Global Information Assurance Certification Paper

SANS 2000 Certification Practical

GIAC Intrusion Detection Curriculum
Practical Assignment for SNAP San Jose
May 8-13 2000

Patrick K. Pearcy

Detect 1

[**] Spoofed IP Address - Possible Snork DOS CVE-1999-0969 [**]

```
9w4d: %SEC-6-IPACCESSLOGP: list 110 denied udp 192.120.200.135(137) -> 192.120.200.255(137), 1 packet
9w4d: %SEC-6-IPACCESSLOGP: list 110 denied udp 192.120.200.17(138) -> 192.120.200.255(138), 1 packet
9w4d: %SEC-6-IPACCESSLOGP: list 110 denied udp 192.120.200.120(138) -> 192.120.200.255(138), 1 packet
9w4d: %SEC-6-IPACCESSLOGP: list 110 denied udp 192.120.200.120(137) -> 192.120.200.255(137), 1 packet
```

1. **Source of Trace:** My Network

2. **Detect was generated by:**

   Cisco router access-control list console log. Activity denied by list 110 which blocks IP address's with internal network numbers on the external (serial) interface. Fields shown above: ACL, Action, Type of Traffic, Source IP/Port, Destination IP/Port, and Number of Packets.

3. **Probability the source address was spoofed:**

   Source Address was definitely spoofed. With assistance of Cisco TAC, we were able to track the spoofed packets back to a network located in California.

4. **Description of attack:**

   Several systems at the source network are apparently generating netbios requests to broadcast addresses on the internal network in an apparent attempt to cause a DOS for systems. System Administrator at remote site states the systems are mis-configured; however, broadcast traffic is still being received. This traffic could also be attributed to a "SNORK" DOS attack (Ref: CVE 1999-0969) against the Windows NT RPC. In this attack, the attacker attempts to cause vulnerable systems to continuously "bounce" packets between various systems on the network. Since the detect traffic IP Address is spoofed, and directed at a broadcast address, this is a strong possibility.

5. **Attack Mechanism:**

   In this type of attack, the attacker attempts to cause remote Windows NT systems to consume 100% CPU utilization by "bouncing" RPC packets between various systems on the affected network.

6. **Correlation's:**

   These packets have been received by our router for approximately 3 weeks. If the systems sending these packets were accidentally mis-configured, then you would assume that within 3 weeks of notification, the system administrator would correct the problem. CVE-199-0969 discusses.

7. **Evidence of active targeting:**

   Packets are spoofed and directed against a broadcast address on the internal network.

8. **Severity:** (3 + 2) - (5 + 5) = -5.

   Critical = 3. Attack could potentially cause DOS on all systems located in affected segment of the network.

   Lethal = 2. Since attack would not cause total lockout by DOS, or user access but is considered more lethal than a null session.

   System Counter Measures = 5. All systems have latest patches to protect against this type of attack.

   Network Counter Measures = 5. Both router and firewall will block this traffic. Considered unlikely that traffic would enter network.

9. **Defensive Recommendations:**

   Re-contact the system administrator of the attacking site. Enlist the aid of their upstream ISP in blocking / stopping this traffic. Ensure router ACL's and Firewall rules block this traffic. Ensure the appropriate patch from Microsoft is applied. Patch information is available at
   http://www.microsoft.com/security/bulletins/ms98-014.htm

10. **Question:**

    The network trace shown below is an example of what type of information?

```
9w4d: %SEC-6-IPACCESSLOGP: list 110 denied udp 192.120.200.135(137) -> 192.120.200.255(137), 1 packet
9w4d: %SEC-6-IPACCESSLOGP: list 110 denied udp 192.120.200.17(138) -> 192.120.200.255(138), 1 packet
9w4d: %SEC-6-IPACCESSLOGP: list 110 denied udp 192.120.200.120(138) -> 192.120.200.255(138), 1 packet
9w4d: %SEC-6-IPACCESSLOGP: list 110 denied udp 192.120.200.120(137) -> 192.120.200.255(137), 1 packet
```

    a. Firewall Log
    b. SNORT IDS Log
    c. Cisco Access Log
    d. Shadow IDS Log

    Answer = C

Detect 2

[**] Possible "Trojan" / "Loki" Probe [**]

```
IPACCESSLOGDP: list 110 denied icmp 216.32.145.8 (Serial0/0 DLCI 408) -> 192.120.192.201 (3/3), 1 packet
IPACCESSLOGDP: list 110 denied icmp 216.32.145.8 (Serial0/0 DLCI 408) -> 192.120.192.201 (3/3), 2 packets
IPACCESSLOGDP: list 110 denied icmp 209.67.9.152 (Serial0/0 DLCI 408) -> 192.120.192.201 (3/13), 1 packet
IPACCESSLOGDP: list 110 denied icmp 210.71.225.30 (Serial0/0 DLCI 408) -> 192.120.192.201 (3/3), 1 packet
```

1. **Source of Trace:** My Network

2. **Detect was generated by:**

   Cisco router access-control list console log. Activity denied by list 110 which blocks all traffic to internal segment before the firewall where Intrusion Detection system is. IP address that external systems are trying to ping is for our IDS, which "should" have no visibility to the outside world. Fields shown above: ACL, Action, Type of Traffic, Source IP/Port, Destination IP/Port, and Number of Packets.

