



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 permitted 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>

Intruder IP: 216.68.15.73
Intruder Name: as1-216-68-15-73.fuse.net
Port Parameters: port=**27374**&name=Sub_7_2
Attack Count: 1
Victim IP: 10.197.41.60

Profile 3

History: Detects from GIAC Web Site

Evidence of Targeting: Yes

Technique: Can be initiated for any workstation with a browser

Intent: Attempted system access

Severity Level: High - test-cgi & aglimpse are programs with known vulnerabilities in the "dynamic content generation" portion of the web server

Trace Extract

CGI Attack - TCP destination port 80/http - notice "POST /cgi-bin/test-cgi"

```
22:00:08.952175 128.175.13.74.53558 > 10.0.0.9.80:  
P 1677621322:1677621391(69) ack 2335601879 win 8760 (DF)  
(ttl 242, id 12223)  
0000: 4500 006d 2fbf 4000 f206 0465 80af 0d4a E..m/..@....e...J  
0010: 0a00 0009 d136 0050 63fe 784a 8b36 74d7 .d...6.Pc.xJ.6t.  
0020: 5018 2238 4af8 0000 504f 5354 202f 6367 P."8J...POST /cg  
0030: 692d 6269 6e2f 7465 7374 2d63 6769 2048 i-bin/test-cgi H  
0040: 5454 502f 312e 300a 436f 6e74 656e 742d TTP/1.0.Content-  
0050: 7479 7065 3a20 2a0a 436f 6e74 656e 742d type: *.Content-  
0060: 6c65 6e67 7468 3a20 300a 0a00 19 length: 0....
```

CGI Attack - TCP destination port 80/http - notice "GET /cgi-bin/aglimpse/80 | IFS"

```
01:14:18.042722 128.175.13.74.42930 > 10.0.0.9.80:  
P 3053993825:3053993920(95) ack 2009011357 win 8760 (DF)  
(ttl 242, id 57632)  
0000: 4500 0087 e120 4000 f206 52e9 80af 0d4a E.... @...R....J  
0010: 0a00 0009 a7b2 0050 b608 3f61 77bf 149d .d.....P..?aw...  
0020: 5018 2238 8704 0000 4745 5420 2f63 6769 P."8....GET /cgi  
0030: 2d62 696e 2f61 676c 696d 7073 652f 3830 -bin/aglimpse/80
```

0040: 7c49 4653 3d5f 3b43 4d44 3d5f 6563 686f |IFS=_;CMD=_echo
0050: 5c3b 6563 686f 5f69 642d 6167 6c69 6d70 \;echo_id-aglimp
0060: 7365 5c3b 756e 616d 655f 2d61 5c3b 6964 se\;uname_-a\;id
0070: 3b65 7661 6c24 434d 443b 2048 5454 502f ;eval\$CMD; HTTP/
0080: 312e 300a 0a00 20 1.0...

Profile 4

History: Detects from GIAC Web Site

Evidence of Targeting: Yes

Technique: Can be initiated from SNMPget (bundled with Linux) or SNMPWalk <http://herbie.aazk.org/snmp>

Intent: Attempted system access through SNMP logon

Severity Level: High - The default SNMP passwords (public and private) are well known by the hacker community. Since access is not restricted as to who can query a server using SNMP, it would be trivial for anyone with access to the network to gather information via SNMP. For example, among the information accessible via SNMP is a list of all the valid usernames on the server, as well as, information regarding the system architecture.

Trace Extract

SNMP Logon - UDP destination port 161/SNMP - notice SMNP "public" string

```
03/17-11:21:19.519401 0:E0:D0:10:EF:7F -> 0:C0:F0:37:D6:51 type:0x800 len:0x67 63.24.141.4:1077 ->
63.224.27.201:161 UDP TTL:116 TOS:0x0 ID:42880 Len: 69
0000: 30 3B 02 01 00 04 06 70 75 62 6C 69 63 A0 2E 02 0;.....public...
0010: 01 01 02 01 00 02 01 00 30 23 30 11 06 0D 2B 06 .....0#0...+.
0020: 01 04 01 0B 02 04 03 08 03 02 00 05 00 30 0E 06 .....0..
0030: 0A 2B 06 01 02 01 02 02 01 06 01 05 00 .+.....
```

Profile 5

History: Detects from GIAC Web Site

Evidence of Targeting: Yes

Technique: SYN/FIN Scan - Crafted Packets abnormal stimulus, notice source port 0 and SYN/FIN segment flags

Intent: Network mapping

Severity Level: Low - recon

Trace Extract

SYN/FIN Scan - TCP destination port 109/POP2 - notice source port 0 and SYN/FIN flag set
Mar 4 17:30:28.902226 128.16.160.1,0 -> 10.0.1.1,109 PR tcp len 20 40 -SF

Profile 6

History: Detects from GIAC Web Site

Evidence of Targeting: Yes

Technique: Trojan Probe

Intent: NetBus "Windows remote administration tool" <http://www.netbus.org/>

Severity Level: Low - recon

Norton AntiVirus will detect NetBus, to download definition <http://www.symantec.com/avcenter/download.html>

Trace Extract

Trojan Scan - TCP destination port 12346/NetBus

Mar 4 11:34:31.616656 24.92.141.130,1371 -> 10.0.1.40,12346 PR tcp len 20 48 -S

Trojan Scan - TCP destination port 12345/NetBus

Feb 12 15:49:20 morton kernel: Packet log: input DENY eth0 PROTO=6 62.157.49.25:12345 :12345 L=40 S=0x00
I=39426 F=0x0000 T=18 SYN (#66)

Profile 7

History: Detects from GIAC Web Site

Evidence of Targeting: Yes

Technique: Trojan Probe

Intent: Back Orifice "Windows remote administration tool" <http://www.bo2k.com/>

Severity Level: Low - Recon

Norton AntiVirus detect Back Orifice, to download definition <http://www.symantec.com/avcenter/download.html>

Trace Extract

Trojan Scan - UDP destination port 31337/back orifice-default port
[**] IDS188/probe-back-orifice [**]
02/13-03:52:42.176130 24.130.49.191:7430 -> 172.16.1.239:31337
UDP TTL:119 TOS:0x0 ID:16631 Len: 26

Profile 8

History: Detects from GIAC Web Site
Evidence of Targeting: Yes
Technique: Port Scan
Intent: Network mapping
Severity Level: Low - Recon

Trace Extract

Port Scan - TCP destination port 8081
Feb 14 10:54:37 morton kernel: Packet log: input DENY eth0 **PROTO=6** 210.55.10.59:4047 63.224.27.201:**8081**
L=64 S=0xD4 I=46690 F=0x4000 T=50 SYN(#66)

This trace I pulled from the GIAC Web Site, and essentially disagree with the analysis. The posted analysis indicates that the Netscape proxy server administration port can be form on TCP port 8081.

The Netscape proxy server uses two port numbers: one for the proxy server itself and another for the administration server. There are no standard port numbers for proxy servers; however, the default proxy server port is TCP/8080. The administration server is typically run on a random port number above 1024. This makes it harder for unauthorized users to determine where your administration server is. The port number for the administration server must be specified during installation. However, it is possible that the admin port could be assigned to TCP/8081.

For more information about Netscape proxy server <http://developer.netscape.com/docs/manuals/proxy>

Profile 9

History: Detects from GIAC Web Site

Evidence of Targeting: Yes

Technique: Trojan Connection

Intent: DeepThroat 3.1 "Windows remote administration tool" <http://www.sohons.com/deept/index2.html>

Severity Level: High - DeepThroat client sending data

DeepThroat listens on: 6670/tcp, 3150/tcp, 2140/tcp, **2140/udp**, 3150/udp.

When scanning for servers, the client will use **source port of 60000** and scan for ports like **2140**.

Norton AntiVirus will detect DeepThroat, to download definition

<http://www.symantec.com/avcenter/download.html>

Trace Extract

Trojan Connection - UDP destination port 2140/DeepThroat

Apr 1 06:29:18 dns2 snort[5950]:

BACKDOOR SIGNATURE -- DeepThroat 3.1 Client Sending Data to Server on Network: 62.125.10.102:**60000** ->

X.Y.Z.66:**2140** -----

[**] BACKDOOR SIGNATURE -- DeepThroat 3.1 Client Sending Data to Server on Network [**]

04/01-06:29:18.696739 62.125.10.102:**60000** -> X.Y.Z.66:**2140** **UDP** TTL:113 TOS:0x0 ID:61950 Len: 10 30 30 00 00

EF 30 8A 06 00 48 68 5E 50 10 44 70 00...0...Hh^P.Dp 00 A7 .. -----

Profile 10

History: BlackICE Defender identified this trace as a possible attack

Evidence of Targeting: Yes

Technique: Windows NT domain structure communications

Intent: SNMP GET command sent to broadcast address

Severity Level: Low - Recon

Trace shows a newly installed Windows NT system attempting to become the backup browser, interesting that Windows uses a **SNMP Get command** sent to a broadcast address as the initial stimulus.

The Windows NT browser service maintains a list of each computer in the domain, and the protocol being used on the network being served by the computer running the browser service. In the Windows NT domain structure, the primary domain controller (PDC) is always selected as the domain master browser. Only the PDC can be a domain master browser. Additionally, one backup browser is allocated for every 32 computers

on the network segment. The backup browser on a given network segment provides a browse list to the client computers located in the same segment.

Trace Extract

SNMP Get - broadcast address

```
264 131.537001  "New WKS IP"      x.x.x.255          BROWSER Host Announcement "New WKS NetBIOS
Name", Workstation, Server, NT Workstation, Potential Browser
791 285.829000  "New WKS IP"      255.255.255.255   SNMP GET
794 286.050000  "Target MAC"     ff:ff:ff:ff:ff:ff  ARP   Who has "New WKS IP?" Tell "Host IP"
795 286.124000  "New WKS MAC"    "Host MAC"        ARP   "New WKS IP" is at "Host MAC"
796 286.124000  "Host IP"        "New WKS IP"      NBNS Name query NBSTAT
*<00><00><00><00><00><00><00><00><00><00><00><00><00><00><00><00>
797 286.124000  "New WKS IP"    "Host IP"         NBNS  Name query response NBSTAT
```

Upcoming Training

Click Here to
{Get CERTIFIED!}



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
Baltimore Fall 2017 - SEC503: Intrusion Detection In-Depth	Baltimore, MD	Sep 25, 2017 - Sep 30, 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
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