Global Information Assurance Certification Paper

SNAP LevelOne Certification Practical

Intrusion Detection Subject Area: 10 Detects with Analyses

Adelle A. McIlroy, CISA, CISSP

February 15, 2000

Time	Src Logical	Src Physical	Src Port	Dest Logical	Dest Physical	Dest Port	Protocol	Size	IP Details
20:53:38.399	IP-10.1.1.10	00:10:4B:FE:DA:B8	1024	IP-10.1.1.5	00:50:04:8C:C8:99	33137	IP UDP	64	
20:53:38.399	IP-10.1.1.5	00:50:04:8C:C8:99		IP-10.1.1.10	00:10:4B:FE:DA:B8		ICMP DUnr	74	Port unreachable: 10.1.1.5

These two captured packets show use of port 31337. This port is characteristic of the BackOrifice exploit. The interesting point, however, is that this port is a legitimate high-numbered port to be selected randomly or by an application programmer. Consequently, traffic to this port may trip intrusion detection systems, but should be treated with caution, not overreaction. Packets to ports often associated with exploits are a common cause of IDS FALSE POSITIVES, and demonstrate the need to establish a baseline of "normal" traffic to eliminate these packets from further investigation. This tactic may also allow capturing of UDP packets to ports 31335 or 27444, or TCP packets to 27665, which are elements in some common implementations of the current distributed denial of service (DDoS) attacks.

Time	Src Logical	Src Physical	Src Port	Dest Logical	Dest Physical	Dest Port	Protocol	Size	IP Details
20:53:54.810	IP-10.1.1.10	00:10:4B:FE:DA:B8	4652	IP-10.1.1.5	00:50:04:8C:C8:99	1562	IP TCP	78	S=3553317581,L= 0,A= 0,W=32120
20:53:54.810	IP-10.1.1.5	00:50:04:8C:C8:99	1562	IP-10.1.1.10	00:10:4B:FE:DA:B8	4652	IP TCP	64	S= 0,L= 0,A=3553317582,W= 0
20:53:54.810	IP-10.1.1.10	00:10:4B:FE:DA:B8	4653	IP-10.1.1.5	00:50:04:8C:C8:99	1563	IP TCP	78	S=3546970923,L= 0,A= 0,W=32120
20:53:54.810	IP-10.1.1.5	00:50:04:8C:C8:99	1563	IP-10.1.1.10	00:10:4B:FE:DA:B8	4653	IP TCP	64	S= 0,L= 0,A=3546970924,W= 0
20:53:54.810	IP-10.1.1.10	00:10:4B:FE:DA:B8	4654	IP-10.1.1.5	00:50:04:8C:C8:99	1564	IP TCP	78	S=3540029093,L= 0,A= 0,W=32120
20:53:54.810	IP-10.1.1.5	00:50:04:8C:C8:99	1564	IP-10.1.1.10	00:10:4B:FE:DA:B8	4654	IP TCP	64	S= 0,L= 0,A=3540029094,W= 0
20:53:54.810	IP-10.1.1.10	00:10:4B:FE:DA:B8	4655	IP-10.1.1.5	00:50:04:8C:C8:99	1565	IP TCP	78	S=3547162008,L= 0,A= 0,W=32120
20:53:54.810	IP-10.1.1.5	00:50:04:8C:C8:99	1565	IP-10.1.1.10	00:10:4B:FE:DA:B8	4655	IP TCP	64	S= 0,L= 0,A=3547162009,W= 0
20:53:54.811	IP-10.1.1.10	00:10:4B:FE:DA:B8	4656	IP-10.1.1.5	00:50:04:8C:C8:99	1566	IP TCP	78	S=3550007385,L= 0,A= 0,W=32120
20:53:54.811	IP-10.1.1.5	00:50:04:8C:C8:99	1566	IP-10.1.1.10	00:10:4B:FE:DA:B8	4656	IP TCP	64	S= 0,L= 0,A=3550007386,W= 0
20:53:54.811	IP-10.1.1.10	00:10:4B:FE:DA:B8	4657	IP-10.1.1.5	00:50:04:8C:C8:99	1567	IP TCP	78	S=3542229348,L= 0,A= 0,W=32120
20:53:54.811	IP-10.1.1.5	00:50:04:8C:C8:99	1026	IP-10.1.1.10	00:10:4B:FE:DA:B8	4117	IP TCP	70	S= 299526,L= 0,A=3541850848,W= 8754
20:53:54.811	IP-10.1.1.5	00:50:04:8C:C8:99	1567	IP-10.1.1.10	00:10:4B:FE:DA:B8	4657	IP TCP	64	S= 0,L= 0,A=3542229349,W= 0
20:53:54.811	IP-10.1.1.10	00:10:4B:FE:DA:B8	4658	IP-10.1.1.5	00:50:04:8C:C8:99	1568	IP TCP	78	S=3544479143,L= 0,A= 0,W=32120
20:53:54.811	IP-10.1.1.5	00:50:04:8C:C8:99	1568	IP-10.1.1.10	00:10:4B:FE:DA:B8	4658	IP TCP	64	S= 0,L= 0,A=3544479144,W= 0
20:53:54.811	IP-10.1.1.10	00:10:4B:FE:DA:B8	4659	IP-10.1.1.5	00:50:04:8C:C8:99	1569	IP TCP	78	S=3545034425,L= 0,A= 0,W=32120
20:53:54.811	IP-10.1.1.5	00:50:04:8C:C8:99	1569	IP-10.1.1.10	00:10:4B:FE:DA:B8	4659	IP TCP	64	S= 0,L= 0,A=3545034426,W= 0
20:53:54.813	IP-10.1.1.10	00:10:4B:FE:DA:B8	4660	IP-10.1.1.5	00:50:04:8C:C8:99	1570	IP TCP	78	S=3544505733,L= 0,A= 0,W=32120
20:53:54.813	IP-10.1.1.10	00:10:4B:FE:DA:B8	4661	IP-10.1.1.5	00:50:04:8C:C8:99	1571	IP TCP	78	S=3555033068,L= 0,A= 0,W=32120
20:53:54.813	IP-10.1.1.5	00:50:04:8C:C8:99	1570	IP-10.1.1.10	00:10:4B:FE:DA:B8	4660	IP TCP	64	S= 0,L= 0,A=3544505734,W= 0
20:53:54.813	IP-10.1.1.5	00:50:04:8C:C8:99	1571	IP-10.1.1.10	00:10:4B:FE:DA:B8	4661	IP TCP	64	S= 0,L= 0,A=3555033069,W= 0

This capture shows the attacker attempting to connect to target host 10.1.1.5 on a variety of TCP ports in an interleaved TCP PORT SCAN.

[redacted]

Time	Src Logical	Src Physical	Src Port	Dest Logical	Dest Physical	Dest Port	Protocol	Size	IP Details
20:53:01.583	IP-10.1.1.10	00:10:4B:FE:DA:B8	51966	IP-10.1.1.5	00:50:04:8C:C8:99	1410	IP UDP	64	
20:53:01.583	IP-10.1.1.10	00:10:4B:FE:DA:B8	51966	IP-10.1.1.5	00:50:04:8C:C8:99	463	IP UDP	64	
20:53:01.583	IP-10.1.1.10	00:10:4B:FE:DA:B8	51966	IP-10.1.1.5	00:50:04:8C:C8:99	410	IP UDP	64	
20:53:01.583	IP-10.1.1.5	00:50:04:8C:C8:99		IP-10.1.1.10	00:10:4B:FE:DA:B8		ICMP DUnr	74	Port unreachable: 10.1.1.5
20:53:01.583	IP-10.1.1.5	00:50:04:8C:C8:99		IP-10.1.1.10	00:10:4B:FE:DA:B8		ICMP DUnr	74	Port unreachable: 10.1.1.5
20:53:01.583	IP-10.1.1.5	00:50:04:8C:C8:99		IP-10.1.1.10	00:10:4B:FE:DA:B8		ICMP DUnr	74	Port unreachable: 10.1.1.5
20:53:01.583	IP-10.1.1.10	00:10:4B:FE:DA:B8	51966	IP-10.1.1.5	00:50:04:8C:C8:99	584	IP UDP	64	
20:53:01.583	IP-10.1.1.10	00:10:4B:FE:DA:B8	51966	IP-10.1.1.5	00:50:04:8C:C8:99	730	IP UDP	64	
20:53:01.583	IP-10.1.1.10	00:10:4B:FE:DA:B8	51966	IP-10.1.1.5	00:50:04:8C:C8:99	1508	IP UDP	64	
20:53:01.583	IP-10.1.1.10	00:10:4B:FE:DA:B8	51966	IP-10.1.1.5	00:50:04:8C:C8:99	401	IP UDP	64	
20:53:01.583	IP-10.1.1.10	00:10:4B:FE:DA:B8	51966	IP-10.1.1.5	00:50:04:8C:C8:99	588	IP UDP	64	
20:53:01.583	IP-10.1.1.5	00:50:04:8C:C8:99		IP-10.1.1.10	00:10:4B:FE:DA:B8		ICMP DUnr	74	Port unreachable: 10.1.1.5
20:53:01.583	IP-10.1.1.5	00:50:04:8C:C8:99		IP-10.1.1.10	00:10:4B:FE:DA:B8		ICMP DUnr	74	Port unreachable: 10.1.1.5
20:53:01.583	IP-10.1.1.5	00:50:04:8C:C8:99		IP-10.1.1.10	00:10:4B:FE:DA:B8		ICMP DUnr	74	Port unreachable: 10.1.1.5
20:53:01.583	IP-10.1.1.5	00:50:04:8C:C8:99		IP-10.1.1.10	00:10:4B:FE:DA:B8		ICMP DUnr	74	Port unreachable: 10.1.1.5
20:53:01.583	IP-10.1.1.5	00:50:04:8C:C8:99		IP-10.1.1.10	00:10:4B:FE:DA:B8		ICMP DUnr	74	Port unreachable: 10.1.1.5

This capture shows the source host 10.1.1.10 attempting UDP connections to the target host on a variety of ports. The destination host is replying for the ports that are not reachable. This pattern of traffic may elude IDS, which are set to detect sequenced scans.