3. **Probability the source address was spoofed:**

   Source Address was apparently not spoofed. Address blocks of the Source IP addresses shown above belong to various ISP's (including CompuServe). Leading to the probability of these being dynamically assigned dial-up lines.

4. **Description of attack:**

   Several systems across the Internet are apparently sending ICMP echo packets to a system on the internal Internet segment of our network. Since this is a Windows NT system that does not have any services running other than the IDS system, these are apparently "probes" to see if the system is active. The traffic may also be indicative of a "loki" style of attack.

5. **Attack Mechanism:**

   Probe of system to see if active. System has been taken off-line and re-built with factory distributed software.

6. **Correlation's:**

   Router filter has been recently changed to block all traffic to the Internet segment of the internal network. The system targeted is essentially passive in nature.

7. **Evidence of active targeting:**

   Packets are not spoofed but are from dial-up connections and directed against a exposed and unprotected (in front of the firewall) address on the internal network.

8. **Severity:** (4 + 4) - (5 + 5) = -2.

   Critical = 4. Attack could potentially allow the intruder to "sniff" all traffic on the internal networks' Internet segment.

   Lethal = 4. If attacker could possible gain "root" access and "sniff" all inbound/outbound Internet traffic.

   System Counter Measures = 5. All systems have latest patches to protect against this type of attack.

   Network Counter Measures = 5. Both router and firewall will block this traffic. Considered unlikely that traffic would enter network.

9. **Defensive Recommendations:**

   Re-load the targeted system with known good software and install all security patches. Change IP Address of system. If possible use two interfaces with no IP assigned to the external interface. Ensure router ACL's and Firewall rules block this traffic.

10. **Question:**

    A "Trojan" program allows the intruder to perform which of the following?

    a. Execute remote commands
    b. Denial of service attacks
    c. Monitor keyboard "strokes" at the remote system
    d. All of the above
    e. None of the above.

    Answer = D

Detect 3

[**]Possible DNS Server Scan - Crafted Packets[**]

110 denied	Udp	207.68.61.76(4999)	192.120.255.100(53),	1 packet
110 denied	Udp	207.68.63.2(4999)	192.120.255.100(53),	1 packet
110 denied	Udp	207.68.62.140(4998)	192.120.255.100(53),	1 packet
110 denied	Udp	207.68.63.16(4999)	192.120.255.100(53),	1 packet
110 denied	Udp	207.68.62.140(4999)	192.120.255.100(53),	1 packet
110 denied	Udp	207.68.62.6(4999)	192.120.255.100(53),	1 packet
110 denied	Udp	207.68.63.15(4998)	192.120.255.100(53),	1 packet
110 denied	Udp	207.68.63.15(4998)	192.120.255.100(53),	1 packet
110 denied	Udp	207.68.62.212(4998)	192.120.255.100(53),	1 packet
110 denied	Udp	207.68.63.15(4999)	192.120.255.100(53),	1 packet
110 denied	Udp	207.68.62.150(4998)	192.120.255.100(53),	1 packet
110 denied	Udp	207.68.62.220(4999)	192.120.255.100(53),	1 packet

1. **Source of Trace:** My Network

2. **Detect was generated by:**

   Cisco router access-control list console log. Activity denied by list 110 which blocks UDP port 53 (DNS) traffic to all systems except designated servers. Fields shown above: ACL, Action, Type of Traffic, Source IP/Port, Destination IP/Port, Number of Packets.

3. **Probability the source address was spoofed:**

   Source Address was not apparently spoofed. Address blocks of the addresses shown above belong to Bell Atlantic Internet Solutions. Leading to the probability of these being dynamically assigned dial-up lines.

4. **Description of attack:**

   Several systems across the Internet are apparently sending crafted UDP packets in an effort to determine DNS servers. Trace shown above was generated over several hours; however, the source ports for requests are similar between different systems. Additionally, these packets are being sent to a broadcast address in an effort the have any DNS server on the segment answer the request. Example of "low and slow" scans since probes were from various systems IP's and spread over a length of time. Attack identified through use of Excel spreadsheet (sorting on IP's etc) to look for various traffic patterns.

5. **Attack Mechanism:**

   "Low and Slow" UDP scan looking for DNS servers by sending packets from various IP Addresses to broadcast IP address. Packets are probably from the same system and "crafted" since source port number stays relatively constant across the probes. This is considered a scan/probe instead of a DOS attack. Packets sent to port 53 of a Windows NT DNS server can cause

a DOS (CVE-1099-0275) but this probe utilized single packets spread over time.

6. **Correlation's:**

   Possibility of the same source port being used for DNS requests from different IP Addresses along with the traffic being directed to a broadcast address indicates these are crafted packets probably from the same system.

7. **Evidence of active targeting:**

   Packets are not spoofed but are from dial-up connections and directed at finding DNS servers on the internal network.

8. **Severity:** (5 + 2) - (5 + 5) = -3.

   Critical = 5. Attack is directed at finding DNS servers. Once server is identified, the attacker could use a variety of tools to attempt penetration of the system..

   Lethal = 2. Attack is a probe to discover DNS servers. A follow-on attack targeting individual servers would have a much higher rating.

   System Counter Measures = 5. All systems have latest patches to protect against this type of attack.

   Network Counter Measures = 5. Both router and firewall will block this traffic. Considered unlikely that traffic would enter network.

9. **Defensive Recommendations:**

   Contact the system administrator at AT&T WorldNet in an attempt to isolate the attacker. Ensure router ACL's and Firewall rules block this traffic.

10. **Question:**

    The below trace indicates which of the following?

110 denied	Udp	207.68.61.76(4999)	192.120.255.100(53),	1 packet
110 denied	Udp	207.68.63.2(4999)	192.120.255.100(53),	1 packet
110 denied	Udp	207.68.63.16(4999)	192.120.255.100(53),	1 packet
110 denied	Udp	207.68.62.140(4999)	192.120.255.100(53),	1 packet

a. DNS Zone Transfer
b. Denial of service attack
c. Sub 7 Attack
d. Crafted Packets

Answer = D

Detect 4

[**]Possible DNS Zone Transfer Request [**]

110	Denied	Tcp	38.185.173.6(2100)	192.120.225.100(53),	1 Packet
110	Denied	Tcp	38.185.173.6(2100)	192.120.225.100(53),	1 Packet

1. **Source of Trace:** My Network

2. **Detect was generated by:**

   Cisco router access-control list console log. Activity denied by list 110 which blocks TCP port 53 (DNS Zone Transfer request) traffic to all systems. Fields shown above: ACL, Action, Type of Traffic, Source IP/Port, Destination IP/Port, Number of Packets.

3. **Probability the source address was spoofed:**

   Source Address was not apparently spoofed. Address blocks of the addresses shown above belong to PSI Net and are assigned to a DNS server.

4. **Description of attack:**

   Possible prelude (reconnaissance) to an attack, or a mis-configured DNS server.

5. **Attack Mechanism:**

   Attacker attempting to retrieve a DNS Listing of the domain as a possible prelude to an attack against specific targets. This may also be indicative of a mis-configured DNS server. While the target system is a DNS server on the internal network, all zone transfers should be taking place between two internal systems (the primary and backup DNS servers for the domain) and no external zone transfers should occur. However, since the source system is a DNS (in-addr-arrpa) server for PSI net, this is probably the most likely cause of this traffic - or the PSI net server is compromised.

6. **Correlation's:**

   Several TCP port 53 requests from the same system at approximately 1 hour intervals.

7. **Evidence of active targeting:**

   Packets are not spoofed but are from a DNS server on another network.

8. **Severity:** (5 + 3) - (5 + 5) = -3.

   Critical = 5. Attack is directed at retrieving a Zone Transfer from the DNS server. If successful, the attacker could use a variety of tools to attempt penetration of the identified systems.

   Lethal = 3. Attack is an attempt at reconnaissance of the DNS servers. A follow-on attack targeting individual systems would have a much higher rating.

   System Counter Measures = 5. All systems have latest patches to protect against this type of attack.

   Network Counter Measures = 5. Both router and firewall will block this traffic. Considered unlikely that traffic would enter network.

9. **Defensive Recommendations:**

   Contact the system administrator at PSI Net in an attempt to isolate correct the system. Ensure router ACL's and Firewall rules block this traffic.

10. **Question:**

    DNS Zone Transfers are _____ ?

    a. A normal method of resolving names to IP Addresses
    b. A form of Denial of service attack
    c. Normally restricted to only DNS servers for the domain.
    d. Crafted Packets designed to overload the target server

    Answer = C

Detect 5

[**]Possible Port Scan, Crafted Packet[**]

110 Denied	udp	24.12.165.75(39559)	192.120.146.146(33524),	1 packet
110 Denied	udp	24.12.165.75(39559)	192.120.146.146(33523),	1 packet
110 Denied	udp	24.12.165.75(39559)	192.120.146.146(33522),	1 packet
110 Denied	udp	24.12.165.75(39559)	192.120.146.146(33521),	1 packet
			…	
			…	
110 Denied	udp	24.12.165.75(39559)	192.120.146.146(33512),	1 packet
110 Denied	udp	24.12.165.75(39559)	192.120.146.146(33511),	1 packet

1. **Source of Trace:** My Network

2. **Detect was generated by:**

   Cisco router access-control list console log. Activity denied by list 110 which blocks UDP traffic above 30000 (trace route) traffic to all systems. Fields shown above: ACL, Action, Type of Traffic, Source IP/Port, Destination IP/Port, Number of Packets.

3. **Probability the source address was spoofed:**

   Source Address was not apparently spoofed. Address blocks of the addresses shown above belong to @Home.COM and are assigned to a static IP Address (c767683-a.crvlls1.or.home.com).

4. **Description of attack:**

   Possible prelude (reconnaissance) to an attack looking for open ports that could be exploited.

5. **Attack Mechanism:**

   Attacker is attempting to find all open ports on any system(s) located in the internal network address block for later exploitation. Note: Packet is probably crafted due to same source port for all requests.

6. **Correlation's:**

   Several UDP port requests from the same system to different destination ports using the same source port at varying intervals.

7. **Evidence of active targeting:**

   Packets are not spoofed but are targeting systems on the internal network, sequentially scanning the system looking for open ports for later exploitation.

Note: Destination system shown above does not exist - which leads to belief that this is part of a larger block of systems being scanned.

8. **Severity:** (3 + 2) - (5 + 5) = -5.

   Critical = 3. Attacker is scanning all systems looking for open ports.

   Lethal = 2. Attack is an attempt at reconnaissance of the network. A follow-on attack targeting individual systems would have a much higher rating.

   System Counter Measures = 5. All systems have latest patches to protect against this type of attack.

   Network Counter Measures = 5. Both router and firewall will block this traffic. Considered unlikely that traffic would enter network.

9. **Defensive Recommendations:**

   Contact the system administrator at @Home.Com in an attempt to isolate and shutdown the system. Ensure router ACL's and Firewall rules block this traffic.

10. **Question:**

    Sequential packets with the same source port number are generally:

    a. A normal event
    b. A result of a Denial of Service Attack
    c. Not going to happen, but if it does disregard.
    d. Crafted Packets

    Answer = D

Detect 6

[**]Smurf Attack, CVE-1999-0513[**]

```
110 denied     icmp      152.163.245.35      192.120.192.201  (3/3),      2 packets
110 Denied     icmp      152.163.245.34      192.120.192.201  (3/3),      1 packet
110 Denied     icmp      152.163.245.34      192.120.192.201  (3/3),      2 packets
110 Denied     icmp      152.163.245.33      192.120.192.201  (3/3),      2 packets
110 Denied     icmp      152.163.245.32      192.120.192.201  (3/3),      1 packet
110 Denied     icmp      152.163.245.32      192.120.192.201  (3/3),      2 packets
110 Denied     icmp      152.163.245.17      192.120.192.201  (3/3),      1 packet
110 Denied     icmp      152.163.245.17      192.120.192.201  (3/3),      2 packets
110 Denied     icmp      152.163.245.16      192.120.192.201  (3/3),      1 packet
110 Denied     icmp      152.163.245.16      192.120.192.201  (3/3),      2 packets
110 Denied     icmp      152.163.245.114     192.120.192.201  (3/3),      1 packet
110 Denied     icmp      152.163.245.114     192.120.192.201  (3/3),      2 packets
110 Denied     icmp      152.163.245.112     192.120.192.201  (3/3),      1 packet
110 Denied     icmp      152.163.245.112     192.120.192.201  (3/3),      2 packets
110 Denied     icmp      152.163.244.99      192.120.192.201  (3/3),      1 packet
```

1. **Source of Trace:** My Network

2. **Detect was generated by:**

   Cisco router access-control list console log. Activity denied by list 110 which blocks ICMP Echo traffic to all systems. Fields shown above: ACL, Action, Type of Traffic, Source IP/Port, Destination IP/Port, Number of Packets.

3. **Probability the source address was spoofed:**

   Source Address was spoofed. A IP Address of a system on our internal network was apparently spoofed and used to generate a Echo request to the 152.163.244.x Network. Source IP network shown above belongs to AOL.

4. **Description of attack:**

   The Smurf Attack is a Denial of Service attack, which uses an intermediary network to overload the target network (in this case our internal network). By sending one echo request (with a spoofed source IP address) to a broadcast address on the intermediary network, the attacker is able to generate massive Echo replies overloading the targeted system/network causing a Denial of Service. Note: Several other sites have also been identified as Smurf Intermediaries in a coordinated attack against the internal network.

5. **Attack Mechanism:**

   Attacker has Spoofed a IP address on our internal network and sent a broadcast echo reply to systems at AOL. AOL has then generated echo replies to our network.

6. **Correlation's:**

   Numerous ICMP echo replies from sequential systems at AOL in response to a system on our internal network which would normally not generate any Echo requests. CVE-1999-0513 and CERT Advisory 98.01 discuss. Note: Used Excel to sort the Cisco Log by IP Address to identify the coordinated attack.

7. **Evidence of active targeting:**

   Packets are spoofed and are targeting a system on the internal network in an attempt to overload the network or system resulting in a Denial of Service.

8. **Severity:** (4 + 5) - (5 + 2) = 2.

   Critical = 4. Attacker is overloading the network..

   Lethal = 5. Attack is almost causing a total DOS to all network users.

   System Counter Measures = 5. All systems have latest patches to protect against this type of attack.

   Network Counter Measures = 2. While both the router and firewall will block this traffic, because of this type of attack can use all available bandwidth to the Internet, even if the traffic does not reach the internal systems, a Denial of Service can occur.

9. **Defensive Recommendations:**

   Contact the system administrator at AOL (mailto:OPSSEC@AOL.COM) in an attempt to prevent their systems from being used as a Intermediary network. For Cisco routers, the Cisco Interface command - "no IP directed-broadcast" and specific ACL's on edge routers can prevent them from being used as a Smurf Intermediary site. Additionally, contact the upstream ISP and ask that a bandwidth limitation be set for ICMP traffic (http://www.cisco.com/warp/public/707/newsflash.html). Additionally, ensure router ACL's and Firewall rules block this traffic.

10. **Question:**

    In a Smurf Attack, the source IP of the packet is _____ and the target IP address is _____.

    a. A broadcast address, Spoofed
    b. Spoofed, Illegal
    c. Spoofed, a broadcast Address.
    d. Spoofed, the Address of victim

    Answer = D

Detect 7

[**]NetBus Attack, CAN-1999-0660[**]

```
list  110 Denied  tcp  210.216.225.206(3786)   192.120.60.255(12345),    1 packet
list  110 Denied  tcp  210.216.225.206(3785)   192.120.60.255(12345),    1 packet
list  110 Denied  tcp  210.216.225.206(3786)   192.120.60.255(12345),    1 packet
```

1. **Source of Trace:** My Network

2. **Detect was generated by:**

   Cisco router access-control list console log. Activity denied by list 110 which blocks traffic to all broadcast addresses. Fields shown above: ACL, Action, Type of Traffic, Source IP/Port, Destination IP/Port, Number of Packets.

3. **Probability the source address was spoofed:**

   Source Address was not apparently spoofed. The address block is registered to a Korean ISP. Strong probability that the IP Address of the attacker is a dial-up connection.

4. **Description of attack:**

   NetBus is a Trojan horse program for Windows 9x and NT systems that allow a remote operator to take total control of a system. NetBus listens on port 12345 for commands. Note: This appears to be a coordinated attack from several sites - while the trace above does not show the other sites (omitted for clarity/brevity), analysis of the incoming traffic shows that different sites are scanning different ranges of IP addresses for the NetBus "Trojan" sequentially.

5. **Attack Mechanism:**

   An unsuspecting user installs a "Trojan" program on a target system. Later, the attacker broadcasts a TCP packet to port 12345 which systems with the Trojan program installed will respond to. Once a system has responded to the initial query packet, the Attacker will then send further packets / commands to the system.

6. **Correlation's:**

   Traffic to port 12345 of a internal broadcast address. CAN-1999-0660 discusses.

7. **Evidence of active targeting:**

   Packets are not spoofed but belong to a Korean ISP targeting a "Trojan" program on the internal network.

8. **Severity:** (2 + 5) - (5 + 5) = -3.

   Critical = 2. Attacker is generally targeting Desktop systems on the internal network.

   Lethal = 5. Attack could allow the attacker "root" access to the system.

   System Counter Measures = 5. All systems have latest patches to protect against this type of attack.

   Network Counter Measures = 5. Both the router and firewall will block this traffic. Additionally, installed anti-virus software will detect the "Trojan" program.

9. **Defensive Recommendations:**

   Contact the system administrator at the Korean ISP (BoraNet) and attempt to isolate / prevent this traffic. Ensure router ACL's and Firewall rules block this traffic.

10. **Question:**

    Netbus is a program, which will allow a remote user/attacker to perform which of the following on the compromised system:

    a. Observe Keystrokes
    b. Open/Close CD-ROM drive
    c. Play Sounds.
    d. Copy files
    e. All the Above
    f. None of the Above

    Answer = E

Detect 8

[**]Back Orifice Scan CAN-1999-0660[**]

```
12-Jun-00 11:49:29 drop   Blocked_TCP31337-BackOrifice   192.120.1.31   192.120.226.101     tcp   61785
12-Jun-00 11:49:29 drop   Blocked_TCP31337-BackOrifice   192.120.1.31   192.120.226.101     tcp   61963
12-Jun-00 11:49:29 drop   Blocked_TCP31337-BackOrifice   192.120.1.31   192.120.226.101     tcp   62135
12-Jun-00 11:49:33 drop   Blocked_TCP31337-BackOrifice   192.120.1.31   192.120.226.101     tcp   63320
12-Jun-00 11:49:34 drop   Blocked_TCP31337-BackOrifice   192.120.1.31   192.120.226.101     tcp   63327
12-Jun-00 11:49:34 drop   Blocked_TCP31337-BackOrifice   192.120.1.31   192.120.226.101     tcp   63334
12-Jun-00 11:54:32 drop   Blocked_TCP31337-BackOrifice   192.120.1.31   192.120.226.102     tcp   64167
12-Jun-00 11:54:33 drop   Blocked_TCP31337-BackOrifice   192.120.1.31   192.120.226.102     tcp   64346
12-Jun-00 11:54:33 drop   Blocked_TCP31337-BackOrifice   192.120.1.31   192.120.226.102     tcp   64505
12-Jun-00 11:54:36 drop   Blocked_TCP31337-BackOrifice   192.120.1.31   192.120.226.102     tcp   65059
12-Jun-00 11:54:36 drop   Blocked_TCP31337-BackOrifice   192.120.1.31   192.120.226.102     tcp   65066
12-Jun-00 11:54:37 drop   Blocked_TCP31337-BackOrifice   192.120.1.31   192.120.226.102     tcp   65073
12-Jun-00 14:48:17 drop   Blocked_TCP31337-BackOrifice   192.120.1.31   192.120.152.127     tcp   37382
12-Jun-00 14:48:17 drop   Blocked_TCP31337-BackOrifice   192.120.1.31   192.120.152.127     tcp   37396
12-Jun-00 14:50:18 drop   Blocked_TCP31337-BackOrifice   192.120.1.31   192.120.152.127     tcp   42432
12-Jun-00 14:50:18 drop   Blocked_TCP31337-BackOrifice   192.120.1.31   192.120.152.127     tcp   42445
12-Jun-00 14:56:46 drop   Blocked_TCP31337-BackOrifice   192.120.1.31   192.120.152.129     tcp   44876
12-Jun-00 14:56:46 drop   Blocked_TCP31337-BackOrifice   192.120.1.31   192.120.152.129     tcp   44895
12-Jun-00 14:57:49 drop   Blocked_TCP31337-BackOrifice   192.120.1.31   192.120.152.129     tcp   47664
```

1. **Source of Trace:** My Network

2. **Detect was generated by:**

   Checkpoint FW-1 Activity Log. Activity denied by rule 2 which blocks traffic to known "hacker ports". Fields shown above: Date, Time, Action, Service (destination port/type), Source IP, Destination IP, Traffic Type, and Source Port.

3. **Probability the source address was spoofed:**

   Source Address was not spoofed. All traffic shown above was detected on the internal network The source IP address shown above is valid and assigned to a user on our internal network.

4. **Description of attack:**

   Back Orifice is a client/server application that can gather information, execute system commands, reconfigure systems and redirect network traffic. Back Orifice by default listens on port 31337 but this may be reconfigured as the attacker needs.

5. **Attack Mechanism:**

   An unsuspecting user installs a "Trojan" program on a target system. Later, the attacker sends traffic to port 31337 which systems with the Trojan

program installed will respond to. Once a system has responded to the initial query packet, the Attacker will then send further packets / commands to the system.

6. **Correlation's:**

   Traffic to port 31337 of a internal broadcast address. CAN-1999-0660 discusses. Additionally, contacted system administrator of source IP system. He admitted to a scan of some internal systems under his control using NMAP to locate any Back Orifice installations.

7. **Evidence of active targeting:**

   Packets are not spoofed and are assigned to a valid IP address. Apparent probe to locate Back Orifice servers.

8. **Severity:** (2 + 5) - (5 + 5) = -3.

   Critical = 2. Attacker is generally targeting Desktop systems on the internal network.

   Lethal = 5. Attack could allow the attacker "root" access to the system.

   System Counter Measures = 5. All systems have latest patches to protect against this type of attack.

   Network Counter Measures = 5. Both the router and firewall will block this traffic. Additionally, installed anti-virus software will detect the "Trojan" program.

9. **Defensive Recommendations:**

   Contact the system administrator and ensure appropriate administrative action is taken to prevent scans/probes in the future. Ensure router ACL's, Firewall rules block this traffic and systems have latest virus software installed.

10. **Question:**

    Back Orifice is a program, which is best described as:

    a. Harmless used for playing jokes on system administrators only.
    b. Flawed, does not work but causes anti-virus software to alert
    c. Trojan program which allows remote control of a system
    d. Acts as host for playing network games
    e. None of the Above

    Answer = C

Detect 9

[**]SYN-FIN Scan [**]
07:48:07.940670 211.50.52.135.111 > sxaa.axxx.org.111: SF 436513241:436513241(0) win 1028
07:48:07.954774 211.50.52.135.111 > xxc.axxx.org.111: SF 436513241:436513241(0) win 1028
07:48:07.977643 211.50.52.135.111 > xxc.axxx.org.111: SF 436513241:436513241(0) win 1028
07:48:07.997632 211.50.52.135.111 > xxst.sxxx.org.111: SF 436513241:436513241(0) win 1028
07:48:08.037526 211.50.52.135.111 > xxsc.axxx.org.111: SF 436513241:436513241(0) win 1028
07:48:08.041061 211.50.52.135.111 > xxgen.axxx.org.111: SF 436513241:436513241(0) win 1028
07:48:08.080712 211.50.52.135.111 > xxrp.axxx.org.111: SF 436513241:436513241(0) win 1028
07:48:08.095522 211.50.52.135.111 > xxcxey.axxx.org.111: SF 436513241:436513241(0) win 1028
07:48:08.100523 211.50.52.135.111 > rxxsp.axxx.org.111: SF 436513241:436513241(0) win 1028
07:48:08.114693 211.50.52.135.111 > ixxosleuth.axxx.org.111: SF 436513241:436513241(0) win 1028
07:48:08.137628 211.50.52.135.111 > xxbxxrk.axxx.org.111: SF 436513241:436513241(0) win 1028
07:48:08.154635 211.50.52.135.111 > xxexxse.axxx.org.111: SF 436513241:436513241(0) win 1028

1. **Source of Trace:** My Network

2. **Detect was generated by:**

   Shadow Activity Log. Fields shown above: Time, Source IP/Port, Destination IP/Port, Flags, Sequence Number, and Windows size.

3. **Probability the source address was spoofed:**

   Source Address was probably not spoofed. Since the intent of this attack is to map network systems, the source IP must be valid to obtain the information from the scan.

4. **Description of attack:**

   In this scan, the attacker used a impossible flag combination (SYN-FIN set simultaneously) to scan a range of systems on the internal network. Under normal conditions these flags will never be set together.

5. **Attack Mechanism:**

   The attacker is using a crafted packet (SYN-FIN set and with the same sequence number for each packet). When a Linux system receives these packets, it responds with a SYN-FIN-ACK. Additionally, by using this combination, the attacker is hoping to bypass some Intrusion Detection devices, or Firewall/Router rules.

6. **Correlation's:**

   Crafted packets to port 111 (Sun RPC) of a range of systems. Similar bug-traq posting at http://www.securityfocus.com

7. **Evidence of active targeting:**

   Packets are crafted and not spoofed targeting a range of IP's on the internal network. Apparent probe to locate systems/servers.

8. **Severity:** (3 + 2) - (5 + 5) = -5.

   Critical = 3. Attacker is probing for systems on internal network.

   Lethal = 2. Attack is a probe. After systems are identified, the attacker would then use other tools in an attempt to compromise the system.

   System Counter Measures = 5. All systems have latest patches to protect against this type of attack.

   Network Counter Measures = 5. Both the router and firewall will block this traffic.

9. **Defensive Recommendations:**

   Contact the system administrator and ensure appropriate administrative action is taken to prevent scans/probes in the future. Ensure router ACL's, Firewall rules block this traffic and systems have latest virus software installed.

10. **Question:**

    The network trace below indicates which of the following:

```
07:48:07.940670 211.50.52.135.111 > 192.168.201.201.111: SF 436513241:436513241(0) win 1028
07:48:07.954774 211.50.52.135.111 > 192.168.201.202.111: SF 436513241:436513241(0) win 1028
07:48:07.977643 211.50.52.135.111 > 192.168.201.203.111: SF 436513241:436513241(0) win 1028
07:48:07.997632 211.50.52.135.111 > 192.168.201.204.111: SF 436513241:436513241(0) win 1028
07:48:08.037526 211.50.52.135.111 > 192.168.201.205.111: SF 436513241:436513241(0) win 1028
```

    a. Normal network traffic.
    b. Smurf Attack
    c. Trojan program which allows remote control of a system
    d. Crafted Packet
    e. None of the Above

    Answer = D

Detect 10

[**]RingZero Trojan Scan[**]
202.9.149.104 > 147.120.127.195
06:24:33.715047 202.9.149.104.3932 > 192.120.127.195.3128: S 3275695:3275695(0) win 8192 (DF)
06:24:36.772339 202.9.149.104.3932 > 192.120.127.195.3128: S 3275695:3275695(0) win 8192 (DF)
06:24:42.828153 202.9.149.104.3932 > 192.120.127.195.3128: S 3275695:3275695(0) win 8192 (DF)
06:24:55.037172 202.9.149.104.3932 > 192.120.127.195.3128: S 3275695:3275695(0) win 8192 (DF)

202.63.110.9 > 147.120.0.1
06:56:53.040845 202.63.110.9.1169 > 192.120.0.1.3128: S 1127582:1127582(0) win 8192 (DF)
06:56:59.486707 202.63.110.9.1169 > 192.120.0.1.3128: S 1127582:1127582(0) win 8192 (DF)
06:57:12.373837 202.63.110.9.1169 > 192.120.0.1.3128: S 1127582:1127582(0) win 8192 (DF)
06:57:49.883539 202.63.110.9.1178 > 192.120.0.1.3128: S 1187663:1187663(0) win 8192 (DF)
06:57:53.084963 202.63.110.9.1178 > 192.120.0.1.3128: S 1187663:1187663(0) win 8192 (DF)

1. **Source of Trace:** My Network

2. **Detect was generated by:**

   Shadow Activity Log. Fields shown above: Time, Source IP/Port, Destination IP/Port, Flags, Sequence Number, and Windows size.

3. **Probability the source address was spoofed:**

   Source Address was not apparently spoofed. The address block is registered to the Asia Pacific Internet Company. Strong probability that the IP Address of the attacker is a dial-up connection.
   .

4. **Description of attack:**

   RingZero is a "Trojan" program, which is usually distributed as a Windows Executable. When installed on systems, the program scans random addresses for responses to ports 80 /8080 / 3128 (known proxy ports). When a response is received, a CGI Program is run recording the Proxy Servers IP Address.

5. **Attack Mechanism:**

   The "Trojan" program is installed in Windows systems and run each time the OS Starts. During execution, the "Trojan" scans networks for responses to port 80, 8080 or 3128 (common proxy ports). When a response is received, a CGI script appears to be executed storing the information about the proxy servers.

6. **Correlation's:**

   Please see: http://www.oit.gatech.edu/security/pc/ringzero.html or http://www.symantec.com/avcenter/cgi-bin/virauto.cgi?vid=10476.

7. **Evidence of active targeting:**

   Packets are not spoofed and are directed to a internal broadcast address. Apparent probe to locate Proxy servers. Actual victim in this case is the Source IP Systems.

8. **Severity:** (3 + 3) - (5 + 5) = -3.

   Critical = 2. Attacker is generally targeting Desktop systems on the internal network.

   Lethal = 2. Attack scans for proxy servers.

   System Counter Measures = 5. All systems have latest patches to protect against this type of attack.

   Network Counter Measures = 5. Both the router and firewall will block this traffic. Additionally, installed anti-virus software will detect the "Trojan" program.

9. **Defensive Recommendations:**

   Contact the system administrator of the source IP and ensure appropriate administrative action is taken to prevent scans/probes in the future. Ensure router ACL's, Firewall rules block this traffic and systems have latest virus software installed.

10. **Question:**

    The following best describes what a "Proxy" server is:

    a. Used to host Network Based games such as "Quake".
    b. Used to allow Internet Relay Chat (IRC) communications
    c. Used as a Intermediary system allowing commands to be issued from it
    d. Acts as host for NMAP
    e. None of the Above

    Answer = C

Last Updated: July 22nd, 2017

Upcoming Training

SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
SANS vLive - SEC503: Intrusion Detection In-Depth	SEC503 - 201709,	Sep 11, 2017 - Oct 18, 2017	vLive
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Baltimore Fall 2017 - SEC503: Intrusion Detection In-Depth	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS Scottsdale SEC503	Scottsdale, AZ	Oct 02, 2017 - Oct 07, 2017	Community SANS
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
San Diego Fall 2017 - SEC503: Intrusion Detection In-Depth	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
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 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 Dallas 2018	Dallas, TX	Feb 19, 2018 - Feb 24, 2018	Live Event
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced