175	192.168.10.1	TCP	66	63482 > netbios-ssn [ACK] Seq=73 Ack=5 Win=524280 Len=0 TSval=1915950070 TSecr=945202
529	11.596499	192.168.10.175	192.168.10.1	SMB	117	Negotiate Protocol Request
544	11.744002	192.168.10.1	192.168.10.175	SMB	197	Negotiate Protocol Response
545	11.744077	192.168.10.175	192.168.10.1	TCP	66	63482 > netbios-ssn [ACK] Seq=124 Ack=136 Win=524280 Len=0 TSval=1915950211 TSecr=945
546	11.755865	192.168.10.175	192.168.10.1	DNS	65	Standard query SOA local
548	11.758157	192.168.10.175	192.168.10.1	DNS	78	Standard query A MERLIN.camelot.lan
549	11.758281	192.168.10.175	192.168.10.1	DNS	78	Standard query AAAA MERLIN.camelot.lan

Frame 1516: 418 bytes on wire (3344 bits), 418 bytes captured (3344 bits)

Ethernet II, Src: IcpElect_c5:f3:e0 (00:08:9b:c5:f3:e0), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)

Internet Protocol Version 4, Src: 192.168.10.10 (192.168.10.10), Dst: 239.255.255.250 (239.255.255.250)

User Datagram Protocol, Src Port: ssdp (1900), Dst Port: ssdp (1900)

Hypertext Transfer Protocol

0000 01 00 5e 7f ff fa 00 08 9b c5 f3 e0 00 00 45 00 ..^.....E.
0010 01 94 00 00 40 00 04 11 ba ac c0 a8 0a 0a ef ff@... ..
0020 ff fa 07 8c 07 8c 01 80 80 a3 4e 4f 54 49 46 59 ...l...NOTIFY
0030 20 2a 20 48 54 54 50 2f 31 2e 31 0d 0a 48 4f 53 * HTTP/ 1.1..HOS
0040 54 3a 20 32 33 38 2e 32 35 35 2e 32 35 35 2e 32 T: 239.2 55.255.2
0050 35 30 3a 31 39 30 30 0d 0a 43 41 43 48 45 2d 43 50:1900. .CACHE-C
0060 4f 4e 54 52 4f 4c 3a 20 6d 61 78 2d 61 67 65 3d CONTROL: max-age=
0070 31 38 31 30 0d 0a 4c 4f 43 41 54 49 4f 4e 3a 20 1810..LO CATION;
0080 68 74 74 70 3a 2f 2f 31 39 32 2e 31 36 38 2e 31 http://1 92.168.1
0090 30 2e 31 30 3a 39 30 30 30 2f 54 4d 53 44 65 76 0.10:900 0/TMSDev
00a0 69 63 65 44 65 73 63 72 69 70 74 69 6f 6e 2e 78 iceDescription.x
00b0 6d 6c 0d 0a 4e 54 3a 20 75 72 6e 3a 73 63 68 65 m...NT: urn:sche

en1: <live capture in progress> File... Packets: 12508 Displayed: 214 Marked: 0 Profile: Default