Global Information Assurance Certification Paper

*** Northcutt, 70

GIAC Certification Requirement: PRACTICAL

Andrew J Boncek
Date Submitted: 04/29/2000

ALL IPs HAVE BEEN SCRUBBED FOR CONFIDENTIALITY PURPOSES. MONTHS AND DAYS HAVE BEEN "xx" OUT FOR CONFIDENTIALITY.

CONVENTIONS
FW = Firewall
RS = RealSecure
SH = SHADOW
SRT = Snort
BI = BlackICE

DB = Database

Incident #1: Port 139 Windows Access Attempt from a foreign country

RS 2000/xx/xx 07:48:09 Windows_Access_Error 192.168.1.1.2357 > my.site.139 TCP INFO: ERROR logon failure
RS 2000/xx/xx 07:48:09 Windows_Access_Error 192.168.1.1.2357 > my.site.139 TCP INFO: CODE C000006D
RS 2000/xx/xx 07:4:11 Windows_Access_Error 192.168.1.1.2357 > my.site.139 TCP INFO: ERROR logon failure
RS 2000/xx/xx 07:48:11 Windows_Access_Error 192.168.1.1.2357 > my.site.139 TCP INFO: CODE C000006D
RS 2000/xx/xx 07:49:15 Windows_Access_Error 192.168.1.1.2357 > my.site.139 TCP INFO: ERROR logon failure
RS 2000/xx/xx 07:48:15 Windows_Access_Error 192.168.1.1.2357 > my.site.139 TCP INFO: CODE C000006D
RS 2000/xx/xx 07:48:24 Windows_Access_Error 192.168.1.1.2357 > my.site.139 TCP INFO: ERROR logon failure
RS 2000/xx/xx 07:48:24 Windows_Access_Error 192.168.1.1.2357 > my.site.139 TCP INFO: CODE C000006D
etc....

1. Origin

Foreign Country. One host was the perpetrator for approximately 4 incident reports through the course of two months. We blocked the IP at the border router and firewall.

2. Technique

Repititious source port 2357 and 3-9 second interval makes this appear to be some type of constructed packet or automated tool. Possible

3. Intent

Logon to Windows NT machine on DMZ.

4. Active Targeting

Yes. Located a Windows NT machine (with probable prior probing via nmap or other OS fingerprinting tool). Prior history queries on DB did not return traffic from that or prior probes.

5. Research

No known exploit has this signature in the Whitehats.com DB, Packetstorm tool search, or open-source email search. It is possible it is a buffer overflow attempt on port 139 or just a typical logon sequence.

6. Evaluation/Recommendation

Definite attempt to penetrate a DMZ machine via a tool or known exploit. Host was blacklisted and put on a watch list for other attempts at the site.

Incident #2: nmap source port 0, OS fingerprint scan of single host

SH 2000/xx/xx 20:06:58 172.16.x.x.7599 > my.site.53 domain
RS 2000/xx/xx 20:10:08 IPFrag 172.16.x.x.0 > my.site.0 S
RS 2000/xx/xx 20:10:13 IPFrag 172.16.x.x.0 > my.site.0 S

RS 2000/xx/xx 20:07:03 IPFrag 172.16.x.x.0 > my.site.0 S
RS 2000/xx/xx 20:13:18 PING 172.16.x.x > my.site ICMP
RS 2000/xx/xx 20:13:18 PING 172.16.x.x > my.site ICMP
RS 2000/xx/xx 20:13:18 PING 172.16.x.x > my.site ICMP
RS 2000/xx/xx 20:13:23 IPFrag PING 172.16.x.x > my.site ICMP
RS 2000/xx/xx 20:13:23 IPFrag PING 172.16.x.x > my.site ICMP
RS 2000/xx/xx 20:13:23 IPFrag PING 172.16.x.x > my.site ICMP

1. Origin

Nonexistent, IANA reserved (172.16.x.x.). Spoofed source IP.

2. Technique

Used nmap's IP fragmentation charateristics to probe single host for a particular OS. Used a spoofed IP charateristics inherent to nmap.

3. Intent

Target a specific host and try and determine which OS it is using. Also, the pings could be an attempt to distance vector the host to the intruder, although unlikely.

4. Active targeting

Yes. Single host probe and attempt to determine OS.

5. Research

Open-source research points to this as the common characteristics of an nmap OS fingerprinting scan with source hiding.

6. Evaluation/Recommendation

Host is actively targeting a single host and trying to OS fingerprint. Intruder's intentions should be considered in the first phase of actively attempting to use an exploit and compromise the system.

Incident #3: DNS Poisoning and possible Trojan Scan

FW 2000/xx/xx 00:17:51 smoked.so.much.pot.he.went.madd.net.36714 > my.site.6004 drop
SH 2000/xx/xx 00:17:51 smoked.so.much.pot.he.went.madd.net.36714 > my.site.6004
SH 2000/xx/xx 00:17:52 smoked.so.much.pot.he.went.madd.net.36714 > my.site.6004

1. Origin

Unknown. Host has obviously chosen to poison a particular DNS server's cache to mask the true identity.

2. Technique

Scanned a single host for port 6004.

3. Intent

Possibly looking for a Trojan. Will research for port on common Trojan lists.

4. Active Targetting

Yes. Singled out an internal host that was running web services.

5. Research

Port 6004 is a common X11 port. Also, Port 6004 did not appear on the ONTEK and other Trojan portlists as a trojan port.

6. Evaluation/Recommendation

Locate DNS server that had cache poisoning and contact sys admin. Check host for possible traffic on port 6004 or an X11 server.

Incident #4: Port Mapping including NetBus Pro port 35002
Ports are high, 34000-36000

RS 2000/xx/xx 03:07:10 192.168.1.1.20 > my.site.35002 S
SH 2000/xx/xx 03:06:30 192.168.1.1.20 > my.site.35002 S
SH 2000/xx/xx 03:06:41 192.168.1.1.20 > my.site.35002 S
SH 2000/xx/xx 03:06:45 192.168.1.1.20 > my.site.35002 S
SH 2000/xx/xx 03:06:54 192.168.1.1.20 > my.site.35002 S
SH 2000/xx/xx 03:07:01 192.168.1.1.20 > my.site.35002 S
SH 2000/xx/xx 03:07:07 192.168.1.1.20 > my.site.35002 S
SH 2000/xx/xx 03:07:19 192.168.1.1.20 > my.site.35002 S

1. Origin

Foreign country.

2. Technique

Send SYN packets to port 35002 to attempt to initiate a connection. Probe high ports 34000-36000 and NetBus Pro port 35002 for listening connection.

3. Intent

Discover NetBus Pro remote administration port access for further exploitation.

4. Active Targetting

Not known. Past queries did not result in further traffic for host scans.

5. Research

Typical probe for NetBus Pro.

6. Evaluation/Recommendation

Not a high priority incident and the target host did not have Netbus Pro installed.

Incident #5: sunrpc portscan

FW 2000/xx/xx 12:20:21 192.168.1.1.55891 > my.site.111 drop
RS 2000/xx/xx 12:20:21 pmapdump 192.168.1.1.55981 > my.site.111
SH 2000/xx/xx 12:20:21 192.168.1.1.55981 > my.site.111 sunrpc
SNT 2000/xx/xx 12:20:21 192.168.1.1.55981 > my.site.111

1. Origin

Foreign country.

2. Technique

Standard sunrpc scan but with only a single packet. Intruder may have thought he/she could "fly-low" and not be noticed but all the sensors and firewalls picked it up.

3. Intent

Compromise vulnerable Sun box via port 111 or map all ports.

4. Active targetting

Probably yes. No prior history of scanning for boxes in DB but does not necessarily mean the attacker had not in the past.

5. Research

See affore mentioned sunrpc comments

6. Evaluation/Recommendation

Typical sunrpc probe that tried to "fly-low". However, the intruder will be on the watch list and examined for possible further attempts to access the site.

Incident #6: Suspicious or corrupted traffic from mail host

FW 2000/xx/xx 05:21:01 mail.net.30929 > my.site.20 ftp-data drop
SH 2000/xx/xx 13:48:31 mail.net.3832 > my.site.25 smtp (6 packets) FLAGS: S SA FA FA FPA R
SH 2000/xx/xx 13:48:31 mail.net.4096 > my.site.25 smtp (8 packets) FLAGS: S SA FA FA FA R R R
FW 2000/xx/xx 05:21:01 mail.net.30929 > my.ste.20 ftp-data drop
SH 2000/xx/xx 13:48:31 mail.net.2711 > my.site.25 smtp (3 packets) FLAGS: S SA FA

SH 2000/xx/xx 12:39:30 Misc TCP mail.net.50632 > my.site.50632 FLAGS: SFRPA (Christmas tree packet)
SNT 2000/xx/xx 12:39:30 SCAN-NULLScan mail.net.30720 > my.site.104
continued mail and ftp connections....

1. Origin

Demon.net mail host. Demon.net (as mentioned in the IDIC courses) has a "bad router" that seems to continually corrupt packets.

2. Technique

Potentially, this is a simple mail transfer. However, the packets demonstrating a an ftp connection at 13:48 are concerning since the hosts in question are merely mail servers.

3. Intent

Unknown. Again, could be a possible corrupted packets from the Demon.net router in question.

4. Active Targeting

No.

5. Research

Calls to Demon.net indicate that it could be from the router. However, the suggest looking into why their where ftp connections to and from the host with only a small amount of data pushed. They are also checking their system for compromise and will email back. Applied knowledge gained at SANS about Demon.net.

6. Evaluation/Recommendations

Continue to monitor ftp and smtp traffic to and from these hosts. Watch for continued "corrupted packets" or possible malicious intent.

Incident #7: BackOrifice Scan port 31337

RS 2000/xx/xx 23:00:09 somewhere.edu.3099 > my.site.31337 BackOrifice
RS 2000/xx/xx 23:00:09 somewhere.edu.3099 > my.site.31337 BackOrifice
RS 2000/xx/xx 23:02:30 somewhere.edu.3099 > my.site.31337 BackOrifice
etc..... Scanned 3 Class C address spaces without specific host identification.

1. Origin

University host.

2. Technique

Probe 3 Class C address spaces for BackOrifice clients. Scanned from a location near our site in an attempt to possibly mask id.

3. Intent

Find BackOrifice clients.

4. Active Targeting

No. Scanned 3 seperate Class C's in a semi-random (oscillating) fashion. Probably had two or more instances of the scanning tool active to mask intended targets.

5. Research

Well-known scan type (BackOrifice port 31337)

6. Evaluation/Recommendation

Contacted university. Representative responded and informed us that the activity would cease.

Incident #8: SYN/FIN Scan on port 109

SH 2000/xx/xx 20:47:04 web.university.edu.109 > my.site.1.109 pop2 SF
SH 2000/xx/xx 20:47:04 web.university.edu.109 > my.site.2.109 pop2 SF
SH 2000/xx/xx 20:47:04 web.university.edu.109 > my.site.3.109 pop2 SF
SH 2000/xx/xx 20:47:04 web.university.edu.109 > my.site.4.109 pop2 SF
SH 2000/xx/xx 20:47:04 web.university.edu.109 > my.site.5.109 pop2 SF
SH 2000/xx/xx 20:47:04 web.university.edu.109 > my.site.7.109 pop2 SF
SH 2000/xx/xx 20:47:04 web.university.edu.109 > my.site.9.109 pop2 SF
SH 2000/xx/xx 20:47:04 web.university.edu.109 > my.site.8.109 pop2 SF
SH 2000/xx/xx 20:47:04 web.university.edu.109 > my.site.10.109 pop2 SF
SH 2000/xx/xx 20:47:04 web.university.edu.109 > my.site.11.109 pop2 SF
etc.... Class C

1. Origin

University. Possible spoofed packet.

2. Technique

Use SYN/FIN scan via nmap or another tool to probe port 109.

3. Intent

Probably looking for the booger trojan (port 109) or vulnerable pop2 hosts.

4. Active Targeting

No. Scanned entire Class C.

5. Research

Research via known Trojan port lists to find port 109 pop2 or the booger trojan. Open-source research demonstrated increased talk about trojan and may indicate renewed interest.

6. Evaluation/Recommendation

Contacted university and verified that our hosts did not have running pop2 services or Trojan. Recommended university check web server for possible misuse or intrusion.

Incident #9: Subseven Trojan

SH 2000/xx/xx 19:56:05 university.edu.2631 > my.site.1.1243 S
SH 2000/xx/xx 19:56:05 university.edu.2631 > my.site.115.1243 S

SH 2000/xx/xx 19:56:05 university.edu.2631 > my.site.5.1243 S
SH 2000/xx/xx 19:56:05 university.edu.2631 > my.site.120.1243 S
SH 2000/xx/xx 19:56:05 university.edu.2631 > my.site.9.1243 S
SH 2000/xx/xx 19:56:06 university.edu.2631 > my.site.111.1243 S
SH 2000/xx/xx 19:56:06 university.edu.2631 > my.site.8.1243 S
SH 2000/xx/xx 19:56:07 university.edu.2631 > my.site.190.1243 S
SH 2000/xx/xx 19:56:07 university.edu.2631 > my.site.10.1243 S
SH 2000/xx/xx 19:56:08 university.edu.2631 > my.site.121.1243 S
SH 2000/xx/xx 19:56:08 university.edu.2631 > my.site.15.1243 S

1. Origin

University

2. Technique

Send SYN packets to port 1243 in attempt to locate SubSeven Trojan.

3. Intent

Locate and exploit Subseven Trojan.

4. Active Targeting

No. Scanned 2 Class B address spaces in rapid succession. Also, low and then high addresses indicate two instances or more of the running scanner.

5. Research

Researched open-source traffic and found renewed discussion on the SubSeven Trojan scans around the Internet.

6. Evaluation/Recommendation

Contact university and check systems for return traffic. None found.

Incident #10: Quick ftp, and smtp port scan

BlackICE Defender (ClearICE Report Utility provided dump)

BI 20:44:42 192.168.1.1.0 > my.site.25 Count=2 SMTP SCAN
BI 20:44:42 192.168.1.1.0 > my.site.21 Count=2 FTP SCAN
BI 20:30:42 192.168.1.1.0 > my.site Count=4 WHATSUP SCAN

Short Analysis: Upon further investigation with a certain telco company that was supplying my DSL line, the individual was a problem scanner. Supposedly, BlackICE reports the scan first as a 4 count "WhatsUP" scan (WhatsUP is a commercial security scanner supposed to be used only on one's own machine ;)) and then divides the scan into sections: 2 count for the SMTP scan and 2 count for the FTP scan. Very interesting ability BlackICE has for sectionalizing the scanning components.

Andrew J Boncek