

Analisi traffico Wireshark

Cattura traffico

Notiamo in grigio le molteplici richieste TCP inviate dall'host attaccante con IP 192.168.200.100, mentre in rosso notiamo le risposte dell'host vittima con IP 192.168.200.150

The image shows a Wireshark packet capture window titled "Cattura_U3_W1_L3.pcapng". The main pane displays a list of captured packets. The first column shows the packet number, time, source IP, destination IP, protocol, length, and a brief description. The second column shows the packet details, including the Ethernet II header, Internet Protocol Version 4 header, User Datagram Protocol header, NetBIOS Datagram Service header, SMB (Server Message Block Protocol) header, and Microsoft Windows Browser Protocol header. The third column shows the packet bytes in hexadecimal and ASCII.

Time	Source	Destination	Protocol	Length	Info
40	36.775975876	192.168.200.100	TCP	66	55656 → 22 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
41	36.776005853	192.168.200.100	TCP	66	53062 → 80 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
42	36.776179338	192.168.200.100	TCP	74	50684 → 199 [SYN] Seq=0 Win=64240 Len=0
43	36.776233880	192.168.200.100	TCP	74	54220 → 995 [SYN] Seq=0 Win=64240 Len=0
44	36.776330610	192.168.200.100	TCP	74	34648 → 587 [SYN] Seq=0 Win=64240 Len=0
45	36.776385694	192.168.200.100	TCP	74	33042 → 445 [SYN] Seq=0 Win=64240 Len=0
46	36.776402500	192.168.200.100	TCP	74	49814 → 256 [SYN] Seq=0 Win=64240 Len=0
47	36.776451284	192.168.200.150	TCP	60	199 → 50684 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
48	36.776451357	192.168.200.150	TCP	60	995 → 54220 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
49	36.776478201	192.168.200.100	TCP	74	46990 → 139 [SYN] Seq=0 Win=64240 Len=0
50	36.776496366	192.168.200.100	TCP	74	33206 → 143 [SYN] Seq=0 Win=64240 Len=0
51	36.776512221	192.168.200.100	TCP	74	60632 → 25 [SYN] Seq=0 Win=64240 Len=0
52	36.776568606	192.168.200.100	TCP	74	49654 → 110 [SYN] Seq=0 Win=64240 Len=0
53	36.776671271	192.168.200.100	TCP	74	37282 → 53 [SYN] Seq=0 Win=64240 Len=0
54	36.776720715	192.168.200.100	TCP	74	54898 → 500 [SYN] Seq=0 Win=64240 Len=0
55	36.776813123	192.168.200.150	TCP	60	587 → 34648 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
56	36.776843423	192.168.200.100	TCP	74	51534 → 487 [SYN] Seq=0 Win=64240 Len=0
57	36.776904828	192.168.200.150	TCP	74	445 → 33042 [SYN, ACK] Seq=0 Ack=1 Win=0 Len=0
58	36.776904922	192.168.200.150	TCP	60	256 → 49814 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
59	36.776904961	192.168.200.150	TCP	74	139 → 46990 [SYN, ACK] Seq=0 Ack=1 Win=0 Len=0
60	36.776905004	192.168.200.150	TCP	60	143 → 33206 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
61	36.776905043	192.168.200.150	TCP	74	25 → 60632 [SYN, ACK] Seq=0 Ack=1 Win=0 Len=0
62	36.776905082	192.168.200.150	TCP	60	110 → 49654 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
63	36.776905123	192.168.200.150	TCP	74	53 → 37282 [SYN, ACK] Seq=0 Ack=1 Win=0 Len=0
64	36.776905162	192.168.200.150	TCP	60	500 → 54898 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Frame 1: 286 bytes on wire (2288 bits), 286 bytes captured (2288 bits) on interface 0
Ethernet II, Src: PcsCompu fd:87:1e (08:00:27:fd:87:1e), Dst: 08:00:27:fd:87:1e
Internet Protocol Version 4, Src: 192.168.200.150, Dst: 192.168.200.100
User Datagram Protocol, Src Port: 138, Dst Port: 138
NetBIOS Datagram Service
SMB (Server Message Block Protocol)
SMB MailSlot Protocol
Microsoft Windows Browser Protocol

Packets: 2083 · Displayed: 2083 (100.0%) | Profile: Default

Vettore d'attacco

Multiple richieste TCP su ampi intervalli di porte

Azioni per ridurre l'impatto dell'attacco

Possiamo bandire tutte le future richieste provenienti dall'indirizzo IP malevolo e tramite firewall chiudere le porte vulnerabili