[redacted]

Time	Src Logical	Src Physical	Src Port	Dest Logical	Dest Physical	Dest Port	Protocol	Size	IP Details
21:08:19.883	IP-10.1.1.1	00:50:04:8D:7D:7E			FF:FF:FF:FF:FF:FF		ARP Req	64	10.1.1.2 = ?
21:08:19.885	IP-10.1.1.1	00:50:04:8D:7D:7E			FF:FF:FF:FF:FF:FF		ARP Req	64	10.1.1.3 = ?
21:08:19.887	IP-10.1.1.1	00:50:04:8D:7D:7E			FF:FF:FF:FF:FF:FF		ARP Req	64	10.1.1.4 = ?
21:08:19.890	IP-10.1.1.1	00:50:04:8D:7D:7E			FF:FF:FF:FF:FF:FF		ARP Req	64	10.1.1.5 = ?
21:08:19.890	IP-10.1.1.5	00:50:04:8C:C8:99			00:50:04:8D:7D:7E		ARP Rsp	64	00:50:04:8C:C8:99 = 10.1.1.5
21:08:19.890	IP-10.1.1.1	00:50:04:8D:7D:7E	1190	IP-10.1.1.5	00:50:04:8C:C8:99	139	TCP NetBIOS	66	S=3755004984,L= 0,A= 0,W=16384
21:08:19.890	IP-10.1.1.5	00:50:04:8C:C8:99	139	IP-10.1.1.1	00:50:04:8D:7D:7E	1190	TCP NetBIOS	66	S= 109595,L= 0,A=3755004985,W= 8760
21:08:19.891	IP-10.1.1.1	00:50:04:8D:7D:7E	1190	IP-10.1.1.5	00:50:04:8C:C8:99	139	TCP NB SessMsg	64	S=3755004985,L= 0,A= 109596,W=17520
21:08:19.893	IP-10.1.1.1	00:50:04:8D:7D:7E			FF:FF:FF:FF:FF:FF		ARP Req	64	10.1.1.6 = ?
21:08:19.895	IP-10.1.1.1	00:50:04:8D:7D:7E			FF:FF:FF:FF:FF:FF		ARP Req	64	10.1.1.7 = ?
21:08:19.897	IP-10.1.1.1	00:50:04:8D:7D:7E			FF:FF:FF:FF:FF:FF		ARP Req	64	10.1.1.8 = ?
21:08:19.899	IP-10.1.1.1	00:50:04:8D:7D:7E			FF:FF:FF:FF:FF:FF		ARP Req	64	10.1.1.9 = ?
21:08:19.902	IP-10.1.1.1	00:50:04:8D:7D:7E			FF:FF:FF:FF:FF:FF		ARP Req	64	10.1.1.10 = ?
21:08:19.902	IP-10.1.1.10	00:10:4B:FE:DA:B8			00:50:04:8D:7D:7E		ARP Rsp	64	00:10:4B:FE:DA:B8 = 10.1.1.10
21:08:19.902	IP-10.1.1.1	00:50:04:8D:7D:7E	1195	IP-10.1.1.10	00:10:4B:FE:DA:B8	139	TCP NetBIOS	66	S=3755252342,L= 0,A= 0,W=16384
21:08:19.902	IP-10.1.1.10	00:10:4B:FE:DA:B8	139	IP-10.1.1.1	00:50:04:8D:7D:7E	1195	TCP NB SessMsg	64	S= 0,L= 0,A=3755252343,W= 0
21:08:20.313	IP-10.1.1.1	00:50:04:8D:7D:7E	1195	IP-10.1.1.10	00:10:4B:FE:DA:B8	139	TCP NetBIOS	66	S=3755252342,L= 0,A= 0,W=16384
21:08:20.314	IP-10.1.1.10	00:10:4B:FE:DA:B8	139	IP-10.1.1.1	00:50:04:8D:7D:7E	1195	TCP NB SessMsg	64	S= 0,L= 0,A=3755252343,W= 0
21:08:20.814	IP-10.1.1.1	00:50:04:8D:7D:7E	1195	IP-10.1.1.10	00:10:4B:FE:DA:B8	139	TCP NetBIOS	66	S=3755252342,L= 0,A= 0,W=16384
21:08:20.814	IP-10.1.1.10	00:10:4B:FE:DA:B8	139	IP-10.1.1.1	00:50:04:8D:7D:7E	1195	TCP NB SessMsg	64	S= 0,L= 0,A=3755252343,W= 0

This capture shows a host scan, which instigates further action on the discovery of a host. In this case, hosts 10.1.1.5 and 10.1.1.10 respond to the ARP request. After the reply to the ARP request for 10.1.1.5, the source host attempts a TCP session to port 139, a common port to attempt the WinNuke exploit. Both 10.1.1.5 and 10.1.1.10 respond on this port. 10.1.1.5 completes the three-way handshake to establish the session; 10.1.1.10 does not complete, and the connection is attempted three times.

Time	Src Logical	Src Physical	Src Port	Dest Logical	Dest Physical	Dest Port	Protocol	Size	IP Details
20:56:36.637	IP-10.1.1.1	00:50:04:8D:7D:7E		IP-10.1.1.5	00:50:04:8C:C8:99		PING Req	1518	Echo
20:56:36.638	IP-10.1.1.1	00:50:04:8D:7D:7E		IP-10.1.1.5	00:50:04:8C:C8:99		PING Rpl	1518	Echo reply
20:56:36.639	IP-10.1.1.1	00:50:04:8D:7D:7E		IP-10.1.1.5	00:50:04:8C:C8:99		PING Rpl	1518	Echo reply
20:56:36.640	IP-10.1.1.1	00:50:04:8D:7D:7E		IP-10.1.1.5	00:50:04:8C:C8:99		PING Rpl	1518	Echo reply
20:56:36.642	IP-10.1.1.1	00:50:04:8D:7D:7E		IP-10.1.1.5	00:50:04:8C:C8:99		PING Rpl	1518	Echo reply
20:56:36.643	IP-10.1.1.1	00:50:04:8D:7D:7E		IP-10.1.1.5	00:50:04:8C:C8:99		PING Rpl	1518	Echo reply
20:56:36.644	IP-10.1.1.1	00:50:04:8D:7D:7E		IP-10.1.1.5	00:50:04:8C:C8:99		PING Rpl	1518	Echo reply
20:56:36.645	IP-10.1.1.1	00:50:04:8D:7D:7E		IP-10.1.1.5	00:50:04:8C:C8:99		PING Rpl	1518	Echo reply
20:56:36.647	IP-10.1.1.1	00:50:04:8D:7D:7E		IP-10.1.1.5	00:50:04:8C:C8:99		PING Rpl	1518	Echo reply
20:56:36.648	IP-10.1.1.1	00:50:04:8D:7D:7E		IP-10.1.1.5	00:50:04:8C:C8:99		PING Rpl	1518	Echo reply
20:56:36.649	IP-10.1.1.1	00:50:04:8D:7D:7E		IP-10.1.1.5	00:50:04:8C:C8:99		PING Rpl	1518	Echo reply
20:56:36.650	IP-10.1.1.1	00:50:04:8D:7D:7E		IP-10.1.1.5	00:50:04:8C:C8:99		PING Rpl	1518	Echo reply
20:56:36.651	IP-10.1.1.1	00:50:04:8D:7D:7E		IP-10.1.1.5	00:50:04:8C:C8:99		PING Rpl	1518	Echo reply
20:56:36.653	IP-10.1.1.1	00:50:04:8D:7D:7E		IP-10.1.1.5	00:50:04:8C:C8:99		PING Rpl	1518	Echo reply
20:56:36.654	IP-10.1.1.1	00:50:04:8D:7D:7E		IP-10.1.1.5	00:50:04:8C:C8:99		PING Rpl	1518	Echo reply
20:56:36.655	IP-10.1.1.1	00:50:04:8D:7D:7E		IP-10.1.1.5	00:50:04:8C:C8:99		PING Rpl	1518	Echo reply
20:56:36.656	IP-10.1.1.1	00:50:04:8D:7D:7E		IP-10.1.1.5	00:50:04:8C:C8:99		PING Rpl	1518	Echo reply

This capture shows an echo request to the target host followed by a series of echo replies. In determining if these replies were unsolicited, we should be certain to ensure that the detection mechanism records all echo requests. In this case, source and destination are on the same subnet, and physically sharing the same medium. In a larger networked environment, log parameters might easily exclude the “outbound” echo requests, creating the illusion of unsolicited replies. Unsolicited echo replies, when targeted at different hosts, may indicate an attempt to map the network with an inverse ping scan, which succeeds when an intermediate device informs the source host when destination hosts are not reachable. This produces a map of non-existent hosts on the target network, easily inverted to show the existing devices. Inbound echo replies which prompt an outbound echo reply may indicate the presence of distributed denial of service “Servers” which often communicate to DDoS clients using ICMP as the transport.

Time	Src Logical	Src Physical	Src Port	Dest Logical	Dest Physical	Dest Port	Protocol	Size	IP Details
20:53:42.203	IP-10.1.1.10	00:10:4B:FE:DA:B8	1070	IP-10.1.1.1	00:50:04:8D:7D:7E	43	TCP Whois	78	S=3529417286,L= 0,A= 0,W=32120
20:53:42.204	IP-10.1.1.10	00:10:4B:FE:DA:B8	1080	IP-10.1.1.1	00:50:04:8D:7D:7E	53	TCP DNS	78	S=3536917363,L= 0,A= 0,W=32120
20:53:42.205	IP-10.1.1.1	00:50:04:8D:7D:7E	43	IP-10.1.1.10	00:10:4B:FE:DA:B8	1070	TCP Whois	64	S= 0,L= 0,A=3529417287,W= 0
20:53:42.206	IP-10.1.1.1	00:50:04:8D:7D:7E	53	IP-10.1.1.10	00:10:4B:FE:DA:B8	1080	TCP DNS	64	S= 0,L= 0,A=3536917364,W= 0
20:53:42.209	IP-10.1.1.10	00:10:4B:FE:DA:B8	1094	IP-10.1.1.1	00:50:04:8D:7D:7E	67	TCP BOOTP	78	S=3543420520,L= 0,A= 0,W=32120
20:53:42.209	IP-10.1.1.10	00:10:4B:FE:DA:B8	1096	IP-10.1.1.1	00:50:04:8D:7D:7E	69	TCP TFTP	78	S=3529585123,L= 0,A= 0,W=32120
20:53:42.209	IP-10.1.1.10	00:10:4B:FE:DA:B8	1097	IP-10.1.1.1	00:50:04:8D:7D:7E	70	TCP GOPHER	78	S=3535636513,L= 0,A= 0,W=32120
20:53:42.210	IP-10.1.1.10	00:10:4B:FE:DA:B8	1106	IP-10.1.1.1	00:50:04:8D:7D:7E	79	TCP Finger	78	S=3529211645,L= 0,A= 0,W=32120

This capture displays a scan for certain services (noted by the packet-capturing software) often targeted to gather information or to exploit vulnerabilities. Note that in this scan, the target host 10.1.1.1 is replying for the whois and DNS ports scanned, 43 and 53. A subsequent review of this device indicated that the host was an end-user's desktop PC, for which these services were unnecessary.

[redacted]

Src Logical	Src Physical	Src Port	Dest Logical	Dest Physical	Dest Port	Protocol	Size	IP Details
IP-10.1.1.10	00:10:4B:FE:DA:B8	63865	IP-10.1.1.5	00:50:04:8C:C8:99	346	IP TCP	64	S=3701386843,L= 0,A= 0,W= 2048
IP-10.1.1.10	00:10:4B:FE:DA:B8	63865	IP-10.1.1.5	00:50:04:8C:C8:99	93	IP TCP	64	S=3701386843,L= 0,A= 0,W= 2048
IP-10.1.1.10	00:10:4B:FE:DA:B8	63865	IP-10.1.1.5	00:50:04:8C:C8:99	1375	IP TCP	64	S=3701386843,L= 0,A= 0,W= 2048
IP-10.1.1.5	00:50:04:8C:C8:99	346	IP-10.1.1.10	00:10:4B:FE:DA:B8	63865	IP TCP	64	S= 0,L= 0,A=3701386844,W= 0
IP-10.1.1.5	00:50:04:8C:C8:99	93	IP-10.1.1.10	00:10:4B:FE:DA:B8	63865	IP TCP	64	S= 0,L= 0,A=3701386844,W= 0
IP-10.1.1.5	00:50:04:8C:C8:99	1375	IP-10.1.1.10	00:10:4B:FE:DA:B8	63865	IP TCP	64	S= 0,L= 0,A=3701386844,W= 0
IP-10.1.1.10	00:10:4B:FE:DA:B8	63865	IP-10.1.1.5	00:50:04:8C:C8:99	8888	IP TCP	64	S=3701386843,L= 0,A= 0,W= 2048
IP-10.1.1.10	00:10:4B:FE:DA:B8	63865	IP-10.1.1.5	00:50:04:8C:C8:99	1999	IP TCP	64	S=3701386843,L= 0,A= 0,W= 2048
IP-10.1.1.5	00:50:04:8C:C8:99	8888	IP-10.1.1.10	00:10:4B:FE:DA:B8	63865	IP TCP	64	S= 0,L= 0,A=3701386844,W= 0
IP-10.1.1.5	00:50:04:8C:C8:99	1999	IP-10.1.1.10	00:10:4B:FE:DA:B8	63865	IP TCP	64	S= 0,L= 0,A=3701386844,W= 0
IP-10.1.1.10	00:10:4B:FE:DA:B8	63865	IP-10.1.1.5	00:50:04:8C:C8:99	537	IP TCP	64	S=3701386843,L= 0,A= 0,W= 2048
IP-10.1.1.10	00:10:4B:FE:DA:B8	63865	IP-10.1.1.5	00:50:04:8C:C8:99	375	IP TCP	64	S=3701386843,L= 0,A= 0,W= 2048
IP-10.1.1.5	00:50:04:8C:C8:99	537	IP-10.1.1.10	00:10:4B:FE:DA:B8	63865	IP TCP	64	S= 0,L= 0,A=3701386844,W= 0
IP-10.1.1.5	00:50:04:8C:C8:99	375	IP-10.1.1.10	00:10:4B:FE:DA:B8	63865	IP TCP	64	S= 0,L= 0,A=3701386844,W= 0
IP-10.1.1.10	00:10:4B:FE:DA:B8	63865	IP-10.1.1.5	00:50:04:8C:C8:99	89	IP TCP	64	S=3701386843,L= 0,A= 0,W= 2048
IP-10.1.1.10	00:10:4B:FE:DA:B8	63865	IP-10.1.1.5	00:50:04:8C:C8:99	1387	IP TCP	64	S=3701386843,L= 0,A= 0,W= 2048
IP-10.1.1.10	00:10:4B:FE:DA:B8	63865	IP-10.1.1.5	00:50:04:8C:C8:99	1475	IP TCP	64	S=3701386843,L= 0,A= 0,W= 2048
IP-10.1.1.5	00:50:04:8C:C8:99	89	IP-10.1.1.10	00:10:4B:FE:DA:B8	63865	IP TCP	64	S= 0,L= 0,A=3701386844,W= 0
IP-10.1.1.5	00:50:04:8C:C8:99	1387	IP-10.1.1.10	00:10:4B:FE:DA:B8	63865	IP TCP	64	S= 0,L= 0,A=3701386844,W= 0
IP-10.1.1.5	00:50:04:8C:C8:99	1475	IP-10.1.1.10	00:10:4B:FE:DA:B8	63865	IP TCP	64	S= 0,L= 0,A=3701386844,W= 0

This capture shows a scan of available ports from source host 10.1.1.10 port 63865 to a variety of ports on the target host 10.1.1.5. The interesting factor in this detect is the pattern (or lack thereof) in the TCP sequence numbers. The attacker is crafting packets, all of which use the TCP sequence number 3701386843. This is not characteristic of normal TCP traffic, which should generate differing sequence numbers in the attempts to connect to these ports.

[redacted]

Time	Src Logical	Src Physical	Src Port	Dest Logical	Dest Physical	Dest Port	Protocol	Size	IP Details
20:53:01.583	IP-10.1.1.10	00:10:4B:FE:DA:B8	51966	IP-10.1.1.5	00:50:04:8C:C8:99	1410	IP UDP	64	
20:53:01.583	IP-10.1.1.10	00:10:4B:FE:DA:B8	51966	IP-10.1.1.5	00:50:04:8C:C8:99	463	IP UDP	64	
20:53:01.583	IP-10.1.1.10	00:10:4B:FE:DA:B8	51966	IP-10.1.1.5	00:50:04:8C:C8:99	410	IP UDP	64	
20:53:01.583	IP-10.1.1.5	00:50:04:8C:C8:99		IP-10.1.1.10	00:10:4B:FE:DA:B8		ICMP DUnr	74	Port unreachable: 10.1.1.5
20:53:01.583	IP-10.1.1.5	00:50:04:8C:C8:99		IP-10.1.1.10	00:10:4B:FE:DA:B8		ICMP DUnr	74	Port unreachable: 10.1.1.5
20:53:01.583	IP-10.1.1.5	00:50:04:8C:C8:99		IP-10.1.1.10	00:10:4B:FE:DA:B8		ICMP DUnr	74	Port unreachable: 10.1.1.5
20:53:01.583	IP-10.1.1.10	00:10:4B:FE:DA:B8	51966	IP-10.1.1.5	00:50:04:8C:C8:99	584	IP UDP	64	
20:53:01.583	IP-10.1.1.10	00:10:4B:FE:DA:B8	51966	IP-10.1.1.5	00:50:04:8C:C8:99	730	IP UDP	64	
20:53:01.583	IP-10.1.1.10	00:10:4B:FE:DA:B8	51966	IP-10.1.1.5	00:50:04:8C:C8:99	1508	IP UDP	64	
20:53:01.583	IP-10.1.1.10	00:10:4B:FE:DA:B8	51966	IP-10.1.1.5	00:50:04:8C:C8:99	401	IP UDP	64	
20:53:01.583	IP-10.1.1.10	00:10:4B:FE:DA:B8	51966	IP-10.1.1.5	00:50:04:8C:C8:99	588	IP UDP	64	
20:53:01.583	IP-10.1.1.5	00:50:04:8C:C8:99		IP-10.1.1.10	00:10:4B:FE:DA:B8		ICMP DUnr	74	Port unreachable: 10.1.1.5
20:53:01.583	IP-10.1.1.5	00:50:04:8C:C8:99		IP-10.1.1.10	00:10:4B:FE:DA:B8		ICMP DUnr	74	Port unreachable: 10.1.1.5

20:53:01.583	IP-10.1.1.5	00:50:04:8C:C8:99		IP-10.1.1.10	00:10:4B:FE:DA:B8		ICMP DUnr	74	Port unreachable: 10.1.1.5
20:53:01.583	IP-10.1.1.5	00:50:04:8C:C8:99		IP-10.1.1.10	00:10:4B:FE:DA:B8		ICMP DUnr	74	Port unreachable: 10.1.1.5
20:53:01.583	IP-10.1.1.5	00:50:04:8C:C8:99		IP-10.1.1.10	00:10:4B:FE:DA:B8		ICMP DUnr	74	Port unreachable: 10.1.1.5
20:53:01.584	IP-10.1.1.10	00:10:4B:FE:DA:B8	51966	IP-10.1.1.5	00:50:04:8C:C8:99	454	IP UDP	64	
20:53:01.584	IP-10.1.1.5	00:50:04:8C:C8:99		IP-10.1.1.10	00:10:4B:FE:DA:B8		ICMP DUnr	74	Port unreachable: 10.1.1.5

This capture shows both the initiating traffic from source host 10.1.1.10 and the response from destination host 10.1.1.5. The host traffic is all originating from one high-number port 51966 to a variety of UDP ports on the destination host. The destination host is replying with port unreachable messages for the closed ports. This type of scan is designed to determine what ports are open on the target host, and potentially what services are available. As a result, this type of scan is known as a UDP PORT SCAN.

[redacted]

Time	Src Logical	Src Physical	Src Port	Dest Logical	Dest Physical	Dest Port	Protocol	Size	IP Details
20:52:01.176	IP-10.1.1.10	00:10:4B:FE:DA:B8			FF:FF:FF:FF:FF:FF		ARP Req	64	10.1.1.253 = ?
20:52:01.210	IP-10.1.1.10	00:10:4B:FE:DA:B8			FF:FF:FF:FF:FF:FF		ARP Req	64	10.1.1.252 = ?
20:52:01.236	IP-10.1.1.10	00:10:4B:FE:DA:B8			FF:FF:FF:FF:FF:FF		ARP Req	64	10.1.1.251 = ?
20:52:01.266	IP-10.1.1.10	00:10:4B:FE:DA:B8			FF:FF:FF:FF:FF:FF		ARP Req	64	10.1.1.250 = ?
20:52:01.296	IP-10.1.1.10	00:10:4B:FE:DA:B8			FF:FF:FF:FF:FF:FF		ARP Req	64	10.1.1.249 = ?
20:52:01.326	IP-10.1.1.10	00:10:4B:FE:DA:B8			FF:FF:FF:FF:FF:FF		ARP Req	64	10.1.1.248 = ?
20:52:01.356	IP-10.1.1.10	00:10:4B:FE:DA:B8			FF:FF:FF:FF:FF:FF		ARP Req	64	10.1.1.247 = ?
20:52:01.386	IP-10.1.1.10	00:10:4B:FE:DA:B8			FF:FF:FF:FF:FF:FF		ARP Req	64	10.1.1.246 = ?
20:52:01.418	IP-10.1.1.10	00:10:4B:FE:DA:B8			FF:FF:FF:FF:FF:FF		ARP Req	64	10.1.1.245 = ?
20:52:01.446	IP-10.1.1.10	00:10:4B:FE:DA:B8			FF:FF:FF:FF:FF:FF		ARP Req	64	10.1.1.244 = ?
20:52:01.476	IP-10.1.1.10	00:10:4B:FE:DA:B8			FF:FF:FF:FF:FF:FF		ARP Req	64	10.1.1.243 = ?
20:52:01.506	IP-10.1.1.10	00:10:4B:FE:DA:B8			FF:FF:FF:FF:FF:FF		ARP Req	64	10.1.1.242 = ?
20:52:01.536	IP-10.1.1.10	00:10:4B:FE:DA:B8			FF:FF:FF:FF:FF:FF		ARP Req	64	10.1.1.241 = ?
20:52:01.566	IP-10.1.1.10	00:10:4B:FE:DA:B8			FF:FF:FF:FF:FF:FF		ARP Req	64	10.1.1.240 = ?
20:52:01.596	IP-10.1.1.10	00:10:4B:FE:DA:B8			FF:FF:FF:FF:FF:FF		ARP Req	64	10.1.1.239 = ?
20:52:01.626	IP-10.1.1.10	00:10:4B:FE:DA:B8			FF:FF:FF:FF:FF:FF		ARP Req	64	10.1.1.238 = ?
20:52:01.656	IP-10.1.1.10	00:10:4B:FE:DA:B8			FF:FF:FF:FF:FF:FF		ARP Req	64	10.1.1.237 = ?
20:52:01.686	IP-10.1.1.10	00:10:4B:FE:DA:B8			FF:FF:FF:FF:FF:FF		ARP Req	64	10.1.1.236 = ?
20:52:01.716	IP-10.1.1.10	00:10:4B:FE:DA:B8			FF:FF:FF:FF:FF:FF		ARP Req	64	10.1.1.235 = ?
20:52:01.746	IP-10.1.1.10	00:10:4B:FE:DA:B8			FF:FF:FF:FF:FF:FF		ARP Req	64	10.1.1.234 = ?

This capture displays an excerpt of a log that included scans across the entire subnet. In this case, the source machine (10.1.1.10) is attempting to identify all machines connected on the 10.1.1.0 subnet by performing ARP requests. The physical broadcast ensures that connected devices process the packet, and the attacker hopes to gain a record of all devices with actives IP addresses. This is generally called a HOST SCAN.

[redacted]

Time	Src Logical	Src Physical	Src Port	Dest Logical	Dest Physical	Dest Port	Protocol	Size	IP Details
20:52:08.864	IP-10.1.1.10	00:10:4B:FE:DA:B8			FF:FF:FF:FF:FF:FF		ARP Req	64	10.1.1.130 = ?
20:52:08.884	IP-10.1.1.10	00:10:4B:FE:DA:B8			FF:FF:FF:FF:FF:FF		ARP Req	64	10.1.1.96 = ?
20:52:08.894	IP-10.1.1.10	00:10:4B:FE:DA:B8			FF:FF:FF:FF:FF:FF		ARP Req	64	10.1.1.129 = ?
20:52:08.914	IP-10.1.1.10	00:10:4B:FE:DA:B8			FF:FF:FF:FF:FF:FF		ARP Req	64	10.1.1.95 = ?
20:52:08.924	IP-10.1.1.10	00:10:4B:FE:DA:B8			FF:FF:FF:FF:FF:FF		ARP Req	64	10.1.1.128 = ?
20:52:08.944	IP-10.1.1.10	00:10:4B:FE:DA:B8			FF:FF:FF:FF:FF:FF		ARP Req	64	10.1.1.94 = ?
20:52:08.954	IP-10.1.1.10	00:10:4B:FE:DA:B8			FF:FF:FF:FF:FF:FF		ARP Req	64	10.1.1.127 = ?
20:52:08.974	IP-10.1.1.10	00:10:4B:FE:DA:B8			FF:FF:FF:FF:FF:FF		ARP Req	64	10.1.1.93 = ?

20:52:08.984	IP-10.1.1.10	00:10:4B:FE:DA:B8	FF:FF:FF:FF:FF:FF	ARP Req	64	10.1.1.126 = ?
20:52:09.005	IP-10.1.1.10	00:10:4B:FE:DA:B8	FF:FF:FF:FF:FF:FF	ARP Req	64	10.1.1.92 = ?
20:52:09.014	IP-10.1.1.10	00:10:4B:FE:DA:B8	FF:FF:FF:FF:FF:FF	ARP Req	64	10.1.1.125 = ?
20:52:09.034	IP-10.1.1.10	00:10:4B:FE:DA:B8	FF:FF:FF:FF:FF:FF	ARP Req	64	10.1.1.91 = ?
20:52:09.044	IP-10.1.1.10	00:10:4B:FE:DA:B8	FF:FF:FF:FF:FF:FF	ARP Req	64	10.1.1.124 = ?
20:52:09.064	IP-10.1.1.10	00:10:4B:FE:DA:B8	FF:FF:FF:FF:FF:FF	ARP Req	64	10.1.1.90 = ?
20:52:09.074	IP-10.1.1.10	00:10:4B:FE:DA:B8	FF:FF:FF:FF:FF:FF	ARP Req	64	10.1.1.123 = ?

This capture displays an excerpt of a log including additional HOST SCANNING. In particular, the pattern of scanning is designed to attempt to reduce the likelihood of detection by automated detection systems by alternating the scan between two descending host series, in this case, 130 and below and 96 and below.

Last Updated: September 21st, 2017

Upcoming Training

SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
Community SANS Ottawa SEC503	Ottawa, ON	Oct 16, 2017 - Oct 21, 2017	Community SANS
SANS Berlin 2017	Berlin, Germany	Oct 23, 2017 - Oct 28, 2017	Live Event
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
San Diego Fall 2017 - SEC503: Intrusion Detection In-Depth	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
Community SANS Pensacola SEC503	Pensacola, FL	Nov 27, 2017 - Dec 02, 2017	Community SANS
SIEM & Tactical Analytics Summit & Training	Scottsdale, AZ	Nov 28, 2017 - Dec 05, 2017	Live Event
SANS Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS Las Vegas 2018	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	Live Event
SANS London February 2018	London, United Kingdom	Feb 05, 2018 - Feb 10, 2018	Live Event
SANS Dallas 2018	Dallas, TX	Feb 19, 2018 - Feb 24, 2018	Live Event
SANS Northern VA Spring - Tysons 2018	Tysons, VA	Mar 17, 2018 - Mar 24, 2018	Live Event
SANS Secure Canberra 2018	Canberra, Australia	Mar 19, 2018 - Mar 24, 2018	Live Event
SANS 2018	Orlando, FL	Apr 03, 2018 - Apr 10, 2018	Live Event
SANS Baltimore Spring 2018	Baltimore, MD	Apr 21, 2018 - Apr 28, 2018	Live Event
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced