GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Intrusion Detection In-Depth (Security 503)"
at http://www.giac.org/registration/gcia

SNAP Certification Practical

10 Detects with analysis

Toby Miller
Counterpane Internet Security Inc.

22 March 2000

Grader: Jeff Stutzman
Grade: 87/ Pass
See comments in RED.

© SANS Institute 2000 - 2002 Author retains full rights.

Detect 1:

Mar 16 19:06:54.114 host1 kernel: 226 IP packet dropped (fsuj83.rz.uni-jena.de[XXX.XXX.XXX.XXX]->host1. [x.x.x.1]: Protocol=TCP[SYN] Port 49442->512): Restricted Port: Protocol=TCP[SYN] Port 49442->512 (received on interface x.x.x.1)

Mar 16 19:06:54.269 host1 ftpd[14378]: 121 Statistics: duration=0.05 id=7DBqm sent=63 rcvd=103 src=XXX.XXX.XXX.XXX/49441 proto=ftp (Authentication failed)

Mar 16 19:06:54.277 host1 httpd[14989]: 121 Statistics: duration=0.07 id=7DPkT sent=168 rcvd=402 srcif=le1 src=XXX.XXX.XXX.XXX/49443 srcname=fsuj83.rz.uni-jena.de dstif=le1 dst= x.x.x.1/80 dstname=host1. op=POST arg=/cgi-bin/perl result="403 Forbidden" proto=http (request denied by process)

Mar 16 19:06:54.288 host1 httpd[14989]: 121 Statistics: duration=0.07 id=7DPkU sent=147 rcvd=402 srcif=le1 src=XXX.XXX.XXX.XXX/49444 srcname=fsuj83.rz.uni-jena.de dstif=le1 dst= x.x.x.1/80 dstname=host1. op=POST arg=/cgi-bin/phf?Qname=x%0a/bin/sh+-s%0a result="403 Forbidden" proto=http (request denied by process)

Mar 16 19:06:54.295 host1 httpd[14989]: 121 Statistics: duration=0.07 id=7DPkW sent=95 rcvd=402 srcif=le1 src=XXX.XXX.XXX.XXX/49445 srcname=fsuj83.rz.uni-jena.de dstif=le1 dst= x.x.x.1/80 dstname=host1. op=GET arg=/cgi-bin/aglimpse/80|IFS=_;CMD =_echo\\;echo_id-aglimpse\\;uname_-a\\;id;eval$CMD; result="403 Forbidden"

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

proto=http (request denied by process)

Mar 16 19:06:54.300 host1 httpd[14989]: 121 Statistics: duration=0.08 id=7DPkX sent=57 rcvd=402 srcif=le1 src=XXX.XXX.XXX.XXX/49446 srcname=fsuj83.rz.uni-jena.de dstif=le1 dst= x.x.x.1/80 dstname=host1. op=GET arg=/cgi-bin/view-source?cgi-bin/view-source result="403 Forbidden" proto=http (request denied by process)

Mar 16 19:06:54.305 host1 httpd[14989]: 121 Statistics: duration=0.08 id=7DPkY sent=73 rcvd=402 srcif=le1 src=XXX.XXX.XXX.XXX/49447 srcname=fsuj83.rz.uni-jena.de dstif=le1 dst= x.x.x.1/80 dstname=host1. op=POST arg=/cgi-bin/nph-test-cgi result="403 Forbidden" proto=http (request denied by process)

Mar 16 19:06:54.310 host1 httpd[14989]: 121 Statistics: duration=0.08 id=7DPkZ sent=69 rcvd=402 srcif=le1 src=XXX.XXX.XXX.XXX/49448 srcname=fsuj83.rz.uni-jena.de dstif=le1 dst= x.x.x.1/80 dstname=host1. op=POST arg=/cgi-bin/test-cgi result="403 Forbidden" proto=http (request denied by process)

Mar 16 19:06:54.107 host2 kernel: 226 IP packet dropped (fsuj83.rz.uni-jena.de[XXX.XXX.XXX.XXX]->host2[x.x.x.1]: Protocol=TCP[SYN] Port 49450->512): Restricted Port: Protocol=TCP[SYN] Port 49450->512 (received on interface x.x.x.1)

Mar 16 19:06:54.255 host2 ftpd[16398]: 121 Statistics: duration=0.06 id=9eNKb sent=63 rcvd=103 src=XXX.XXX.XXX.XXX/49449 proto=ftp (Authentication failed)

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Mar 16 19:06:54.263 host2 httpd[16394]: 121 Statistics: duration=0.06 id=9f5SW sent=168 rcvd=402 srcif=le1 src=XXX.XXX.XXX.XXX/49451 srcname=fsuj83.rz.uni-jena.de dstif=le1 dst= x.x.x.1/80 dstname=host2. op=POST arg=/cgi-bin/perl result="403 Forbidden" proto=http (request denied by process)

Mar 16 19:06:54.271 host2 httpd[16394]: 121 Statistics: duration=0.07 id=9f5SX sent=147 rcvd=402 srcif=le1 src=XXX.XXX.XXX.XXX/49452 srcname=fsuj83.rz.uni-jena.de dstif=le1 dst= x.x.x.1/80 dstname=host2. op=POST arg=/cgi-bin/phf?Qname=x%0a/bin/sh+-s%0a result="403 Forbidden" proto=http (request denied by process)

Mar 16 19:06:54.275 host2 httpd[16394]: 121 Statistics: duration=0.07 id=9f5SY sent=95 rcvd=402 srcif=le1 src=XXX.XXX.XXX.XXX/49453 srcname=fsuj83.rz.uni-jena.de dstif=le1 dst= x.x.x.1/80 dstname=host2. op=GET arg=/cgi-bin/aglimpse/80|IFS=_;CMD =_echo\\;echo_id-aglimpse\\;uname_-a\\;id;eval$CMD; result="403 Forbidden" proto=http (request denied by process)

Mar 16 19:06:54.280 host2 httpd[16394]: 121 Statistics: duration=0.07 id=9f5SZ sent=57 rcvd=402 srcif=le1 src=XXX.XXX.XXX.XXX/49454 srcname=fsuj83.rz.uni-jena.de dstif=le1 dst= x.x.x.1/80 dstname=host2. op=GET arg=/cgi-bin/view-source?cgi-bin/view-source result="403 Forbidden" proto=http (request denied by process)

Mar 16 19:06:54.285 host2 httpd[16394]: 121 Statistics: duration=0.07 id=9f5T0 sent=73 rcvd=402 srcif=le1 src=XXX.XXX.XXX.XXX/49455

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

srcname=fsuj83.rz.uni-jena.de dstif=le1 dst= x.x.x.1/80 dstname=host2. op=POST arg=/cgi-bin/nph-test-cgi result="403 Forbidden" proto=http (request denied by process)

Mar 16 19:06:54.289 host2 httpd[16394]: 121 Statistics: duration=0.07 id=9f5T1 sent=69 rcvd=402 srcif=le1 src=XXX.XXX.XXX.XXX/49456 srcname=fsuj83.rz.uni-jena.de dstif=le1 dst= x.x.x.1/80 dstname=host2. op=POST arg=/cgi-bin/test-cgi result="403 Forbidden" proto=http (request denied by process)

Analysis 1:

These packets suggest the following information:

- Appears to be automated.
- Source Ports are high.
- Attempted to connect using port 512/tcp (exec).
- Most attacks were common CGI-BIN attacks.
- De is the country code for Germany. From this information we can figure out what time zone the attack originated from and possibly the thought process behind the attack. Agree, but does this mean .de was actually the origin? -2

© SANS Institute 2000 - 2002, Author retains full rights.

Detect 2:

Mar 13 23:40:01.771369 209.166.41.8,53 -> 10.0.1.1,111 PR tcp len 20 40 -S

Mar 13 23:41:10.128107 209.166.41.8,53 -> 10.0.2.1,111 PR tcp len 20 40 -S

Mar 13 23:42:03.888377 209.166.41.8,53 -> 10.0.3.1,111 PR tcp len 20 40 -S

Mar 14 04:12:06.818904 209.166.41.8,53 -> 10.0.1.2,111 PR tcp len 20 40 -S

Mar 14 04:13:13.846747 209.166.41.8,53 -> 10.0.2.2,111 PR tcp len 20 40 -S

Mar 14 04:14:07.132362 209.166.41.8,53 -> 10.0.3.2,111 PR tcp len 20 40 -S

Mar 14 08:28:23.719263 209.166.41.8,53 -> 10.0.0.3,111 PR tcp len 20 40 -S

Mar 14 08:29:30.881752 209.166.41.8,53 -> 10.0.1.3,111 PR tcp len 20 40 -S

Mar 14 08:30:25.284416 209.166.41.8,53 -> 10.0.2.3,111 PR tcp len 20 40 -S

Mar 14 08:31:18.807869 209.166.41.8,53 -> 10.0.3.3,111 PR tcp len 20 40 -S

Mar 14 12:55:31.960881 209.166.41.8,53 -> 10.0.0.4,111 PR tcp len 20 40 -S

Mar 14 12:56:39.329164 209.166.41.8,53 -> 10.0.1.4,111 PR tcp len 20 40 -S

Mar 14 12:57:33.761394 209.166.41.8,53 -> 10.0.2.4,111 PR tcp len 20 40 -S

Mar 14 12:58:40.860329 209.166.41.8,53 -> 10.0.3.4,111 PR tcp len 20 40 -S

Analysis 2:

These packets suggest the following information:

- This is a Host Scan.
- All packets had a source port of 53 (DNS).
- Normal traffic rarely uses port 53 as a source port unless the source is a DNS server.
- Slow Scan. The attacker sent one packet per machine over a 13 hour time period. This method is used to hide packets. This is actually a 'Stealth Scan', or half-open scan. Your analysis is correct that the slow scanning is a method for hiding the packets. **-5**
- Searching for RPC vulnerabilities on various hosts. No mention of destination port 111. This guy is actually looking for vulnerabilities in SunRPC/Portmapper. A wide RPC vulnerability scan might have taken into account any number of ports. **-5**

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Detect 3: Good.

Mar 7 16:05:02.985 firewall kernel: 232 Sending ICMP port unreachable.

Original packet (206.251.19.88->firewall.mydomain.edu[10.0.0.1]:

Protocol=UDP Port 2814->33434) received on interface 10.0.0.1

(probable traceroute as ttl=1)

Mar 7 16:10:30.271 firewall kernel: 232 Sending ICMP port unreachable.

Original packet (167.8.29.52->firewall.mydomain.edu[10.0.0.1]:

Protocol=UDP Port 2711->33434) received on interface 10.0.0.1

(probable traceroute as ttl=1)

Analysis 3: Good.

These packets suggest the following information:

- Using trace route port 33434.
- TTL = 1. This can indicate that intelligence gathering might have been done. For more information see http://packetstorm.securify.com/UNIX/audit/firewalk/firewalk-final.html.
- Trace route packets were sent by two different IP addresses 5 minutes apart.
- The firewall does not allow trace routes into its network.

© SANS Institute 2000 - 2002, Author retains full rights.

Detect 4:

Mar 11 23:44:16 morton kernel: Packet log: input DENY eth0 PROTO=6

205.229.221.1:4183 63.224.27.201:53 L=60 S=0x00 I=40348 F=0x4000 T=49 SYN (#64)

Mar 11 23:44:17 www kernel: Packet log: input DENY eth0 PROTO=6

205.229.221.1:4187 63.224.27.205:53 L=60 S=0x00 I=40388 F=0x4000 T=49 SYN (#51)

Mar 11 23:44:26 www kernel: Packet log: input DENY eth0 PROTO=6

205.229.221.1:4187 63.224.27.205:53 L=60 S=0x00 I=40656 F=0x4000 T=49 SYN (#51)

Analysis 4:

These packets suggest the following information:

- Automated Host Scan. Scanned two hosts 63.224.27.201.3 | 63.224.27.201.205.
- Possible DNS Zone Transfer. This might also be simple host ID efforts. **-1**
- Scanning for 53/tcp (DNS).

© SANS Institute 2000 - 2002, Author retains full rights.

Detect 5:

Mar 6 10:46:34 ardvark kernel: Packet log: input DENY eth0 PROTO=6

64.24.22.102:4974 209.46.114.11:143 L=60 S=0x00 I=18800 F=0x4000 T=48 SYN (#54)

Mar 6 10:46:37 ardvark kernel: Packet log: input DENY eth0 PROTO=6

64.24.22.102:4974 209.46.114.11:143 L=60 S=0x00 I=19166 F=0x4000 T=48 SYN (#54)

Mar 6 10:46:42 ardvark kernel: Packet log: input DENY eth0 PROTO=6

64.24.22.102:4974 209.46.114.11:143 L=60 S=0x00 I=19768 F=0x4000 T=48 SYN (#54)

Analysis 5: Good.

These packets suggest the following information:

- IMAP scan. 143/TCP (IMAP).
- Probably automated. Source ports stay consistent throughout the scan.

© SANS Institute 2000 - 2002, Author retains full rights.

Detect 6:

Mar 11 18:24:56 morton kernel: Packet log: input DENY eth0 PROTO=6

194.87.6.47:3529 63.224.27.201:3128 L=48 S=0x00 I=30462 F=0x0000 T=45 SYN (#64)

Mar 11 19:42:56 morton kernel: Packet log: input DENY eth0 PROTO=6

194.87.6.47:3645 63.224.27.201:3128 L=48 S=0x00 I=54327 F=0x0000 T=45 SYN (#64)

Analysis 6: Good.

These packets suggest the following information:

- Ring Zero (Port 3128|Squid Proxy).
- This type of scanning began the following September. SANS released information about this in October. Ports 8080 and 1080 were also being scanned.

© SANS Institute 2000 - 2002, Author retains full rights.

Detect 7:

Mar 8 00:42:37 library portsentry[8852]: attackalert: Unknown Type: Packet Flags: SYN: 1 FIN: 1 ACK: 0 PSH: 0 URG: 0 RST: 0 from host: 192.168.0.2/192.168.0.2 to TCP port: 109

Analysis 7: Good.

These packets suggest the following information:

- Probing port 109 (POP2).
- This scan used a SYN|FIN combination. This combination is not normal according to RFC 793.
- This type of traffic is normally used to sneak by IDS systems and some Firewalls.
- This combination could also be used in OS Fingerprinting. An older version of Linux used to reply to SYN|FIN combinations with SYN|FIN|ACK.

© SANS Institute 2000 - 2002 Author retains full rights.

Detect 8:

01 Mar 00 07:29:58 udp 64.32.14.98.137 ->

10.16.98.215.137 2 0 116 0 TIM

01 Mar 00 07:30:07 udp 64.32.14.98.137 ->

10.16.98.216.137 2 0 116 0 TIM

01 Mar 00 07:30:13 udp 64.32.14.98.137 ->

10.16.98.217.137 3 0 174 0 TIM

Analysis 8: Good.

These packets suggest the following information:

- Packets use port 137/udp (NetBios).
- Very well could be normal traffic.
- NetBios is used mainly in a Windows enviroment.
- Because of the information it gives out NetBios traffic should be blocked at the router level or Firewall level.

© SANS Institute 2000 - 2002, Author retains full rights.

Detect 9:

Feb 29 12:29:49 host1 portsentry[524]: attackalert:

Connect from host: 206.49.154.100/206.49.154.100 to UDP port: 31337

Feb 29 12:29:49 host1 portsentry[524]: attackalert:

Connect from host: 206.49.154.100/206.49.154.100 to UDP port: 31337

Feb 29 12:29:49 host2 portsentry[420]: attackalert:

Connect from host: 206.49.154.100/206.49.154.100 to UDP port: 31337

Feb 29 12:32:40 host3 portsentry[16512]: attackalert:

Connect from host: 206.49.154.100/206.49.154.100 to UDP port: 31337

Analysis 9:

These packets suggest the following information:

- Trying to use UDP port 31337 to communicate.
- 31337/udp is most commonly associated with Back Orifice. Correct.
- After discovering such a probe one should inspect servers and clients for BO and other Trojans that might have been installed after BO was installed.

© SANS Institute 2000 - 2002, Author retains full rights.

Detect 10:

Mar 7 22:48:40 www kernel: Packet log: input DENY eth0 PROTO=6

207.175.252.210:1527 63.224.27.205:1243 L=48 S=0x00 I=23649 F=0x4000 T=111 SYN

Mar 7 22:48:40 morton kernel: Packet log: input DENY eth0 PROTO=6

207.175.252.210:1523 63.224.27.201:1243 L=48 S=0x00 I=22625 F=0x4000 T=113 SYN

Mar 7 22:48:40 pooky kernel: Packet log: input DENY eth0 PROTO=6

207.175.252.210:1526 63.224.27.204:1243 L=48 S=0x00 I=23393 F=0x4000 T=111

Mar 4 06:12:06 morton kernel: Packet log: input DENY eth0 PROTO=6

207.175.252.210:2264 63.224.27.201:1243 L=48 S=0x00 I=19830 F=0x4000 T=113 SYN

Mar 4 06:12:06 pooky kernel: Packet log: input DENY eth0 PROTO=6

207.175.252.210:2267 63.224.27.204:1243 L=48 S=0x00 I=20598 F=0x4000 T=111

Mar 4 06:12:06 www kernel: Packet log: input DENY eth0 PROTO=6

207.175.252.210:2268 63.224.27.205:1243 L=48 S=0x00 I=20854 F=0x4000 T=111 SYN

Mar 2 05:25:43 morton kernel: Packet log: input DENY eth0 PROTO=6

207.175.252.210:3836 63.224.27.201:1243 L=48 S=0x00 I=16548 F=0x4000 T=113 SYN

Mar 2 05:25:43 www kernel: Packet log: input DENY eth0 PROTO=6

207.175.252.210:3840 63.224.27.205:1243 L=48 S=0x00 I=17572 F=0x4000 T=111 SYN

Mar 2 05:25:43 pooky kernel: Packet log: input DENY eth0 PROTO=6

207.175.252.210:3839 63.224.27.204:1243 L=48 S=0x00 I=17316 F=0x4000 T=111

Analysis 10:

These packets suggest the following information:

- Host Scan.
- Looking for TCP port 1243. This port is associated with the BackDoor-G and SubSeven Trojan. Good.
- Slow scan. Scanned over a five-day period. Most likely trying to hide the packets.
- Scanned either in the early morning or late at night. Again hoping not to be detected.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Last Updated: October 24th, 2017

Upcoming Training

SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 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 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
Las Vegas 2018 - SEC503: Intrusion Detection In-Depth	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	vLive
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	McLean, 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 vLive - SEC503: Intrusion Detection In-Depth	SEC503 - 201805,	May 02, 2018 - Jun 07, 2018	vLive
SANS Security West 2018	San Diego, CA	May 11, 2018 - May 18, 2018	Live Event
Community SANS Columbia SEC503	Columbia, MD	Aug 13, 2018 - Aug 18, 2018	Community SANS
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced