Global Information Assurance Certification Paper

Network Intrusion and Reconnaissance Detection Analysis

Abstract

This paper presents a series of intrusion and/or reconnaissance attempts made against a registered domain and their correlated analysis. Additionally, I have included suggestions to safeguard against the attempt succeeding, where appropriate. Most of the intrusion/reconnaissance attempts are well known, but I have tried to select unique or unusual examples where possible.

1. Introduction

A demonstration of Practical Analysis Skills, put forth as required by GIAC for consideration for certification as a GIAC Certified Intrusion Detection Analyst.

2. Methodology

Most detects have been culled from a combination of: Dragon-Fire 2.1, Snort v1.6, BlackIce and system logs. Shadow was deployed, but was never effective due to numerous, persistent tcpdump filter problems. Log file, alert and other "raw" data has been provided in an appendix following the main document to improve readability. Hyperlinks have been put inline for rapid access to the raw data.

Severity results were calculated by assigning a value between one and five, with one being the lowest score and five the highest, to four objects. The objects are: Criticality of Machine, Lethality of attack, System countermeasures and Network countermeasures. The formula for calculating this is (Criticality + Lethality) - (System + Network). The total can be any number from eight (can be compromised by a six year old with an Atari) to negative eight (totally secure), with most attacks falling in the zero to three range.

Detects were obtained from a purpose built network containing three separate target machines, a SPARC running Solaris 8 beta, a Celeron running OpenBSD and a Pentium II running Windows NT SP4. The network was built and administered by myself and Todd Garrision, who is also a candidate for GCIA Certification.

Unfortunately for the purposes of this paper, approximately 95%+ of the detects on this network were of four types: mscan, NMap, SMB Wildcard and WinGate, run with the out-of-box default options, so pickings were a bit slim.

3. Results

Detect 1

Detect 1 Data

Generated by: Snort

Source IP spoof probability: Minimal

Description: Outbound traffic on ports known to be used by Trojan programs

Mechanism: This looks like a series of attacks coming from a Name Server. Since the attacks are staggered, with varying times and days between attacks, at first glance it looks like the server has been compromised and someone is going "low and slow". On further analysis, it is apparent that

these are spurious detects caused by Snort's tendency to only see the NSLOOKUP reply traffic. Coupling that with the fact that requests are made on ephemeral ports that by happenstance meet known ports used by attacks and trojans causes the alarms. Correlation to this is provided by the fact that examination of the Dragon-Fire logs for the same times and source addresses do not show any suspicious activity, as well the local syslog does not show any aberrations during any of the times of the attacks.

Correlations: Although I was unable to find anything on the WWW, it would seem to be reasonable that similar false alarms have occurred in the past.

Active Targeting: False Alarm

Severity: None/False

Defense: Study pattern of apparent attacks and be aware of known false alarm tendencies in local IDS configuration(s).

Test Question:

What are some of the known limitations of the Snort host based IDS?

A) It can send a false alarm when it mis-reads the IP header

B) There is no way to get detailed data from the log, only the Snort abstract

C) If you filter by inside source port, it can send a false alarm

D) It only works to detect truffles if you're in the forest

Answer: C

Detect 2

Detect 2 Data

Generated by: Snort and Dragon-Fire

Source IP spoof probability: Slight, IP is valid with Erol's Internet Service, used as a dial-up POP

Description: Attempt to query or browse SNMP information

Mechanism: This is a fairly obvious attempt to access the "public" SNMP community on the network. From looking at the timestamp data, it appears that this is a scripted attack. Weight is lent to this by the IP sequence numbers and the common source port of 1029. What makes this unusual, is that it seems to be a new script trying to exploit a vulnerability in Solaris 7/8 whereby the SNMP subagent has a default community string/password that allows code to be executed as root. Fortunately (or unfortunately as the case may be) the target for this attack had already been taken off the net by a brute force buffer overflow attack and therefore was not available to be compromised.

Correlation: Anzen/NFR describes several different flavors, as well BugTraq, SecurityFocus, et. al

Active Targeting: Targeting the Windows host on the network

CVE: CAN-1999-0186, CAN-1999-0516, CAN-1999-0517

Severity: (2+5) - (3+2) = 2

Defense: Port 161 should be closed at the border routers, also, community name string needs to be changed to something non-obvious (i.e.: not "private", "internal", your company/division name, etc.) and passworded for both read-only and read/write access. You should also check for SNMP "subagents" and verify that they have updated themselves with the settings from the "master" SNMP service. The latest patches from Sun should also be obtained and installed after compatibility testing.

Test Question:

How do you ensure that any changes you have made to community name string and passwords have been accepted by the SNMP service?

A) Reboot the device

B) Send a "killall -9 *" from the command console

C) Run an SNMP attack such as snmpwalk or snmpinfo against your network

D) From a different machine, test SNMP connectivity with the old and new community name and password

Answer: D

Detect 3

Detect 3 Data

Generated by: Snort

Source IP spoof probability: Moderate, IP is used by BellSouth as part of a block of gateway IP's

Description: A standard mscan

Mechanism: It appears to be more oriented towards UNIX than Windows, despite the fact that the Windows machine was the targeted device. The entire sequence took place within a little less than a one minute, twenty second time period. There was only one other "burst" of activity, some four hours later, showing the exact same pattern, targeting the same machine. All attacks originated from three ports in the first scan - 49562, 49572, 49574 and again three ports for the second series - 34861,34871 34873. The pattern of 62, 72, 74/61, 71, 73 also leads me to suspect mscan again, with mscan using some sort of random number to chose the first three digits of the source port. It is probable that Snort was being a bit misleading again, and that this was a "pure" port scan and the access attempts are a false positive caused by the simple presence of activity on the target ports.

It seems likely that this is a "script-kiddie" attack, perhaps run by someone who does not know how

to determine the OS of the host he or she is trying to "attack" or set mscan options from the command line. The only other activity seen from this source was a few SMB queries from them accessing the web page hosted on this machine. Other than the web page data, nothing was transferred.

Correlation: Best description comes from the JANET site: http://www.ja.net/CERT/JANET-CERT/mscan.html

Active Targeting: Directed towards the Solaris host

Severity: (2+3) - (3+2) = 0

Defense: Other than double checking the target machine for any potential compromise, this would go in my "Keep an eye on" file. Nothing to panic over unless I start seeing more activity from this address range in either direction.

Test Question:

What is the default pattern for an mscan trace?

A) The next source port is always the square root of the previous port

B) It patterns in a series of three, decrementing the last number by one for each subsequent series

C) It patterns in a series of three, decrementing the first three numbers by one and reversing the second two numbers for each subsequent series

D) All of the destination ports are the same each time it is run

Answer: B

Detect 4

Detect 4 Data

Generated by: syslog

Source IP spoof probability: Unknown

Description: Buffer overflow attack against rpc.cmsd

Mechanism: This is a perfect example of one of the "Top Ten" on the Critical List. The attacker kept up the flood for eighty-eight hours straight, averaging one overflow failure on the target machine every one and a half to two minutes. Access was gained at least once, resulting in the attacker apparently restarting the inetd service several times. Eventually the attacker was wholly successful and root access was obtained. The compromiser tried to launch a telnet session back to his own machine, but fortunately one of the things that our firewall did block was all outbound traffic from the target machines back to the ISP network. Although the forensics have not been done yet, I am presuming that the attacker got frustrated and did something to the rc or inet files as the machine now boots, but crashes again after about ten minutes of operation.

Correlation: SANS Top Ten List, http://www.cert.org/advisories/CA-99-08-cmsd.html

Active Targeting: Directed towards the Solaris host

CVE: CVE-1999-0696

*Severity: (2+5) - (3+2) = 2 * This is a bit deceiving, although the machine was not a critical device, the compromise was complete and destructive. The only saving grace is that we had anticipated that some machines might be compromised and so had blocked access getting back out. If this machine were a critical infrastructure component, the damage would be much worse.*

Defense: The latest patches are a must! Also, if you work in an environment with developers, be aware that they have a tendency to run beta code for core server/workstation functions. As well, ports like the calendar port, daytime, etc. should be blocked from passing through the firewall.

Test Question:

How can you tell that this is an attack, rather than a bad installation or corrupted file?

A) There is no easy way to tell, only looking at syslogs and file modified dates can help

B) You can only tell by looking at the tcpdump files for the suspected day and time

C) If you look under the pot of gold at the end of the rainbow, it will tell you

D) A combination of IDS logs and syslogs have to be audited before this can be determined

Answer: A

Detect 5

Detect 5 Data

Generated by: Dragon-Fire

Source IP spoof probability: Unknown, no other IDS detected this

Description: Web server attack, trying to get all environment variables

Mechanism: This one's perhaps a bit unique, for one, it attempts to exploit the SAMBAR web server (which is not exactly the world's most well-known), also, it specifically targets the beta release which had a nasty vulnerability. If you could access it's admin page, and you knew the default username (the password was blank), then you could cause run code with the default system privileges of the web server. The intrepid intruder in this case, must not have realized that although we were indeed running the SAMBAR server, it was not the beta version and did not have this particular vulnerability. The source address had performed a few other scans, mostly mscan and nmap, but other than a single attempt at the SAMBAR vulnerability, and another at an IIS vulnerability, no other traffic was noted.

Not discounting the fact that system access was attempted, this is another for my "Keep an eye on" file. I would be tempted to dismiss this as a curiosity look see, so long as no other activity is seen.

Correlation: http://www.sambar.com/syshelp/security.htm

Active Targeting: This was aimed directly at the SAMBAR server

Severity: (2+5) - (5+2) = 0

Defense: As always, keeping up to date with revision and patch levels. Not running beta software is another. Redirecting admin pages to odd ports and restricting access to specific IP addresses will increase the security. Disabling remote admin is another possibility, however, may not always be feasible depending on the network architecture.

Test Question:

What are some of the more common web served files that an attacker will try to access?

A) CGI and Perl files

B) Windows executables

C) /etc/passwd on UNIX and WINNT\System32*.SAM on Windows

D) Users home directories

Answer: A

Detect 6

Detect 6 Data

Generated by: Snort

Source IP spoof probability: High, this range is registered to Jiangsu Transworld JIBIC Information Co. in China

Description: Sends odd packet fragments to the machine, attemping to fill the buffer

Mechanism: It was kind of unusual to catch this particular DoS attack. The vulnerability is an old one, first introduced in the Linux kernel 2.1 development series, and corrected by 2.4. The attacker sends a series of packet fragments with the offset and fragment ID set to zero, this causes the kernel to store them in the fragment queue. The queue had bad clean-up code and would not drop any fragments until they had completed. Once the queue fills, the network stack halts and the system is off the net.

The reason this is so odd, is that to be vulnerable, you would have to still be running a 2.1 development kernel or an early 2.2 release. Since none of the vulnerable kernels were ever part of a Linux distro's published release, it does narrow the field of possibilities for potential exploitability.

Correlation: RFC 1858, Mitre, Bugtraq mail archive #19990324

Active Targeting: Directed at a non-existant machine, but definitely a specific IP address

CVE: CAN-1999-0431

Severity: (2+5) - (4+2) = -1

Defense: The only reasonable solution is to upgrade the kernel to a version greater than v2.3. You might try filtering for bad or illegal fragment offsets (though CheckPoint FW-1 has displayed a serious problem with illegal fragments) or denying zero length fragments (firewall inside a firewall), but this could have the effect of denying path MTU discovery, as well as being just the slightest bit paranoid.

Test Question:

Some of the clues that you might be dealing with a fragment attack are: (select all that apply)

A) You start to see only parts of words in your email

B) You see (or your IDS alarms on) fragments that have overlapping offsets

C) While running tcpdump, you notice a series of fragments that have the Do Not Fragment bit set

D) You look through the days anomolies and see fragments with no data in the payload

Answer: C

Detect 7

Detect 7 Data

Generated by: Snort

Source IP spoof probability: Low, This is in NetWest's corporate public IP space

Description: CGI vulnerability scan

Mechanism: This is another strange catch. At first it looked like a series of natural packets, the sequence numbers were mostly sequential (the occasional odd jump) and the TTL looked to match the OS identity string. I haven't found the script that does this yet, but it would be good misdirection to appear to map out a BSD box with Windows 95. The attacker sent an entire string of CGI exploits, including *NIX, and IIS vulnerabilities, in a span of approximately two minutes. Then they followed up with a DNS version.bind query. That query alone would indicate that the packets are crafted (since you normally would not look for BIND version from a Windows machine, instead you would be looking for WINS version) at least as far as the OS version ID and Browser ID are concerned, so I am presuming a Linux variant.

From the analysis, I would guess that this is an implementation of the "Whisker" attack, but whoever is attacking did not know (or care) to use the stealthing features. Again, no further activity was seen from this source, so unless I saw continued scans or access attempts from the source IP I would tend to mark it up as a newbie exploring the net.

Correlation: Hotman's Cave http://www.hotmanscave.com/, Packetstorm both list several different

CGI scans, Rain Forest Puppy http://www.wiretrip.net/rfp/ lists one that comes closer than most to meeting this pattern.

Active Targeting: Directed at OpenBSD host machine

CVE: CVE-1999-0146, 0147, 0148, 0149

Severity: (2+4) - (5+2) = -1

Defense: The usual for web servers, check the permissions of cgi-bin and perl scripts called by the web server. Run the web server as a non-privileged account if at all possible. Remove scripts that are not needed for the operation of the web site. If possible in your network, mask the version information for publically accessible services such as BIND.

Test Question:

What is one of the signs of a crafted scan?

A) TTL is always the same

B) Sequence number stays the same

C) Destination port is always the same

D) Has a trademark hex output that says "crafted"

Answer: B

Detect 8

Detect 8 Data

Generated by: Snort

Source IP spoof probability: Low

Description: Anomoly caused by certian web client behavior

Mechanism: This is an entertaining False Alarm. My co-worker (Todd Garrison) wrote a filter for Snort that catches the Whisker scan if it is stealthed. We ran into one small problem though, a few web browsers (Lynx in particular) send so much compatibility data that they trigger the filter limits. Lynx in it's infinite wisdom, sends a pre-emptive strike to web servers, rather than waiting for the web server to ask what type of data the client can accept, it sends a bit over 3Kb of packet back to advertise what it can do. That outpouring of data is suficently large that it triggers the Snort scan for Whisker.

```
# Todd Garrison ... These detect the Whisker stealth modes

#don't let stealth mode 4 get us...

alert tcp any any -> $HOME_NET 80 (dsize: > 512; msg:"Whisker stealth CGI scan- HEAD"; content:"|48
45 41 44|"; offset:0; depth: 4;)
```

```
alert tcp any any -> $HOME_NET 80 (dsize: > 512; msg:"Whisker stealth CGI scan- head"; content:"|68
65 61 64|"; offset:0; depth: 4;)

alert tcp any any -> $HOME_NET 80 (dsize: > 512; msg:"Whisker stealth CGI scan- GET"; content:"|47
45 54|"; offset: 0; depth: 3;)

alert tcp any any -> $HOME_NET 80 (dsize: > 512; msg:"Whisker stealth CGI scan- get"; content:"|67
65 74|"; offset: 0; depth: 3;)
```

The above lines are the culprit! By checking for a dsize greater than 512 (Lynx is 3000+), as needed to catch the Whisker stealth scan mode 4, and looking for the HTTP head or get message, we get a false positive on a legitimate web access request. I'll include the rest so that you can see how it all fits together.

```
#some things that show up in stealth mode 7

alert tcp any any -> $HOME_NET 80 (msg:"Start Stop Web access attempt";
content:"/cfide/administrator/startstop.html"; nocase; flags: PA;)

alert tcp any any -> $HOME_NET 80 (msg:"cfappman access attempt"; content:"/cfappman/index.cfm";
nocase; flags: PA;)

alert tcp any any -> $HOME_NET 80 (msg:"Mall log order access attempt";
content:"/mall_log_files/order.log"; nocase; flags: PA;)

alert tcp any any -> $HOME_NET 80 (msg:"Shopping cart access attempt"; content:"/quikstore.cfg";
nocase; flags: PA;)

alert tcp any any -> $HOME_NET 80 (msg:"Order log access attempt"; content:"/admin_files/order.log";
nocase; flags: PA;)

alert tcp any any -> $HOME_NET 80 (msg:"BigConf access attempt"; content:"/bigconf.cgi"; nocase;
flags: PA;)

alert tcp any any -> $HOME_NET 80 (msg:"WS_FTP.INI access attempt "; content:"/ws_ftp.ini"; nocase;
flags: PA;)

alert tcp any any -> $HOME_NET 80 (msg:"IIS search97 access attempt"; content:"/search97.vts";
nocase; flags: PA;)

alert tcp any any -> $HOME_NET 80 (msg:"mlog access attempt"; content:"/mlog.phtml"; nocase; flags:
PA;)

alert tcp any any -> $HOME_NET 80 (msg:"mylog access attempt"; content:"/mylog.phtml"; nocase;
flags: PA;)

#some things that show up in stealth mode 8

alert tcp any any -> $HOME_NET 80 (msg:"Start Stop Web access attempt - Whisker stealth scan";
content:"/cfide\\administrator\\startstop.html"; flags: PA;)

alert tcp any any -> $HOME_NET 80 (msg:"cfappman access attempt - Whisker stealth scan";
content:"/cfappman\\index.cfm"; flags: PA;)

alert tcp any any -> $HOME_NET 80 (msg:"Mall log order access attempt - Whisker stealth scan";
content:"/mall_log_files\\order.log"; flags: PA;)

alert tcp any any -> $HOME_NET 80 (msg:"Order log access attempt - Whisker stealth scan";
content:"/admin_files\\order.log"; flags: PA;)

alert tcp any any -> $HOME_NET 80 (msg:"DBML Parser access attempt - Whisker stealth scan";
content:"/cfide\\administrator\\startstop.html"; flags: PA;)

alert tcp any any -> $HOME_NET 80 (msg:"Web Distribution access attempt - Whisker stealth scan";
content:"/cgi-bin\\webdist.cgi"; flags: PA;)

alert tcp any any -> $HOME_NET 80 (msg:"Handler CGI access attempt - Whisker stealth scan";
```

```
content:"/cgi-bin\\handler"; flags: PA;)

alert tcp any any -> $HOME_NET 80 (msg:"wrap CGI access attempt - Whisker stealth scan";
content:"/cgi-bin\\wrap"; flags: PA;)

# Thats enough to make whisker get noticed (for now)
```

Correlation: The behavior of Lynx may have been known, but I can't find any other instances of it setting off IDS's

Active Targeting: None

Severity: None/False

Defense: Just be sure as to what you're making a ruckus about before you unnecessarily get up the nose of someone who could make your life miserable!

Test Question:

When making the call that a particular detect is a false alarm, it is important to consider: (select all that apply)

A) The potential impact if the detect is true

B) Any method that can be used to corroborate your judgement

C) Ways to minimize future false alarms

D) Whether you've updated your resume recently

Answer: All of the above

Detect 9

Detect 9 Data

Generated by: Snort and Dragon-Fire

Source IP spoof probability: Moderate, IP is part of Rogers@Home in Canada

Description: Repeated attachments to port 1524

Mechanism: A decent little SYN scan, ran sequentially across 2123 source ports. May have been intended as a buffer overflow or DoS, as the payload data and destination port do not change. Ran for nineteen minutes and we never heard from the would be attacker again. Remarkable only for the persistence shown in continuing an attack that is both very noisy and ineffective. Presuming that this was an actual access attempt, it is likely that the attacker was trying to access the /IISADMPWD directory that is created by default with IISv4. Unfortunately for the attacker, we were using SAMBAR Web server and so were not vulnerable to this particular attack.

Correlation: Packetstorm and Rain Forest Puppy both list several methods of performing this as a DoS and as an attack/scan

Active Targeting: Directed at Windows SAMBAR server

CVE: CVE-1999-0407

Severity: (2+4) - (5+2) = -1

Defense: Patch to the latest version of IISv4 or run IISv5. Also, you can change the location and permissions on the IISADMPWD directory or force the server to use the domain SAM database instead (though using the domain SAM leads to a completely different set of potential vulnerabilities).

Test Question:

In this detect, why would this be more likely to be a DoS rather than a scan?

A) Because the destination port incremented with every packet

B) Because the source port incremented with every packet

C) The destination port was the only constant in the packet trace

D) If all the ships come into the same port, it can get jammed up

Answer: C

Detect 10

Detect 10 Data

Generated by: Dragon-Fire

Source IP spoof probability: Low, IP range is leased to MasterCard International by AT&T for use in their corporate network

Description: SMB scan looking for open shares

Mechanism: Fairly standard SMB-Wildcard scan running against the OpenBSD machine, presumably in hopes that we were running an open SAMBA server. The attacker seemed to be trying to get open share or directory names. The pattern of the scan seems to match the mnemonix/NTInfoScan utility. Although I snipped about two-thirds of the packets (this paper is getting a bit lengthy), the sent attack tried to match open shares by looking for the letters of the alphabet (a-zlA-Z) and then a dictionary list of common names (pub, public, home, My Documents, etc.).

Correlation: Hacking Exposed (S McClure, et. al)

Active Targeting: Directed at OpenBSD host

CVE: CAN-1999-0519, 0520

Severity: (2+3) - (5+2) = -2

Defense: Close off open/unpassworded shares. Upgrade to the latest Samba patches if you have to share out to Windows based machines. Deny outside access to Samba/SMB ports if possible in your network architecture

Test Question:

What is one of the weaknesses of the SAMBA server?

A) It doesn't really have any weaknesses

B) It uses the UNIX crypt function to send username and password

C) It sends username and password in clear text by default

D) It doesn't understand old Windows for Workgroups shares

Answer: C

DETECT 1 DATA

```
[**] Striker [**]

05/21-01:06:38.682114 209.119.36.4:53 -> 192.168.1.66:2565

UDP TTL:59 TOS:0x0 ID:48263

Len: 124

[**] Portal Of Doom [**]

05/21-06:57:57.119339 209.119.36.4:53 -> 192.168.1.66:3700

UDP TTL:59 TOS:0x0 ID:28962

Len: 128

[**] Prosiak [**]

05/21-11:29:09.898485 209.119.36.4:53 -> 192.168.1.67:33333

UDP TTL:59 TOS:0x0 ID:55530

Len: 126

[**] ICQ Trojan [**]

05/21-13:25:07.884696 209.119.36.4:53 -> 192.168.1.66:4950

UDP TTL:59 TOS:0x0 ID:1490
```

```
Len: 181
[**] Sockets De Troie [**]
05/21-13:37:11.298303 209.119.36.4:53 -> 192.168.1.66:5000
UDP TTL:59 TOS:0x0 ID:2789
Len: 127
[**] Psyber Stream [**]
05/21-14:15:48.784922 209.119.36.4:53 -> 192.168.1.66:1170
UDP TTL:59 TOS:0x0 ID:7313
Len: 183
[**] Ultors Trojan [**]
05/21-14:38:54.080872 209.119.36.4:53 -> 192.168.1.66:1234
UDP TTL:59 TOS:0x0 ID:9338
Len: 210
[**] Portal Of Doom [**]
05/22-03:14:45.445608 209.119.36.4:53 -> 192.168.1.66:3700
UDP TTL:59 TOS:0x0 ID:36282
Len: 124
[**] ICQ Trojan [**]
05/22-09:44:21.859517 209.119.36.4:53 -> 192.168.1.66:4950
UDP TTL:59 TOS:0x0 ID:22514
Len: 127
[**] Sockets De Troie [**]
05/22-09:58:56.746265 209.119.36.4:53 -> 192.168.1.66:5000
UDP TTL:59 TOS:0x0 ID:24762
Len: 124
[**] FTP99cmp [**]
05/22-06:25:41.925210 209.119.36.4:53 -> 192.168.1.66:1492
UDP TTL:59 TOS:0x0 ID:49436
Len: 127
[**] Shivka-Burka [**]
```

```
05/22-06:57:35.760860 209.119.36.4:53 -> 192.168.1.66:1600
UDP TTL:59 TOS:0x0 ID:54369
Len: 128
[**] Spy Sender [**]
05/22-07:59:22.624811 209.119.36.4:53 -> 192.168.1.66:1807
UDP TTL:59 TOS:0x0 ID:64941
Len: 127
[**] ShockRave [**]
05/22-08:53:01.125895 209.119.36.4:53 -> 192.168.1.66:1981
UDP TTL:59 TOS:0x0 ID:7170
Len: 124
[**] Back Door [**]
05/22-08:56:33.381694 209.119.36.4:53 -> 192.168.1.66:1999
UDP TTL:59 TOS:0x0 ID:8105
Len: 183
[**] Trojan Cow [**]
05/22-08:56:54.726361 209.119.36.4:53 -> 192.168.1.66:2001
UDP TTL:59 TOS:0x0 ID:8186
Len: 181
[**] Ripper Pro [**]
05/22-09:00:33.955599 209.119.36.4:53 -> 192.168.1.66:2023
UDP TTL:59 TOS:0x0 ID:9047
Len: 128
[**] Psyber Stream [**]
05/22-09:57:50.160828 209.119.36.4:53 -> 192.168.1.66:1170
UDP TTL:59 TOS:0x0 ID:19963
Len: 127
[**] Ultors Trojan [**]
05/22-10:13:38.495224 209.119.36.4:53 -> 192.168.1.66:1234
```

```
UDP TTL:59 TOS:0x0 ID:22331

Len: 127

[**] FTP99cmp [**]

05/22-14:05:38.124572 209.119.36.4:53 -> 192.168.1.66:1492

UDP TTL:59 TOS:0x0 ID:49089

Len: 124

[**] Spy Sender [**]

05/22-20:25:24.694907 209.119.36.4:53 -> 192.168.1.66:1807

UDP TTL:59 TOS:0x0 ID:24854

Len: 124

[**] ShockRave [**]

05/23-00:05:55.598888 209.119.36.4:53 -> 192.168.1.66:1981

UDP TTL:59 TOS:0x0 ID:62823

Len: 124

[**] Back Door [**]

05/23-00:30:25.619042 209.119.36.4:53 -> 192.168.1.66:1999

UDP TTL:59 TOS:0x0 ID:498

Len: 124

[**] Trojan Cow [**]

05/23-00:30:25.701194 209.119.36.4:53 -> 192.168.1.66:2001

UDP TTL:59 TOS:0x0 ID:499

Len: 124

[**] WinCrash [**]

05/23-20:55:21.249071 209.119.36.4:53 -> 192.168.1.66:3024

UDP TTL:59 TOS:0x0 ID:12306

Len: 124

[**] Shivka-Burka [**]

05/25-22:56:52.087437 209.119.36.4:53 -> 192.168.1.66:1600

UDP TTL:59 TOS:0x0 ID:2826

Len: 124
```

```
[**] VooDoo Doll [**]
05/25-16:00:20.473865 209.119.36.4:53 -> 192.168.1.66:1245
UDP TTL:59 TOS:0x0 ID:37610
Len: 124
[**] Sockets De Troie [**]
05/25-11:43:09.490236 209.119.36.4:53 -> 192.168.1.66:5000
UDP TTL:59 TOS:0x0 ID:9195
Len: 124
[**] Psyber Stream [**]
05/25-14:34:40.054290 209.119.36.4:53 -> 192.168.1.66:1170
UDP TTL:59 TOS:0x0 ID:28525
Len: 124
[**] Fore [**]
05/26-05:43:49.832436 209.119.36.4:53 -> 192.168.1.67:50776
UDP TTL:59 TOS:0x0 ID:64020
Len: 260
[**] Bugs [**]
05/26-09:09:24.385390 209.119.36.4:53 -> 192.168.1.66:2115
UDP TTL:59 TOS:0x0 ID:44670
Len: 124
[**] Remote Win Shutdown [**]
05/28-11:12:49.597966 209.119.36.4:53 -> 192.168.1.67:53001
UDP TTL:58 TOS:0x0 ID:11839
Len: 265
[**] Ultors Trojan [**]
05/29-03:35:33.399442 209.119.36.4:53 -> 192.168.1.66:1234
UDP TTL:59 TOS:0x0 ID:5647
Len: 124
[**] Shivka-Burka [**]
```

```
05/29-10:56:30.017220 209.119.36.4:53 -> 192.168.1.66:1600

UDP TTL:59 TOS:0x0 ID:53166

Len: 124

[**] Phineas Phucker [**]

05/30-02:47:38.031963 209.119.36.4:53 -> 192.168.1.66:2801

UDP TTL:59 TOS:0x0 ID:33958

Len: 124

[**] Deep Throat/Invasor [**]

05/30-09:19:39.330363 209.119.36.4:53 -> 192.168.1.66:3150

UDP TTL:59 TOS:0x0 ID:34758

Len: 124

[**] Sockets De Troie [**]

05/31-20:26:42.596015 209.119.36.4:53 -> 192.168.1.66:5000

UDP TTL:59 TOS:0x0 ID:23173

Len: 124

[**] VooDoo Doll [**]

06/01-00:44:06.736729 209.119.36.4:53 -> 192.168.1.66:1245

UDP TTL:59 TOS:0x0 ID:50916

Len: 124
```

Return to Detect 1

DETECT 2 DATA

```
[**] SNMP public access [**]

05/29-16:58:21.047981 216.164.136.103:1029 -> 192.168.1.67:161

UDP TTL:49 TOS:0x0 ID:11015

Len: 51

[**] SNMP public access [**]

05/29-16:58:23.034753 216.164.136.103:1029 -> 192.168.1.67:161

UDP TTL:49 TOS:0x0 ID:11016

Len: 51
```

```
[**] SNMP public access [**]
05/29-16:58:25.029843 216.164.136.103:1029 -> 192.168.1.67:161
UDP TTL:49 TOS:0x0 ID:11017
Len: 51
[**] SNMP public access [**]
05/29-16:58:27.003695 216.164.136.103:1029 -> 192.168.1.67:161
UDP TTL:49 TOS:0x0 ID:11020
Len: 51
[**] SNMP public access [**]
05/29-16:58:29.047705 216.164.136.103:1029 -> 192.168.1.67:161
UDP TTL:49 TOS:0x0 ID:11021
Len: 51
[**] SNMP public access [**]
05/29-16:58:31.042419 216.164.136.103:1029 -> 192.168.1.67:161
UDP TTL:49 TOS:0x0 ID:11023
Len: 51
dragon (Towards) 22:58:22
SOURCE: 216.164.136.103 216-164-136-103.s103.tnt4.lnhva.md.dialup.rcn.com
DEST: 192.168.1.67 solaris.evilscan.com
45 00 00 47 2b 07 00 00 31 11 26 61 d8 a4 88 67 c7 ef 0f 43 E..G+...1.&a...g...C
04 05 00 a1 00 33 a2 95 30 29 02 01 00 04 06 70 75 62 6c 69 .....3..0).....publi
63 a0 1c 02 04 5e 11 07 42 02 01 00 02 01 00 30 0e 30 0c 06 c....^..B......0.0..
08 2b 06 01 02 01 01 01 00 05 00 .+.........
EVENT1: [SNMP:PUBLIC] (udp,dp=161,sp=1029)
dragon (Towards) 22:58:24
SOURCE: 216.164.136.103 216-164-136-103.s103.tnt4.lnhva.md.dialup.rcn.com
DEST: 192.168.1.67 solaris.evilscan.com
45 00 00 47 2b 08 00 00 31 11 26 60 d8 a4 88 67 c7 ef 0f 43 E..G+...1.&`...g...C
04 05 00 a1 00 33 a2 95 30 29 02 01 00 04 06 70 75 62 6c 69 .....3..0).....publi
```

```
63 a0 1c 02 04 5e 11 07 42 02 01 00 02 01 00 30 0e 30 0c 06 c....^..B......0.0..
08 2b 06 01 02 01 01 01 00 05 00 .+.........
EVENT1: [SNMP:PUBLIC] (udp,dp=161,sp=1029)
dragon (Towards) 22:58:26
SOURCE: 216.164.136.103 216-164-136-103.s103.tnt4.lnhva.md.dialup.rcn.com
DEST: 192.168.1.67 solaris.evilscan.com
45 00 00 47 2b 09 00 00 31 11 26 5f d8 a4 88 67 c7 ef 0f 43 E..G+...1.&_...g...C
04 05 00 a1 00 33 a2 95 30 29 02 01 00 04 06 70 75 62 6c 69 .....3..0).....publi
63 a0 1c 02 04 5e 11 07 42 02 01 00 02 01 00 30 0e 30 0c 06 c....^..B......0.0..
08 2b 06 01 02 01 01 01 00 05 00 .+.........
EVENT1: [SNMP:PUBLIC] (udp,dp=161,sp=1029)
dragon (Towards) 22:58:28
SOURCE: 216.164.136.103 216-164-136-103.s103.tnt4.lnhva.md.dialup.rcn.com
DEST: 192.168.1.67 solaris.evilscan.com
45 00 00 47 2b 0c 00 00 31 11 26 5c d8 a4 88 67 c7 ef 0f 43 E..G+...1.&\...g...C
04 05 00 a1 00 33 a2 95 30 29 02 01 00 04 06 70 75 62 6c 69 .....3..0).....publi
63 a0 1c 02 04 5e 11 07 42 02 01 00 02 01 00 30 0e 30 0c 06 c....^..B......0.0..
08 2b 06 01 02 01 01 01 00 05 00 .+.........
EVENT1: [SNMP:PUBLIC] (udp,dp=161,sp=1029)
dragon (Towards) 22:58:30
SOURCE: 216.164.136.103 216-164-136-103.s103.tnt4.lnhva.md.dialup.rcn.com
DEST: 192.168.1.67 solaris.evilscan.com
45 00 00 47 2b 0d 00 00 31 11 26 5b d8 a4 88 67 c7 ef 0f 43 E..G+...1.&[...g...C
04 05 00 a1 00 33 a2 95 30 29 02 01 00 04 06 70 75 62 6c 69 .....3..0).....publi
63 a0 1c 02 04 5e 11 07 42 02 01 00 02 01 00 30 0e 30 0c 06 c....^..B......0.0..
08 2b 06 01 02 01 01 01 00 05 00 .+.........
EVENT1: [SNMP:PUBLIC] (udp,dp=161,sp=1029)
dragon (Towards) 22:58:32
SOURCE: 216.164.136.103 216-164-136-103.s103.tnt4.lnhva.md.dialup.rcn.com
DEST: 192.168.1.67 solaris.evilscan.com
```

```
45 00 00 47 2b 0f 00 00 31 11 26 59 d8 a4 88 67 c7 ef 0f 43 E..G+...1.&Y...g...C

04 05 00 a1 00 33 a2 95 30 29 02 01 00 04 06 70 75 62 6c 69 .....3..0).....publi

63 a0 1c 02 04 5e 11 07 42 02 01 00 02 01 00 30 0e 30 0c 06 c....^..B......0.0..

08 2b 06 01 02 01 01 01 00 05 00 .+.........

EVENT1: [SNMP:PUBLIC] (udp,dp=161,sp=1029)
```

Return to Detect 2

DETECT 3 DATA

```
[**] spp_portscan: PORTSCAN DETECTED from 209.215.54.130 [**]

05/28-22:49:19.762959

[**] Netbus/GabanBus [**]

05/28-22:49:20.393796 209.215.54.130:49562 -> 192.168.1.66:12345

TCP TTL:40 TOS:0x0 ID:57818

**S***** Seq: 0x941104D0 Ack: 0x0 Win: 0x1000

[**] BIND Shell [**]

05/28-22:49:21.979313 209.215.54.130:49562 -> 192.168.1.66:31337

TCP TTL:40 TOS:0x0 ID:17583

**S***** Seq: 0x941104D0 Ack: 0x0 Win: 0x1000

[**] spp_portscan: portscan status from 209.215.54.130: 131 connections across 1 hosts:
TCP(131), UDP(0) [**]

05/28-22:49:22.017794

[**] Netbus/GabanBus [**]

05/28-22:49:22.874189 209.215.54.130:49562 -> 192.168.1.66:12346

TCP TTL:40 TOS:0x0 ID:41314

**S***** Seq: 0x941104D0 Ack: 0x0 Win: 0x1000

[**] spp_portscan: portscan status from 209.215.54.130: 221 connections across 1 hosts:
TCP(221), UDP(0) [**]

05/28-22:49:25.125865

[**] Possible GateCrasher access [**]

05/28-22:49:26.647056 209.215.54.130:49562 -> 192.168.1.66:6969
```

```
TCP TTL:40 TOS:0x0 ID:53762

**S***** Seq: 0x941104D0 Ack: 0x0 Win: 0x1000

[**] spp_portscan: portscan status from 209.215.54.130: 238 connections across 1 hosts:
TCP(238), UDP(0) [**]

05/28-22:49:28.231344

[**] Attempted Sun RPC high port access [**]

05/28-22:49:28.214075 209.215.54.130:49562 -> 192.168.1.66:32771

TCP TTL:40 TOS:0x0 ID:721

**S***** Seq: 0x941104D0 Ack: 0x0 Win: 0x1000

[**] spp_portscan: portscan status from 209.215.54.130: 223 connections across 1 hosts:
TCP(223), UDP(0) [**]

05/28-22:49:31.024403

[**] spp_portscan: portscan status from 209.215.54.130: 299 connections across 1 hosts:
TCP(299), UDP(0) [**]

05/28-22:49:34.030416

[**] default Backdoor access! [**]

05/28-22:49:35.317049 209.215.54.130:49562 -> 192.168.1.66:1524

TCP TTL:40 TOS:0x0 ID:9662

**S***** Seq: 0x941104D0 Ack: 0x0 Win: 0x1000

[**] WinGate 1080 Attempt [**]

05/28-22:49:35.694145 209.215.54.130:49562 -> 192.168.1.66:1080

TCP TTL:40 TOS:0x0 ID:32955

**S***** Seq: 0x941104D0 Ack: 0x0 Win: 0x1000

[**] spp_portscan: portscan status from 209.215.54.130: 283 connections across 1 hosts:
TCP(283), UDP(0) [**]

05/28-22:49:37.039834

[**] NMAP TCP ping! [**]

05/28-22:49:38.455954 209.215.54.130:49572 -> 192.168.1.66:80

TCP TTL:40 TOS:0x0 ID:57214

******A* Seq: 0xB6242F73 Ack: 0x0 Win: 0x1000

TCP Options => WS: 10 NOP MSS: 265 TS: 1061109567 0 EOL EOL

[**] NMAP TCP ping! [**]
```

```
05/28-22:49:38.479859 209.215.54.130:49574 -> 192.168.1.66:82

TCP TTL:40 TOS:0x0 ID:20268

******A* Seq: 0xB6242F73 Ack: 0x0 Win: 0x1000

TCP Options => WS: 10 NOP MSS: 265 TS: 1061109567 0 EOL EOL

[**] spp_portscan: portscan status from 209.215.54.130: 127 connections across 1 hosts:
TCP(126), UDP(1) STEALTH [**]

05/28-22:49:47.979086

[**] spp_portscan: portscan status from 209.215.54.130: 1 connections across 1 hosts:
TCP(1), UDP(0) [**]

05/28-22:49:50.129081

[**] spp_portscan: portscan status from 209.215.54.130: 1 connections across 1 hosts:
TCP(1), UDP(0) [**]

05/28-22:49:53.207880

[**] NMAP TCP ping! [**]

05/28-22:49:54.351612 209.215.54.130:49572 -> 192.168.1.66:80

TCP TTL:40 TOS:0x0 ID:58157

******A* Seq: 0x876DE24E Ack: 0x0 Win: 0x1000

TCP Options => WS: 10 NOP MSS: 265 TS: 1061109567 0 EOL EOL

[**] NMAP TCP ping! [**]

05/28-22:49:54.362404 209.215.54.130:49574 -> 192.168.1.66:82

TCP TTL:40 TOS:0x0 ID:7032

******A* Seq: 0x876DE24E Ack: 0x0 Win: 0x1000

TCP Options => WS: 10 NOP MSS: 265 TS: 1061109567 0 EOL EOL

[**] spp_portscan: portscan status from 209.215.54.130: 5 connections across 1 hosts:
TCP(4), UDP(1) STEALTH [**]

05/28-22:50:03.561120

[**] spp_portscan: portscan status from 209.215.54.130: 1 connections across 1 hosts:
TCP(1), UDP(0) [**]

05/28-22:50:06.440281

[**] spp_portscan: portscan status from 209.215.54.130: 2 connections across 1 hosts:
TCP(2), UDP(0) STEALTH [**]

05/28-22:50:09.891116
```

```
[**] NMAP TCP ping! [**]

05/28-22:50:09.952187 209.215.54.130:49572 -> 192.168.1.66:80

TCP TTL:40 TOS:0x0 ID:50852

******A* Seq: 0x8A276921 Ack: 0x0 Win: 0x1000

TCP Options => WS: 10 NOP MSS: 265 TS: 1061109567 0 EOL EOL

[**] NMAP TCP ping! [**]

05/28-22:50:09.962538 209.215.54.130:49574 -> 192.168.1.66:82

TCP TTL:40 TOS:0x0 ID:5684

******A* Seq: 0x8A276921 Ack: 0x0 Win: 0x1000

TCP Options => WS: 10 NOP MSS: 265 TS: 1061109567 0 EOL EOL

[**] spp_portscan: portscan status from 209.215.54.130: 4 connections across 1 hosts:
TCP(3), UDP(1) STEALTH [**]

05/28-22:50:19.210571

[**] spp_portscan: portscan status from 209.215.54.130: 1 connections across 1 hosts:
TCP(1), UDP(0) [**]

05/28-22:50:22.091019

[**] spp_portscan: portscan status from 209.215.54.130: 1 connections across 1 hosts:
TCP(1), UDP(0) [**]

05/28-22:50:25.270000

[**] spp_portscan: End of portscan from 209.215.54.130 [**]

05/28-22:50:35.377156

[**] spp_portscan: PORTSCAN DETECTED from 209.215.54.130 [**]

05/29-02:28:09.871564

[**] spp_portscan: portscan status from 209.215.54.130: 110 connections across 1 hosts:
TCP(110), UDP(0) [**]

05/29-02:28:12.045283

[**] default Backdoor access! [**]

05/29-02:28:12.121106 209.215.54.130:34861 -> 192.168.1.66:1524

TCP TTL:30 TOS:0x0 ID:40648

**S***** Seq: 0x4A034602 Ack: 0x0 Win: 0x800

[**] BIND Shell [**]

05/29-02:28:12.536546 209.215.54.130:34861 -> 192.168.1.66:31337
```

```
TCP TTL:30 TOS:0x0 ID:8774

**S***** Seq: 0x4A034602 Ack: 0x0 Win: 0x800

[**] spp_portscan: portscan status from 209.215.54.130: 148 connections across 1 hosts:
TCP(148), UDP(0) [**]

05/29-02:28:15.445278

[**] Netbus/GabanBus [**]

05/29-02:28:15.772579 209.215.54.130:34861 -> 192.168.1.66:12346

TCP TTL:30 TOS:0x0 ID:46815

**S***** Seq: 0x4A034602 Ack: 0x0 Win: 0x800

[**] spp_portscan: portscan status from 209.215.54.130: 192 connections across 1 hosts:
TCP(192), UDP(0) [**]

05/29-02:28:18.023681

[**] Netbus/GabanBus [**]

05/29-02:28:20.413811 209.215.54.130:34861 -> 192.168.1.66:12345

TCP TTL:30 TOS:0x0 ID:21720

**S***** Seq: 0x4A034602 Ack: 0x0 Win: 0x800

[**] spp_portscan: portscan status from 209.215.54.130: 262 connections across 1 hosts:
TCP(262), UDP(0) [**]

05/29-02:28:21.026363

[**] Attempted Sun RPC high port access [**]

05/29-02:28:21.288272 209.215.54.130:34861 -> 192.168.1.66:32771

TCP TTL:30 TOS:0x0 ID:5184

**S***** Seq: 0x4A034602 Ack: 0x0 Win: 0x800

[**] spp_portscan: portscan status from 209.215.54.130: 185 connections across 1 hosts:
TCP(185), UDP(0) [**]

05/29-02:28:24.023538

[**] Possible GateCrasher access [**]

05/29-02:28:26.362715 209.215.54.130:34861 -> 192.168.1.66:6969

TCP TTL:30 TOS:0x0 ID:31894

**S***** Seq: 0x4A034602 Ack: 0x0 Win: 0x800

[**] spp_portscan: portscan status from 209.215.54.130: 251 connections across 1 hosts:
TCP(251), UDP(0) [**]
```

```
05/29-02:28:27.086021

[**] WinGate 1080 Attempt [**]

05/29-02:28:27.374282 209.215.54.130:34861 -> 192.168.1.66:1080

TCP TTL:30 TOS:0x0 ID:6582

**S***** Seq: 0x4A034602 Ack: 0x0 Win: 0x800

[**] spp_portscan: portscan status from 209.215.54.130: 265 connections across 1 hosts:
TCP(265), UDP(0) [**]

05/29-02:28:30.042711

[**] NMAP TCP ping! [**]

05/29-02:28:31.331202 209.215.54.130:34871 -> 192.168.1.66:80

TCP TTL:30 TOS:0x0 ID:25036

******A* Seq: 0x7566BE32 Ack: 0x0 Win: 0x800

TCP Options => WS: 10 NOP MSS: 265 TS: 1061109567 0 EOL EOL

[**] NMAP TCP ping! [**]

05/29-02:28:31.355285 209.215.54.130:34873 -> 192.168.1.66:564

TCP TTL:30 TOS:0x0 ID:6512

******A* Seq: 0x7566BE32 Ack: 0x0 Win: 0x800

TCP Options => WS: 10 NOP MSS: 265 TS: 1061109567 0 EOL EOL

[**] spp_portscan: portscan status from 209.215.54.130: 109 connections across 1 hosts:
TCP(108), UDP(1) STEALTH [**]

05/29-02:28:35.518336

[**] spp_portscan: portscan status from 209.215.54.130: 1 connections across 1 hosts:
TCP(1), UDP(0) [**]

05/29-02:28:40.624355

[**] spp_portscan: portscan status from 209.215.54.130: 1 connections across 1 hosts:
TCP(1), UDP(0) [**]

05/29-02:28:43.304574

[**] spp_portscan: portscan status from 209.215.54.130: 2 connections across 1 hosts:
TCP(2), UDP(0) STEALTH [**]

05/29-02:28:46.657774

[**] NMAP TCP ping! [**]

05/29-02:28:46.710335 209.215.54.130:34871 -> 192.168.1.66:80
```

```
TCP TTL:30 TOS:0x0 ID:2036

******A* Seq: 0x8510D104 Ack: 0x0 Win: 0x800

TCP Options => WS: 10 NOP MSS: 265 TS: 1061109567 0 EOL EOL

[**] NMAP TCP ping! [**]

05/29-02:28:46.722963 209.215.54.130:34873 -> 192.168.1.66:564

TCP TTL:30 TOS:0x0 ID:26358

******A* Seq: 0x8510D104 Ack: 0x0 Win: 0x800

TCP Options => WS: 10 NOP MSS: 265 TS: 1061109567 0 EOL EOL

[**] spp_portscan: portscan status from 209.215.54.130: 4 connections across 1 hosts:
TCP(3), UDP(1) STEALTH [**]

05/29-02:28:55.587228

[**] spp_portscan: portscan status from 209.215.54.130: 1 connections across 1 hosts:
TCP(1), UDP(0) [**]

05/29-02:28:58.264902

[**] spp_portscan: portscan status from 209.215.54.130: 2 connections across 1 hosts:
TCP(2), UDP(0) STEALTH [**]

05/29-02:29:01.617074

[**] NMAP TCP ping! [**]

05/29-02:29:01.677414 209.215.54.130:34871 -> 192.168.1.66:80

TCP TTL:30 TOS:0x0 ID:38605

******A* Seq: 0x1AC32EC6 Ack: 0x0 Win: 0x800

TCP Options => WS: 10 NOP MSS: 265 TS: 1061109567 0 EOL EOL

[**] NMAP TCP ping! [**]

05/29-02:29:01.688062 209.215.54.130:34873 -> 192.168.1.66:564

TCP TTL:30 TOS:0x0 ID:35186

******A* Seq: 0x1AC32EC6 Ack: 0x0 Win: 0x800

TCP Options => WS: 10 NOP MSS: 265 TS: 1061109567 0 EOL EOL

[**] spp_portscan: portscan status from 209.215.54.130: 4 connections across 1 hosts:
TCP(3), UDP(1) STEALTH [**]

05/29-02:29:10.616622

[**] spp_portscan: portscan status from 209.215.54.130: 1 connections across 1 hosts:
TCP(1), UDP(0) [**]
```

```
05/29-02:29:13.296248

[**] spp_portscan: portscan status from 209.215.54.130: 1 connections across 1 hosts:
TCP(1), UDP(0) [**]

05/29-02:29:24.292248

[**] spp_portscan: End of portscan from 209.215.54.130 [**]

05/29-02:29:45.367800
```

Return to Detect 3

DETECT 4 DATA

```
May 25 22:56:40 solaris rpc.cmsd: [ID 767094 daemon.error] svc_reg(tcp) failed

May 25 22:58:42 solaris rpc.cmsd: [ID 767094 daemon.error] svc_reg(tcp) failed

May 25 23:00:42 solaris rpc.cmsd: [ID 767094 daemon.error] svc_reg(tcp) failed

May 25 23:02:42 solaris rpc.cmsd: [ID 767094 daemon.error] svc_reg(tcp) failed

May 25 23:04:42 solaris rpc.cmsd: [ID 767094 daemon.error] svc_reg(tcp) failed

May 26 00:47:04 solaris rpc.cmsd: [ID 767094 daemon.error] svc_reg(tcp) failed

May 26 00:49:04 solaris rpc.cmsd: [ID 767094 daemon.error] svc_reg(tcp) failed

May 26 00:51:04 solaris rpc.cmsd: [ID 767094 daemon.error] svc_reg(tcp) failed

May 26 03:39:39 solaris rpc.cmsd: [ID 767094 daemon.error] svc_reg(tcp) failed

May 26 03:41:40 192.168.1.67 rpc.cmsd: [ID 767094 daemon.error] svc_reg(tcp) failed

May 26 03:43:40 solaris rpc.cmsd: [ID 767094 daemon.error] svc_reg(tcp) failed

May 26 15:31:17 solaris rpc.cmsd: [ID 767094 daemon.error] svc_reg(tcp) failed

May 26 15:32:07 fw inet: inetd shutdown succeeded

May 26 15:33:18 solaris rpc.cmsd: [ID 767094 daemon.error] svc_reg(tcp) failed

May 26 15:34:58 fw inet: inetd shutdown succeeded

May 26 15:35:19 solaris rpc.cmsd: [ID 767094 daemon.error] svc_reg(tcp) failed

May 26 15:36:37 fw inet: inetd shutdown succeeded

May 26 15:37:20 solaris rpc.cmsd: [ID 767094 daemon.error] svc_reg(tcp) failed

May 26 15:37:40 fw inet: inetd shutdown succeeded

May 26 15:38:38 fw inet: inetd shutdown succeeded

May 26 15:39:21 solaris rpc.cmsd: [ID 767094 daemon.error] svc_reg(tcp) failed
```

```
May 26 15:40:27 fw inet: inetd shutdown succeeded

May 26 15:41:22 solaris rpc.cmsd: [ID 767094 daemon.error] svc_reg(tcp) failed

May 26 15:43:23 solaris rpc.cmsd: [ID 767094 daemon.error] svc_reg(tcp) failed

May 30 15:55:54 solaris rpc.cmsd: [ID 767094 daemon.error] svc_reg(tcp) failed
```

Return to Detect 4

DETECT 5 DATA

```
GET /cgi-bin/dumpenv.pl HTTP/1.1{D}{A}

Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-excel,
application/msword, application/vnd.ms-powerpoint, application/x-comet, */*{D}{A}

Accept-Language: en-us{D}{A}

Accept-Encoding: gzip, deflate{D}{A}

User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Windows NT){D}{A}

Host: 192.168.1.66{D}{A}

Connection: Keep-Alive{D}{A}

{D}{A}
```

Return to Detect 5

DETECT 6 DATA

```
[**] Tiny Fragments - Possible Hostile Activity [**]

05/22-19:01:39.829894 202.102.20.10 -> 192.168.1.132

TCP TTL:109 TOS:0x0 ID:16904 DF MF

Frag Offset: 0x0 Frag Size: 0x1A

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................

00 00 00 00 00 00 00 00 00 00 ..........

[**] Tiny Fragments - Possible Hostile Activity [**]

05/22-19:01:40.026845 202.102.20.10 -> 192.168.1.132

TCP TTL:109 TOS:0x0 ID:17416 DF MF

Frag Offset: 0x0 Frag Size: 0x1A

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................

00 00 00 00 00 00 00 00 00 00 ..........
```

```
[**] Tiny Fragments - Possible Hostile Activity [**]
05/22-19:01:40.198503 202.102.20.10 -> 192.168.1.132
TCP TTL:109 TOS:0x0 ID:17672 DF MF
Frag Offset: 0x0 Frag Size: 0x1A
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00 00 00 00 00 00 00 00 00 00 .........
[**] Tiny Fragments - Possible Hostile Activity [**]
05/22-19:01:40.395744 202.102.20.10 -> 192.168.1.132
TCP TTL:109 TOS:0x0 ID:17928 DF MF
Frag Offset: 0x0 Frag Size: 0x1A
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00 00 00 00 00 00 00 00 00 00 .........
[**] Tiny Fragments - Possible Hostile Activity [**]
05/22-19:01:40.575302 202.102.20.10 -> 192.168.1.132
TCP TTL:109 TOS:0x0 ID:18184 DF MF
Frag Offset: 0x0 Frag Size: 0x1A
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00 00 00 00 00 00 00 00 00 00 .........
[**] Tiny Fragments - Possible Hostile Activity [**]
05/22-19:01:40.765545 202.102.20.10 -> 192.168.1.132
TCP TTL:109 TOS:0x0 ID:18440 DF MF
Frag Offset: 0x0 Frag Size: 0x1A
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00 00 00 00 00 00 00 00 00 00 .........
[**] Tiny Fragments - Possible Hostile Activity [**]
05/22-19:08:22.021479 202.102.20.10 -> 192.168.1.132
TCP TTL:109 TOS:0x0 ID:33544 DF MF
Frag Offset: 0x0 Frag Size: 0x1A
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
```

```
00 00 00 00 00 00 00 00 00 00 ..........

[**] Tiny Fragments - Possible Hostile Activity [**]

05/22-19:08:22.210386 202.102.20.10 -> 192.168.1.132

TCP TTL:109 TOS:0x0 ID:34056 DF MF

Frag Offset: 0x0 Frag Size: 0x1A

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................

00 00 00 00 00 00 00 00 00 00 ..........

[**] Tiny Fragments - Possible Hostile Activity [**]

05/22-19:08:22.398123 202.102.20.10 -> 192.168.1.132

TCP TTL:109 TOS:0x0 ID:34312 DF MF

Frag Offset: 0x0 Frag Size: 0x1A

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................

00 00 00 00 00 00 00 00 00 00 ..........

[**] Tiny Fragments - Possible Hostile Activity [**]

05/22-19:08:22.591218 202.102.20.10 -> 192.168.1.132

TCP TTL:109 TOS:0x0 ID:34568 DF MF

Frag Offset: 0x0 Frag Size: 0x1A

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................

00 00 00 00 00 00 00 00 00 00 ..........

[**] Tiny Fragments - Possible Hostile Activity [**]

05/22-19:08:22.775812 202.102.20.10 -> 192.168.1.132

TCP TTL:109 TOS:0x0 ID:34824 DF MF

Frag Offset: 0x0 Frag Size: 0x1A

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................

00 00 00 00 00 00 00 00 00 00 ..........

[**] Tiny Fragments - Possible Hostile Activity [**]

05/22-19:08:22.965729 202.102.20.10 -> 192.168.1.132

TCP TTL:109 TOS:0x0 ID:35080 DF MF

Frag Offset: 0x0 Frag Size: 0x1A

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
```

```
00 00 00 00 00 00 00 00 00 00 ..........
```

Return to Detect 6

DETECT 7 DATA

```
[**] Webdist CGI access attempt [**]
05/26-18:16:26.013643 209.240.161.252:21041 -> 192.168.1.68:80
TCP TTL:45 TOS:0x0 ID:25761 DF
*****PA* Seq: 0x49BD43E4 Ack: 0xB12AE032 Win: 0x3EBC
TCP Options => NOP NOP TS: 14850272 1303415
48 45 41 44 20 2F 63 67 69 2D 62 69 6E 2F 77 65 HEAD /cgi-bin/we
62 64 69 73 74 2E 63 67 69 20 48 54 54 50 2F 31 bdist.cgi HTTP/1
2E 30 0D 0A 55 73 65 72 2D 41 67 65 6E 74 3A 20 .0..User-Agent:
4D 6F 7A 69 6C 6C 61 2F 34 2E 37 20 5B 65 6E 5D Mozilla/4.7 [en]
20 28 57 69 6E 39 35 3B 20 55 29 0D 0A 52 65 66 (Win95; U)..Ref
65 72 65 72 3A 20 68 74 74 70 3A 2F 2F 6F 70 65 erer: http://ope
6E 62 73 64 2E 72 6F 6F 74 77 61 72 2E 63 6F 6D nbsd.rootwar.com
2F 0D 0A 43 6F 6E 6E 65 63 74 69 6F 6E 3A 20 63 /..Connection: c
6C 6F 73 65 0D 0A 0D 0A lose....
[**] HANDLER probe! [**]
05/26-18:16:26.552381 209.240.161.252:21042 -> 192.168.1.68:80
TCP TTL:45 TOS:0x0 ID:25769 DF
*****PA* Seq: 0x498E7F08 Ack: 0xB12E02B1 Win: 0x3EBC
TCP Options => NOP NOP TS: 14850325 1303416
48 45 41 44 20 2F 63 67 69 2D 62 69 6E 2F 68 61 HEAD /cgi-bin/ha
6E 64 6C 65 72 20 48 54 54 50 2F 31 2E 30 0D 0A ndler HTTP/1.0..
55 73 65 72 2D 41 67 65 6E 74 3A 20 4D 6F 7A 69 User-Agent: Mozi
6C 6C 61 2F 34 2E 37 20 5B 65 6E 5D 20 28 57 69 lla/4.7 [en] (Wi
6E 39 35 3B 20 55 29 0D 0A 52 65 66 65 72 65 72 n95; U)..Referer
3A 20 68 74 74 70 3A 2F 2F 6F 70 65 6E 62 73 64 : http://openbsd
```

```
2E 72 6F 6F 74 77 61 72 2E 63 6F 6D 2F 0D 0A 43 .rootwar.com/..C
6F 6E 6E 65 63 74 69 6F 6E 3A 20 63 6C 6F 73 65 onnection: close
0D 0A 0D 0A ....
[**] Wrap CGI access attempt [**]
05/26-18:16:27.092688 209.240.161.252:21043 -> 192.168.1.68:80
TCP TTL:45 TOS:0x0 ID:25776 DF
*****PA* Seq: 0x4A157979 Ack: 0xB12F2390 Win: 0x3EBC
TCP Options => NOP NOP TS: 14850379 1303417
48 45 41 44 20 2F 63 67 69 2D 62 69 6E 2F 77 72 HEAD /cgi-bin/wr
61 70 20 48 54 54 50 2F 31 2E 30 0D 0A 55 73 65 ap HTTP/1.0..Use
72 2D 41 67 65 6E 74 3A 20 4D 6F 7A 69 6C 6C 61 r-Agent: Mozilla
2F 34 2E 37 20 5B 65 6E 5D 20 28 57 69 6E 39 35 /4.7 [en] (Win95
3B 20 55 29 0D 0A 52 65 66 65 72 65 72 3A 20 68 ; U)..Referer: h
74 74 70 3A 2F 2F 6F 70 65 6E 62 73 64 2E 72 6F ttp://openbsd.ro
6F 74 77 61 72 2E 63 6F 6D 2F 0D 0A 43 6F 6E 6E otwar.com/..Conn
65 63 74 69 6F 6E 3A 20 63 6C 6F 73 65 0D 0A 0D ection: close...
0A .
[**] CGI pfdisplay access attempt [**]
05/26-18:16:27.602703 209.240.161.252:21044 -> 192.168.1.68:80
TCP TTL:45 TOS:0x0 ID:25785 DF
*****PA* Seq: 0x496E71F7 Ack: 0xB1310070 Win: 0x3EBC
TCP Options => NOP NOP TS: 14850431 1303418
48 45 41 44 20 2F 63 67 69 2D 62 69 6E 2F 70 66 HEAD /cgi-bin/pf
64 69 73 70 6C 61 79 2E 63 67 69 20 48 54 54 50 display.cgi HTTP
2F 31 2E 30 0D 0A 55 73 65 72 2D 41 67 65 6E 74 /1.0..User-Agent
3A 20 4D 6F 7A 69 6C 6C 61 2F 34 2E 37 20 5B 65 : Mozilla/4.7 [e
6E 5D 20 28 57 69 6E 39 35 3B 20 55 29 0D 0A 52 n] (Win95; U)..R
65 66 65 72 65 72 3A 20 68 74 74 70 3A 2F 2F 6F eferer: http://o
70 65 6E 62 73 64 2E 72 6F 6F 74 77 61 72 2E 63 penbsd.rootwar.c
6F 6D 2F 0D 0A 43 6F 6E 6E 65 63 74 69 6F 6E 3A om/..Connection:
```

```
20 63 6C 6F 73 65 0D 0A 0D 0A close....
[**] Perlshop CGI access attempt [**]
05/26-18:16:37.732802 209.240.161.252:21063 -> 192.168.1.68:80
TCP TTL:45 TOS:0x0 ID:25907 DF
*****PA* Seq: 0x4A9E9622 Ack: 0xB15B86FE Win: 0x3EBC
TCP Options => NOP NOP TS: 14851443 1303438
48 45 41 44 20 2F 63 67 69 2D 62 69 6E 2F 70 65 HEAD /cgi-bin/pe
72 6C 73 68 6F 70 2E 63 67 69 20 48 54 54 50 2F rlshop.cgi HTTP/
31 2E 30 0D 0A 55 73 65 72 2D 41 67 65 6E 74 3A 1.0..User-Agent:
20 4D 6F 7A 69 6C 6C 61 2F 34 2E 37 20 5B 65 6E Mozilla/4.7 [en
5D 20 28 57 69 6E 39 35 3B 20 55 29 0D 0A 52 65 ] (Win95; U)..Re
66 65 72 65 72 3A 20 68 74 74 70 3A 2F 2F 6F 70 ferer: http://op
65 6E 62 73 64 2E 72 6F 6F 74 77 61 72 2E 63 6F enbsd.rootwar.co
6D 2F 0D 0A 43 6F 6E 6E 65 63 74 69 6F 6E 3A 20 m/..Connection:
63 6C 6F 73 65 0D 0A 0D 0A close....
[**] Bnbform CGI access attempt [**]
05/26-18:16:38.832511 209.240.161.252:21065 -> 192.168.1.68:80
TCP TTL:45 TOS:0x0 ID:25920 DF
*****PA* Seq: 0x4A3C8B93 Ack: 0xB15E2181 Win: 0x3EBC
TCP Options => NOP NOP TS: 14851554 1303440
48 45 41 44 20 2F 63 67 69 2D 62 69 6E 2F 62 6E HEAD /cgi-bin/bn
62 66 6F 72 6D 2E 63 67 69 20 48 54 54 50 2F 31 bform.cgi HTTP/1
2E 30 0D 0A 55 73 65 72 2D 41 67 65 6E 74 3A 20 .0..User-Agent:
4D 6F 7A 69 6C 6C 61 2F 34 2E 37 20 5B 65 6E 5D Mozilla/4.7 [en]
20 28 57 69 6E 39 35 3B 20 55 29 0D 0A 52 65 66 (Win95; U)..Ref
65 72 65 72 3A 20 68 74 74 70 3A 2F 2F 6F 70 65 erer: http://ope
6E 62 73 64 2E 72 6F 6F 74 77 61 72 2E 63 6F 6D nbsd.rootwar.com
2F 0D 0A 43 6F 6E 6E 65 63 74 69 6F 6E 3A 20 63 /..Connection: c
6C 6F 73 65 0D 0A 0D 0A lose....
```

```
[**] rwwwshell CGI access attempt [**]
05/26-18:16:39.891908 209.240.161.252:21067 -> 192.168.1.68:80
TCP TTL:45 TOS:0x0 ID:25933 DF
*****PA* Seq: 0x4B942813 Ack: 0xB1643C8D Win: 0x3EBC
TCP Options => NOP NOP TS: 14851660 1303443
48 45 41 44 20 2F 63 67 69 2D 62 69 6E 2F 72 77 HEAD /cgi-bin/rw
77 77 73 68 65 6C 6C 2E 70 6C 20 48 54 54 50 2F wwshell.pl HTTP/
31 2E 30 0D 0A 55 73 65 72 2D 41 67 65 6E 74 3A 1.0..User-Agent:
20 4D 6F 7A 69 6C 6C 61 2F 34 2E 37 20 5B 65 6E Mozilla/4.7 [en
5D 20 28 57 69 6E 39 35 3B 20 55 29 0D 0A 52 65 ] (Win95; U)..Re
66 65 72 65 72 3A 20 68 74 74 70 3A 2F 2F 6F 70 ferer: http://op
65 6E 62 73 64 2E 72 6F 6F 74 77 61 72 2E 63 6F enbsd.rootwar.co
6D 2F 0D 0A 43 6F 6E 6E 65 63 74 69 6F 6E 3A 20 m/..Connection:
63 6C 6F 73 65 0D 0A 0D 0A close....
[**] IIS Search97 access attempt [**]
05/26-18:16:51.095284 209.240.161.252:21088 -> 192.168.1.68:80
TCP TTL:45 TOS:0x0 ID:26062 DF
*****PA* Seq: 0x4CB18B83 Ack: 0xB18D296E Win: 0x3EBC
TCP Options => NOP NOP TS: 14852780 1303465
48 45 41 44 20 2F 73 65 61 72 63 68 39 37 2E 76 HEAD /search97.v
74 73 20 48 54 54 50 2F 31 2E 30 0D 0A 55 73 65 ts HTTP/1.0..Use
72 2D 41 67 65 6E 74 3A 20 4D 6F 7A 69 6C 6C 61 r-Agent: Mozilla
2F 34 2E 37 20 5B 65 6E 5D 20 28 57 69 6E 39 35 /4.7 [en] (Win95
3B 20 55 29 0D 0A 52 65 66 65 72 65 72 3A 20 68 ; U)..Referer: h
74 74 70 3A 2F 2F 6F 70 65 6E 62 73 64 2E 72 6F ttp://openbsd.ro
6F 74 77 61 72 2E 63 6F 6D 2F 0D 0A 43 6F 6E 6E otwar.com/..Conn
65 63 74 69 6F 6E 3A 20 63 6C 6F 73 65 0D 0A 0D ection: close...
0A .
[**] TEST-CGI probe! [**]
05/26-18:16:52.171655 209.240.161.252:21090 -> 192.168.1.68:80
```

```
TCP TTL:45 TOS:0x0 ID:26074 DF
*****PA* Seq: 0x4C56CA20 Ack: 0xB1913FC6 Win: 0x3EBC
TCP Options => NOP NOP TS: 14852888 1303467
48 45 41 44 20 2F 63 67 69 2D 62 69 6E 2F 74 65 HEAD /cgi-bin/te
73 74 2D 63 67 69 20 48 54 54 50 2F 31 2E 30 0D st-cgi HTTP/1.0.
0A 55 73 65 72 2D 41 67 65 6E 74 3A 20 4D 6F 7A .User-Agent: Moz
69 6C 6C 61 2F 34 2E 37 20 5B 65 6E 5D 20 28 57 illa/4.7 [en] (W
69 6E 39 35 3B 20 55 29 0D 0A 52 65 66 65 72 65 in95; U)..Refere
72 3A 20 68 74 74 70 3A 2F 2F 6F 70 65 6E 62 73 r: http://openbs
64 2E 72 6F 6F 74 77 61 72 2E 63 6F 6D 2F 0D 0A d.rootwar.com/..
43 6F 6E 6E 65 63 74 69 6F 6E 3A 20 63 6C 6F 73 Connection: clos
65 0D 0A 0D 0A e....
[**] Campas CGI access attempt [**]
05/26-18:16:52.713229 209.240.161.252:21091 -> 192.168.1.68:80
TCP TTL:45 TOS:0x0 ID:26080 DF
*****PA* Seq: 0x4C0EA7CC Ack: 0xB193393F Win: 0x3EBC
TCP Options => NOP NOP TS: 14852941 1303468
48 45 41 44 20 2F 63 67 69 2D 62 69 6E 2F 63 61 HEAD /cgi-bin/ca
6D 70 61 73 20 48 54 54 50 2F 31 2E 30 0D 0A 55 mpas HTTP/1.0..U
73 65 72 2D 41 67 65 6E 74 3A 20 4D 6F 7A 69 6C ser-Agent: Mozil
6C 61 2F 34 2E 37 20 5B 65 6E 5D 20 28 57 69 6E la/4.7 [en] (Win
39 35 3B 20 55 29 0D 0A 52 65 66 65 72 65 72 3A 95; U)..Referer:
20 68 74 74 70 3A 2F 2F 6F 70 65 6E 62 73 64 2E http://openbsd.
72 6F 6F 74 77 61 72 2E 63 6F 6D 2F 0D 0A 43 6F rootwar.com/..Co
6E 6E 65 63 74 69 6F 6E 3A 20 63 6C 6F 73 65 0D nnection: close.
0A 0D 0A ...
[**] WWW-SQL CGI access attempt [**]
05/26-18:16:53.251575 209.240.161.252:21092 -> 192.168.1.68:80
TCP TTL:45 TOS:0x0 ID:26086 DF
```

```
*****PA* Seq: 0x4C5D9309 Ack: 0xB1961370 Win: 0x3EBC
TCP Options => NOP NOP TS: 14852995 1303469
48 45 41 44 20 2F 63 67 69 2D 62 69 6E 2F 77 77 HEAD /cgi-bin/ww
77 2D 73 71 6C 20 48 54 54 50 2F 31 2E 30 0D 0A w-sql HTTP/1.0..
55 73 65 72 2D 41 67 65 6E 74 3A 20 4D 6F 7A 69 User-Agent: Mozi
6C 6C 61 2F 34 2E 37 20 5B 65 6E 5D 20 28 57 69 lla/4.7 [en] (Wi
6E 39 35 3B 20 55 29 0D 0A 52 65 66 65 72 65 72 n95; U)..Referer
3A 20 68 74 74 70 3A 2F 2F 6F 70 65 6E 62 73 64 : http://openbsd
2E 72 6F 6F 74 77 61 72 2E 63 6F 6D 2F 0D 0A 43 .rootwar.com/..C
6F 6E 6E 65 63 74 69 6F 6E 3A 20 63 6C 6F 73 65 onnection: close
0D 0A 0D 0A ....
[**] COUNT.cgi probe! [**]
05/26-18:16:56.931709 209.240.161.252:21095 -> 192.168.1.68:80
TCP TTL:45 TOS:0x0 ID:26128 DF
*****PA* Seq: 0x4C7D9F63 Ack: 0xB1A3D95C Win: 0x3EBC
TCP Options => NOP NOP TS: 14853363 1303477
48 45 41 44 20 2F 63 67 69 2D 62 69 6E 2F 43 6F HEAD /cgi-bin/Co
75 6E 74 2E 63 67 69 20 48 54 54 50 2F 31 2E 30 unt.cgi HTTP/1.0
0D 0A 55 73 65 72 2D 41 67 65 6E 74 3A 20 4D 6F ..User-Agent: Mo
7A 69 6C 6C 61 2F 34 2E 37 20 5B 65 6E 5D 20 28 zilla/4.7 [en] (
57 69 6E 39 35 3B 20 55 29 0D 0A 52 65 66 65 72 Win95; U)..Refer
65 72 3A 20 68 74 74 70 3A 2F 2F 6F 70 65 6E 62 er: http://openb
73 64 2E 72 6F 6F 74 77 61 72 2E 63 6F 6D 2F 0D sd.rootwar.com/.
0A 43 6F 6E 6E 65 63 74 69 6F 6E 3A 20 63 6C 6F .Connection: clo
73 65 0D 0A 0D 0A se....
[**] NPH CGI access attempt [**]
05/26-18:16:57.932439 209.240.161.252:21097 -> 192.168.1.68:80
TCP TTL:45 TOS:0x0 ID:26140 DF
*****PA* Seq: 0x4CF66059 Ack: 0xB1A59F4E Win: 0x3EBC
TCP Options => NOP NOP TS: 14853465 1303479
```

```
48 45 41 44 20 2F 63 67 69 2D 62 69 6E 2F 6E 70 HEAD /cgi-bin/np
68 2D 74 65 73 74 2D 63 67 69 20 48 54 54 50 2F h-test-cgi HTTP/
31 2E 30 0D 0A 55 73 65 72 2D 41 67 65 6E 74 3A 1.0..User-Agent:
20 4D 6F 7A 69 6C 6C 61 2F 34 2E 37 20 5B 65 6E Mozilla/4.7 [en
5D 20 28 57 69 6E 39 35 3B 20 55 29 0D 0A 52 65 ] (Win95; U)..Re
66 65 72 65 72 3A 20 68 74 74 70 3A 2F 2F 6F 70 ferer: http://op
65 6E 62 73 64 2E 72 6F 6F 74 77 61 72 2E 63 6F enbsd.rootwar.co
6D 2F 0D 0A 43 6F 6E 6E 65 63 74 69 6F 6E 3A 20 m/..Connection:
63 6C 6F 73 65 0D 0A 0D 0A close....
[**] Webgais CGI access attempt [**]
05/26-18:16:58.452039 209.240.161.252:21098 -> 192.168.1.68:80
TCP TTL:45 TOS:0x0 ID:26146 DF
*****PA* Seq: 0x4CBE85D7 Ack: 0xB1A5FEBF Win: 0x3EBC
TCP Options => NOP NOP TS: 14853515 1303480
48 45 41 44 20 2F 63 67 69 2D 62 69 6E 2F 77 65 HEAD /cgi-bin/we
62 67 61 69 73 20 48 54 54 50 2F 31 2E 30 0D 0A bgais HTTP/1.0..
55 73 65 72 2D 41 67 65 6E 74 3A 20 4D 6F 7A 69 User-Agent: Mozi
6C 6C 61 2F 34 2E 37 20 5B 65 6E 5D 20 28 57 69 lla/4.7 [en] (Wi
6E 39 35 3B 20 55 29 0D 0A 52 65 66 65 72 65 72 n95; U)..Referer
3A 20 68 74 74 70 3A 2F 2F 6F 70 65 6E 62 73 64 : http://openbsd
2E 72 6F 6F 74 77 61 72 2E 63 6F 6D 2F 0D 0A 43 .rootwar.com/..C
6F 6E 6E 65 63 74 69 6F 6E 3A 20 63 6C 6F 73 65 onnection: close
0D 0A 0D 0A ....
[**] Websendmail CGI access attempt [**]
05/26-18:16:58.962019 209.240.161.252:21099 -> 192.168.1.68:80
TCP TTL:45 TOS:0x0 ID:26152 DF
*****PA* Seq: 0x4C3B515F Ack: 0xB1A9B246 Win: 0x3EBC
TCP Options => NOP NOP TS: 14853567 1303481
48 45 41 44 20 2F 63 67 69 2D 62 69 6E 2F 77 65 HEAD /cgi-bin/we
```

```
62 73 65 6E 64 6D 61 69 6C 20 48 54 54 50 2F 31 bsendmail HTTP/1
2E 30 0D 0A 55 73 65 72 2D 41 67 65 6E 74 3A 20 .0..User-Agent:
4D 6F 7A 69 6C 6C 61 2F 34 2E 37 20 5B 65 6E 5D Mozilla/4.7 [en]
20 28 57 69 6E 39 35 3B 20 55 29 0D 0A 52 65 66 (Win95; U)..Ref
65 72 65 72 3A 20 68 74 74 70 3A 2F 2F 6F 70 65 erer: http://ope
6E 62 73 64 2E 72 6F 6F 74 77 61 72 2E 63 6F 6D nbsd.rootwar.com
2F 0D 0A 43 6F 6E 6E 65 63 74 69 6F 6E 3A 20 63 /..Connection: c
6C 6F 73 65 0D 0A 0D 0A lose....
[**] FAXSURVEY probe! [**]
05/26-18:17:00.532801 209.240.161.252:21102 -> 192.168.1.68:80
TCP TTL:45 TOS:0x0 ID:26170 DF
*****PA* Seq: 0x4C6396EF Ack: 0xB1AE1759 Win: 0x3EBC
TCP Options => NOP NOP TS: 14853725 1303484
48 45 41 44 20 2F 63 67 69 2D 62 69 6E 2F 66 61 HEAD /cgi-bin/fa
78 73 75 72 76 65 79 20 48 54 54 50 2F 31 2E 30 xsurvey HTTP/1.0
0D 0A 55 73 65 72 2D 41 67 65 6E 74 3A 20 4D 6F ..User-Agent: Mo
7A 69 6C 6C 61 2F 34 2E 37 20 5B 65 6E 5D 20 28 zilla/4.7 [en] (
57 69 6E 39 35 3B 20 55 29 0D 0A 52 65 66 65 72 Win95; U)..Refer
65 72 3A 20 68 74 74 70 3A 2F 2F 6F 70 65 6E 62 er: http://openb
73 64 2E 72 6F 6F 74 77 61 72 2E 63 6F 6D 2F 0D sd.rootwar.com/.
0A 43 6F 6E 6E 65 63 74 69 6F 6E 3A 20 63 6C 6F .Connection: clo
73 65 0D 0A 0D 0A se....
[**] Htmlscript CGI access attempt [**]
05/26-18:17:01.052516 209.240.161.252:21103 -> 192.168.1.68:80
TCP TTL:45 TOS:0x0 ID:26176 DF
*****PA* Seq: 0x4D3EB88F Ack: 0xB1B118C2 Win: 0x3EBC
TCP Options => NOP NOP TS: 14853776 1303485
48 45 41 44 20 2F 63 67 69 2D 62 69 6E 2F 68 74 HEAD /cgi-bin/ht
6D 6C 73 63 72 69 70 74 20 48 54 54 50 2F 31 2E mlscript HTTP/1.
30 0D 0A 55 73 65 72 2D 41 67 65 6E 74 3A 20 4D 0..User-Agent: M
```

```
6F 7A 69 6C 6C 61 2F 34 2E 37 20 5B 65 6E 5D 20 ozilla/4.7 [en]
28 57 69 6E 39 35 3B 20 55 29 0D 0A 52 65 66 65 (Win95; U)..Refe
72 65 72 3A 20 68 74 74 70 3A 2F 2F 6F 70 65 6E rer: http://open
62 73 64 2E 72 6F 6F 74 77 61 72 2E 63 6F 6D 2F bsd.rootwar.com/
0D 0A 43 6F 6E 6E 65 63 74 69 6F 6E 3A 20 63 6C ..Connection: cl
6F 73 65 0D 0A 0D 0A ose....
[**] Aglimpse CGI access attempt [**]
05/26-18:17:01.572511 209.240.161.252:21104 -> 192.168.1.68:80
TCP TTL:45 TOS:0x0 ID:26182 DF
*****PA* Seq: 0x4CFAB515 Ack: 0xB1B2CF20 Win: 0x3EBC
TCP Options => NOP NOP TS: 14853827 1303486
48 45 41 44 20 2F 63 67 69 2D 62 69 6E 2F 61 67 HEAD /cgi-bin/ag
6C 69 6D 70 73 65 20 48 54 54 50 2F 31 2E 30 0D limpse HTTP/1.0.
0A 55 73 65 72 2D 41 67 65 6E 74 3A 20 4D 6F 7A .User-Agent: Moz
69 6C 6C 61 2F 34 2E 37 20 5B 65 6E 5D 20 28 57 illa/4.7 [en] (W
69 6E 39 35 3B 20 55 29 0D 0A 52 65 66 65 72 65 in95; U)..Refere
72 3A 20 68 74 74 70 3A 2F 2F 6F 70 65 6E 62 73 r: http://openbs
64 2E 72 6F 6F 74 77 61 72 2E 63 6F 6D 2F 0D 0A d.rootwar.com/..
43 6F 6E 6E 65 63 74 69 6F 6E 3A 20 63 6C 6F 73 Connection: clos
65 0D 0A 0D 0A e....
[**] CGI Man access attempt [**]
05/26-18:17:02.083209 209.240.161.252:21105 -> 192.168.1.68:80
TCP TTL:45 TOS:0x0 ID:26188 DF
*****PA* Seq: 0x4D0E574E Ack: 0xB1B3AF76 Win: 0x3EBC
TCP Options => NOP NOP TS: 14853880 1303487
48 45 41 44 20 2F 63 67 69 2D 62 69 6E 2F 6D 61 HEAD /cgi-bin/ma
6E 2E 73 68 20 48 54 54 50 2F 31 2E 30 0D 0A 55 n.sh HTTP/1.0..U
73 65 72 2D 41 67 65 6E 74 3A 20 4D 6F 7A 69 6C ser-Agent: Mozil
6C 61 2F 34 2E 37 20 5B 65 6E 5D 20 28 57 69 6E la/4.7 [en] (Win
```

```
39 35 3B 20 55 29 0D 0A 52 65 66 65 72 65 72 3A 95; U)..Referer:
20 68 74 74 70 3A 2F 2F 6F 70 65 6E 62 73 64 2E http://openbsd.
72 6F 6F 74 77 61 72 2E 63 6F 6D 2F 0D 0A 43 6F rootwar.com/..Co
6E 6E 65 63 74 69 6F 6E 3A 20 63 6C 6F 73 65 0D nnection: close.
0A 0D 0A ...
[**] Filemail CGI access attempt [**]
05/26-18:17:03.211742 209.240.161.252:21107 -> 192.168.1.68:80
TCP TTL:45 TOS:0x0 ID:26201 DF
*****PA* Seq: 0x4CEC3B2C Ack: 0xB1B815B9 Win: 0x3EBC
TCP Options => NOP NOP TS: 14853992 1303489
48 45 41 44 20 2F 63 67 69 2D 62 69 6E 2F 66 69 HEAD /cgi-bin/fi
6C 65 6D 61 69 6C 2E 70 6C 20 48 54 54 50 2F 31 lemail.pl HTTP/1
2E 30 0D 0A 55 73 65 72 2D 41 67 65 6E 74 3A 20 .0..User-Agent:
4D 6F 7A 69 6C 6C 61 2F 34 2E 37 20 5B 65 6E 5D Mozilla/4.7 [en]
20 28 57 69 6E 39 35 3B 20 55 29 0D 0A 52 65 66 (Win95; U)..Ref
65 72 65 72 3A 20 68 74 74 70 3A 2F 2F 6F 70 65 erer: http://ope
6E 62 73 64 2E 72 6F 6F 74 77 61 72 2E 63 6F 6D nbsd.rootwar.com
2F 0D 0A 43 6F 6E 6E 65 63 74 69 6F 6E 3A 20 63 /..Connection: c
6C 6F 73 65 0D 0A 0D 0A lose....
[**] JJ CGI access attempt [**]
05/26-18:17:04.282152 209.240.161.252:21109 -> 192.168.1.68:80
TCP TTL:45 TOS:0x0 ID:26213 DF
*****PA* Seq: 0x4D594CD0 Ack: 0xB1BC2D7E Win: 0x3EBC
TCP Options => NOP NOP TS: 14854101 1303491
48 45 41 44 20 2F 63 67 69 2D 62 69 6E 2F 6A 6A HEAD /cgi-bin/jj
20 48 54 54 50 2F 31 2E 30 0D 0A 55 73 65 72 2D HTTP/1.0..User-
41 67 65 6E 74 3A 20 4D 6F 7A 69 6C 6C 61 2F 34 Agent: Mozilla/4
2E 37 20 5B 65 6E 5D 20 28 57 69 6E 39 35 3B 20 .7 [en] (Win95;
55 29 0D 0A 52 65 66 65 72 65 72 3A 20 68 74 74 U)..Referer: htt
70 3A 2F 2F 6F 70 65 6E 62 73 64 2E 72 6F 6F 74 p://openbsd.root
```

```
77 61 72 2E 63 6F 6D 2F 0D 0A 43 6F 6E 6E 65 63 war.com/..Connec
74 69 6F 6E 3A 20 63 6C 6F 73 65 0D 0A 0D 0A tion: close....
[**] Survey CGI access attempt [**]
05/26-18:17:10.282970 209.240.161.252:21110 -> 192.168.1.68:80
TCP TTL:45 TOS:0x0 ID:26279 DF
*****PA* Seq: 0x4D2B4C00 Ack: 0xB1D36A5A Win: 0x3EBC
TCP Options => NOP NOP TS: 14854699 1303503
48 45 41 44 20 2F 63 67 69 2D 62 69 6E 2F 73 75 HEAD /cgi-bin/su
72 76 65 79 2E 63 67 69 20 48 54 54 50 2F 31 2E rvey.cgi HTTP/1.
30 0D 0A 55 73 65 72 2D 41 67 65 6E 74 3A 20 4D 0..User-Agent: M
6F 7A 69 6C 6C 61 2F 34 2E 37 20 5B 65 6E 5D 20 ozilla/4.7 [en]
28 57 69 6E 39 35 3B 20 55 29 0D 0A 52 65 66 65 (Win95; U)..Refe
72 65 72 3A 20 68 74 74 70 3A 2F 2F 6F 70 65 6E rer: http://open
62 73 64 2E 72 6F 6F 74 77 61 72 2E 63 6F 6D 2F bsd.rootwar.com/
0D 0A 43 6F 6E 6E 65 63 74 69 6F 6E 3A 20 63 6C ..Connection: cl
6F 73 65 0D 0A 0D 0A ose....
[**] Environ CGI access attempt [**]
05/26-18:17:11.360883 209.240.161.252:21112 -> 192.168.1.68:80
TCP TTL:45 TOS:0x0 ID:26291 DF
*****PA* Seq: 0x4D196EED Ack: 0xB1D70A66 Win: 0x3EBC
TCP Options => NOP NOP TS: 14854807 1303505
48 45 41 44 20 2F 63 67 69 2D 62 69 6E 2F 65 6E HEAD /cgi-bin/en
76 69 72 6F 6E 2E 63 67 69 20 48 54 54 50 2F 31 viron.cgi HTTP/1
2E 30 0D 0A 55 73 65 72 2D 41 67 65 6E 74 3A 20 .0..User-Agent:
4D 6F 7A 69 6C 6C 61 2F 34 2E 37 20 5B 65 6E 5D Mozilla/4.7 [en]
20 28 57 69 6E 39 35 3B 20 55 29 0D 0A 52 65 66 (Win95; U)..Ref
65 72 65 72 3A 20 68 74 74 70 3A 2F 2F 6F 70 65 erer: http://ope
6E 62 73 64 2E 72 6F 6F 74 77 61 72 2E 63 6F 6D nbsd.rootwar.com
2F 0D 0A 43 6F 6E 6E 65 63 74 69 6F 6E 3A 20 63 /..Connection: c
```

```
6C 6F 73 65 0D 0A 0D 0A lose....

[**] Finger CGI access attempt [**]

05/26-18:17:12.372264 209.240.161.252:21114 -> 192.168.1.68:80

TCP TTL:45 TOS:0x0 ID:26303 DF

*****PA* Seq: 0x4D00B201 Ack: 0xB1DC3371 Win: 0x3EBC

TCP Options => NOP NOP TS: 14854908 1303508

48 45 41 44 20 2F 63 67 69 2D 62 69 6E 2F 66 69 HEAD /cgi-bin/fi

6E 67 65 72 20 48 54 54 50 2F 31 2E 30 0D 0A 55 nger HTTP/1.0..U

73 65 72 2D 41 67 65 6E 74 3A 20 4D 6F 7A 69 6C ser-Agent: Mozil

6C 61 2F 34 2E 37 20 5B 65 6E 5D 20 28 57 69 6E la/4.7 [en] (Win

39 35 3B 20 55 29 0D 0A 52 65 66 65 72 65 72 3A 95; U)..Referer:

20 68 74 74 70 3A 2F 2F 6F 70 65 6E 62 73 64 2E http://openbsd.

72 6F 6F 74 77 61 72 2E 63 6F 6D 2F 0D 0A 43 6F rootwar.com/..Co

6E 6E 65 63 74 69 6F 6E 3A 20 63 6C 6F 73 65 0D nnection: close.

0A 0D 0A ...

[**] Finger CGI access attempt [**]

05/26-18:17:12.891814 209.240.161.252:21115 -> 192.168.1.68:80

TCP TTL:45 TOS:0x0 ID:26309 DF

*****PA* Seq: 0x4D8840F4 Ack: 0xB1DE7E39 Win: 0x3EBC

TCP Options => NOP NOP TS: 14854960 1303509

48 45 41 44 20 2F 63 67 69 2D 62 69 6E 2F 66 69 HEAD /cgi-bin/fi

6E 67 65 72 2E 70 6C 20 48 54 54 50 2F 31 2E 30 nger.pl HTTP/1.0

0D 0A 55 73 65 72 2D 41 67 65 6E 74 3A 20 4D 6F ..User-Agent: Mo

7A 69 6C 6C 61 2F 34 2E 37 20 5B 65 6E 5D 20 28 zilla/4.7 [en] (

57 69 6E 39 35 3B 20 55 29 0D 0A 52 65 66 65 72 Win95; U)..Refer

65 72 3A 20 68 74 74 70 3A 2F 2F 6F 70 65 6E 62 er: http://openb

73 64 2E 72 6F 6F 74 77 61 72 2E 63 6F 6D 2F 0D sd.rootwar.com/.

0A 43 6F 6E 6E 65 63 74 69 6F 6E 3A 20 63 6C 6F .Connection: clo

73 65 0D 0A 0D 0A se....

[**] Finger CGI access attempt [**]
```

```
05/26-18:17:13.402188 209.240.161.252:21116 -> 192.168.1.68:80
TCP TTL:45 TOS:0x0 ID:26315 DF
*****PA* Seq: 0x4D741E92 Ack: 0xB1DFBC81 Win: 0x3EBC
TCP Options => NOP NOP TS: 14855012 1303510
48 45 41 44 20 2F 63 67 69 2D 62 69 6E 2F 66 69 HEAD /cgi-bin/fi
6E 67 65 72 2E 63 67 69 20 48 54 54 50 2F 31 2E nger.cgi HTTP/1.
30 0D 0A 55 73 65 72 2D 41 67 65 6E 74 3A 20 4D 0..User-Agent: M
6F 7A 69 6C 6C 61 2F 34 2E 37 20 5B 65 6E 5D 20 ozilla/4.7 [en]
28 57 69 6E 39 35 3B 20 55 29 0D 0A 52 65 66 65 (Win95; U)..Refe
72 65 72 3A 20 68 74 74 70 3A 2F 2F 6F 70 65 6E rer: http://open
62 73 64 2E 72 6F 6F 74 77 61 72 2E 63 6F 6D 2F bsd.rootwar.com/
0D 0A 43 6F 6E 6E 65 63 74 69 6F 6E 3A 20 63 6C ..Connection: cl
6F 73 65 0D 0A 0D 0A ose....
[**] Maillist CGI access attempt [**]
05/26-18:17:13.922179 209.240.161.252:21117 -> 192.168.1.68:80
TCP TTL:45 TOS:0x0 ID:26321 DF
*****PA* Seq: 0x4E0281FC Ack: 0xB1E21854 Win: 0x3EBC
TCP Options => NOP NOP TS: 14855063 1303511
48 45 41 44 20 2F 63 67 69 2D 62 69 6E 2F 6D 61 HEAD /cgi-bin/ma
69 6C 6C 69 73 74 2E 70 6C 20 48 54 54 50 2F 31 illist.pl HTTP/1
2E 30 0D 0A 55 73 65 72 2D 41 67 65 6E 74 3A 20 .0..User-Agent:
4D 6F 7A 69 6C 6C 61 2F 34 2E 37 20 5B 65 6E 5D Mozilla/4.7 [en]
20 28 57 69 6E 39 35 3B 20 55 29 0D 0A 52 65 66 (Win95; U)..Ref
65 72 65 72 3A 20 68 74 74 70 3A 2F 2F 6F 70 65 erer: http://ope
6E 62 73 64 2E 72 6F 6F 74 77 61 72 2E 63 6F 6D nbsd.rootwar.com
2F 0D 0A 43 6F 6E 6E 65 63 74 69 6F 6E 3A 20 63 /..Connection: c
6C 6F 73 65 0D 0A 0D 0A lose....
[**] MISC-DNS-version-query [**]
05/26-18:18:51.117869 209.240.161.252:1024 -> 192.168.1.68:53
```

```
UDP TTL:45 TOS:0x0 ID:26500

Len: 38

B3 4C 01 80 00 01 00 00 00 00 00 00 07 76 65 72 .L...........ver

73 69 6F 6E 04 62 69 6E 64 00 00 10 00 03 sion.bind.....
```

Return to Detect 7

DETECT 8 DATA

```
[**] Whisker stealth CGI scan- GET [**]

06/03-21:10:19.290979 216.76.208.89:1594 -> 192.168.1.66:80

TCP TTL:45 TOS:0x0 ID:45364 DF

*****PA* Seq: 0x557D30B4 Ack: 0x40542296 Win: 0x7D78

47 45 54 20 2F 73 61 6D 70 6C 65 73 20 48 54 54 GET /samples HTT

50 2F 31 2E 30 0D 0A 48 6F 73 74 3A 20 77 69 6E P/1.0..Host: win

64 6F 77 73 2E 65 76 69 6C 73 63 61 6E 2E 63 6F dows.evilscan.co

6D 0D 0A 41 63 63 65 70 74 3A 20 74 65 78 74 2F m..Accept: text/

68 74 6D 6C 2C 20 74 65 78 74 2F 70 6C 61 69 6E html, text/plain

2C 20 3F 2C 20 61 75 64 69 6F 2F 78 2D 70 6E 2D , ?, audio/x-pn-

72 65 61 6C 61 75 64 69 6F 2C 20 61 75 64 69 6F realaudio, audio

2F 6D 6F 64 2C 20 69 6D 61 67 65 2F 2A 2C 20 76 /mod, image/*, v

69 64 65 6F 2F 2A 2C 20 76 69 64 65 6F 2F 6D 70 ideo/*, video/mp

65 67 2C 20 61 70 70 6C 69 63 61 74 69 6F 6E 2F eg, application/

70 67 70 2C 20 61 70 70 6C 69 63 61 74 69 6F 6E pgp, application

2F 70 67 70 2C 20 61 70 70 6C 69 63 61 74 69 6F /pgp, applicatio

6E 2F 70 64 66 2C 20 6D 65 73 73 61 67 65 2F 70 n/pdf, message/p

61 72 74 69 61 6C 2C 20 6D 65 73 73 61 67 65 2F artial, message/

65 78 74 65 72 6E 61 6C 2D 62 6F 64 79 2C 20 61 external-body, a

70 70 6C 69 63 61 74 69 6F 6E 2F 70 6F 73 74 73 pplication/posts

63 72 69 70 74 2C 20 78 2D 62 65 32 2C 20 61 70 cript, x-be2, ap

70 6C 69 63 61 74 69 6F 6E 2F 61 6E 64 72 65 77 plication/andrew

2D 69 6E 73 65 74 0D 0A 41 63 63 65 70 74 3A 20 -inset..Accept:
```

```
74 65 78 74 2F 72 69 63 68 74 65 78 74 2C 20 74 text/richtext, t
65 78 74 2F 65 6E 72 69 63 68 65 64 2C 20 78 2D ext/enriched, x-
73 75 6E 2D 61 74 74 61 63 68 6D 65 6E 74 2C 20 sun-attachment,
61 75 64 69 6F 2D 66 69 6C 65 2C 20 70 6F 73 74 audio-file, post
73 63 72 69 70 74 2D 66 69 6C 65 2C 20 64 65 66 script-file, def
61 75 6C 74 2C 20 6D 61 69 6C 2D 66 69 6C 65 2C ault, mail-file,
20 73 75 6E 2D 64 65 73 6B 73 65 74 2D 6D 65 73  sun-deskset-mes
73 61 67 65 2C 20 61 70 70 6C 69 63 61 74 69 6F sage, applicatio
6E 2F 78 2D 6D 65 74 61 6D 61 69 6C 2D 70 61 74 n/x-metamail-pat
63 68 2C 20 74 65 78 74 2F 73 67 6D 6C 2C 20 76 ch, text/sgml, v
69 64 65 6F 2F 6D 70 65 67 2C 20 69 6D 61 67 65 ideo/mpeg, image
2F 6A 70 65 67 2C 20 69 6D 61 67 65 2F 74 69 66 /jpeg, image/tif
66 2C 20 69 6D 61 67 65 2F 78 2D 72 67 62 2C 20 f, image/x-rgb,
69 6D 61 67 65 2F 70 6E 67 2C 20 69 6D 61 67 65 image/png, image
2F 78 2D 78 62 69 74 6D 61 70 0D 0A 41 63 63 65 /x-xbitmap..Acce
70 74 3A 20 69 6D 61 67 65 2F 78 2D 78 62 6D 2C pt: image/x-xbm,
20 69 6D 61 67 65 2F 67 69 66 2C 20 61 70 70 6C  image/gif, appl
69 63 61 74 69 6F 6E 2F 70 6F 73 74 73 63 72 69 ication/postscri
70 74 2C 20 2A 2F 2A 3B 71 3D 30 2E 30 31 0D 0A pt, */*;q=0.01..
41 63 63 65 70 74 2D 45 6E 63 6F 64 69 6E 67 3A Accept-Encoding:
20 67 7A 69 70 2C 20 63 6F 6D 70 72 65 73 73 0D  gzip, compress.
0A 41 63 63 65 70 74 2D 4C 61 6E 67 75 61 67 65 .Accept-Language
3A 20 65 6E 0D 0A 55 73 65 72 2D 41 67 65 6E 74 : en..User-Agent
3A 20 4C 79 6E 78 2F 32 2E 38 2E 33 64 65 76 2E : Lynx/2.8.3dev.
31 38 20 6C 69 62 77 77 77 2D 46 4D 2F 32 2E 31 18 libwww-FM/2.1
34 0D 0A 0D 0A 4....
```

```
[**] Whisker stealth CGI scan- GET [**]
06/03-21:10:23.029520 216.76.208.89:1595 -> 192.168.1.66:80
TCP TTL:45 TOS:0x0 ID:45371 DF
```

```
*****PA* Seq: 0x55D61312 Ack: 0x4054317D Win: 0x7D78

47 45 54 20 2F 73 61 6D 70 6C 65 73 2F 20 48 54 GET /samples/ HT
54 50 2F 31 2E 30 0D 0A 48 6F 73 74 3A 20 77 69 TP/1.0..Host: wi
6E 64 6F 77 73 2E 65 76 69 6C 73 63 61 6E 2E 63 ndows.evilscan.c
6F 6D 0D 0A 41 63 63 65 70 74 3A 20 74 65 78 74 om..Accept: text
2F 68 74 6D 6C 2C 20 74 65 78 74 2F 70 6C 61 69 /html, text/plai
6E 2C 20 3F 2C 20 61 75 64 69 6F 2F 78 2D 70 6E n, ?, audio/x-pn
2D 72 65 61 6C 61 75 64 69 6F 2C 20 61 75 64 69 -realaudio, audi
6F 2F 6D 6F 64 2C 20 69 6D 61 67 65 2F 2A 2C 20 o/mod, image/*,
76 69 64 65 6F 2F 2A 2C 20 76 69 64 65 6F 2F 6D video/*, video/m
70 65 67 2C 20 61 70 70 6C 69 63 61 74 69 6F 6E peg, application
2F 70 67 70 2C 20 61 70 70 6C 69 63 61 74 69 6F /pgp, applicatio
6E 2F 70 67 70 2C 20 61 70 70 6C 69 63 61 74 69 n/pgp, applicati
6F 6E 2F 70 64 66 2C 20 6D 65 73 73 61 67 65 2F on/pdf, message/
70 61 72 74 69 61 6C 2C 20 6D 65 73 73 61 67 65 partial, message
2F 65 78 74 65 72 6E 61 6C 2D 62 6F 64 79 2C 20 /external-body,
61 70 70 6C 69 63 61 74 69 6F 6E 2F 70 6F 73 74 application/post
73 63 72 69 70 74 2C 20 78 2D 62 65 32 2C 20 61 script, x-be2, a
70 70 6C 69 63 61 74 69 6F 6E 2F 61 6E 64 72 65 pplication/andre
77 2D 69 6E 73 65 74 0D 0A 41 63 63 65 70 74 3A w-inset..Accept:
20 74 65 78 74 2F 72 69 63 68 74 65 78 74 2C 20 text/richtext,
74 65 78 74 2F 65 6E 72 69 63 68 65 64 2C 20 78 text/enriched, x
2D 73 75 6E 2D 61 74 74 61 63 68 6D 65 6E 74 2C -sun-attachment,
20 61 75 64 69 6F 2D 66 69 6C 65 2C 20 70 6F 73 audio-file, pos
74 73 63 72 69 70 74 2D 66 69 6C 65 2C 20 64 65 tscript-file, de
66 61 75 6C 74 2C 20 6D 61 69 6C 2D 66 69 6C 65 fault, mail-file
2C 20 73 75 6E 2D 64 65 73 6B 73 65 74 2D 6D 65 , sun-deskset-me
73 73 61 67 65 2C 20 61 70 70 6C 69 63 61 74 69 ssage, applicati
6F 6E 2F 78 2D 6D 65 74 61 6D 61 69 6C 2D 70 61 on/x-metamail-pa
74 63 68 2C 20 74 65 78 74 2F 73 67 6D 6C 2C 20 tch, text/sgml,
```

```
76 69 64 65 6F 2F 6D 70 65 67 2C 20 69 6D 61 67 video/mpeg, imag
65 2F 6A 70 65 67 2C 20 69 6D 61 67 65 2F 74 69 e/jpeg, image/ti
66 66 2C 20 69 6D 61 67 65 2F 78 2D 72 67 62 2C ff, image/x-rgb,
20 69 6D 61 67 65 2F 70 6E 67 2C 20 69 6D 61 67 image/png, imag
65 2F 78 2D 78 62 69 74 6D 61 70 0D 0A 41 63 63 e/x-xbitmap..Acc
65 70 74 3A 20 69 6D 61 67 65 2F 78 2D 78 62 6D ept: image/x-xbm
2C 20 69 6D 61 67 65 2F 67 69 66 2C 20 61 70 70 , image/gif, app
6C 69 63 61 74 69 6F 6E 2F 70 6F 73 74 73 63 72 lication/postscr
69 70 74 2C 20 2A 2F 2A 3B 71 3D 30 2E 30 31 0D ipt, */*;q=0.01.
0A 41 63 63 65 70 74 2D 45 6E 63 6F 64 69 6E 67 .Accept-Encoding
3A 20 67 7A 69 70 2C 20 63 6F 6D 70 72 65 73 73 : gzip, compress
0D 0A 41 63 63 65 70 74 2D 4C 61 6E 67 75 61 67 ..Accept-Languag
65 3A 20 65 6E 0D 0A 55 73 65 72 2D 41 67 65 6E e: en..User-Agen
74 3A 20 4C 79 6E 78 2F 32 2E 38 2E 33 64 65 76 t: Lynx/2.8.3dev
2E 31 38 20 6C 69 62 77 77 77 2D 46 4D 2F 32 2E .18 libwww-FM/2.
31 34 0D 0A 0D 0A 14....
```

Return to Detect 8

DETECT 9 DATA

```
[**] default Backdoor access! [**]
05/27-03:17:53.858530 24.112.191.239:2026 -> 192.168.1.67:1524
TCP TTL:48 TOS:0x0 ID:0 DF
**S***** Seq: 0xDEA100C9 Ack: 0x0 Win: 0x7C70
TCP Options => MSS: 1460 SackOK TS: 1184633 68580781 NOP WS: 0
[**] default Backdoor access! [**]
05/27-03:17:56.137444 24.112.191.239:2027 -> 192.168.1.67:1524
TCP TTL:48 TOS:0x0 ID:0 DF
**S***** Seq: 0xDEB4E077 Ack: 0x0 Win: 0x7C70
TCP Options => MSS: 1460 SackOK TS: 1184861 68580781 NOP WS: 0
```

```
[**] default Backdoor access! [**]

05/27-03:17:58.387281 24.112.191.239:2028 -> 192.168.1.67:1524

TCP TTL:48 TOS:0x0 ID:0 DF

**S***** Seq: 0xDE91057A Ack: 0x0 Win: 0x7C70

TCP Options => MSS: 1460 SackOK TS: 1185086 68580781 NOP WS: 0

***

[**] default Backdoor access! [**]

05/27-03:36:34.942667 24.112.191.239:4147 -> 192.168.1.67:1524

TCP TTL:48 TOS:0x0 ID:0 DF

**S***** Seq: 0x253E7D4D Ack: 0x0 Win: 0x7C70

TCP Options => MSS: 1460 SackOK TS: 1296739 0 NOP WS: 0

[**] default Backdoor access! [**]

05/27-03:36:37.182004 24.112.191.239:4148 -> 192.168.1.67:1524

TCP TTL:48 TOS:0x0 ID:0 DF

**S***** Seq: 0x25C2AAF8 Ack: 0x0 Win: 0x7C70

TCP Options => MSS: 1460 SackOK TS: 1296963 0 NOP WS: 0

[**] default Backdoor access! [**]

05/27-03:36:37.283279 24.112.191.239:4149 -> 192.168.1.67:1524

TCP TTL:48 TOS:0x0 ID:0 DF

**S***** Seq: 0x2583FD4A Ack: 0x0 Win: 0x7C70

TCP Options => MSS: 1460 SackOK TS: 1296973 0 NOP WS: 0

15:14:49 [T] 24.112.191.239 192.168.1.67 [TCP-SCAN]
(total=10,min=23,max=618,up=8,down=2,flags=------S-,May27-15:14,May27-15:14) (dragon)

15:15:01 [T] 24.112.191.239 192.168.1.67 [TCP-SCAN]
(total=500,min=1,max=1024,up=259,down=241,flags=------S-,May27-15:14,May27-15:15)
(dragon)

15:15:13 [T] 24.112.191.239 192.168.1.67 [TCP-SCAN]
(total=499,min=2,max=1023,up=237,down=262,flags=------S-,May27-15:15,May27-15:15)
(dragon)
```

Return to Detect 9

DETECT 10 DATA

```
dragon (Towards) 00:21:51
```

```
SOURCE: 209.64.117.215

DEST: 192.168.1.68 openbsd.evilscan.com

45 00 00 4e 73 07 00 00 71 11 b8 4c d1 40 75 d7 c7 ef 0f 44 E..Ns...q..L.@u....D

00 89 00 89 00 3a b7 f6 e9 ec 00 00 00 01 00 00 00 00 00 00 .....:..............

20 43 4b 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 CKAAAAAAAAAAAAAAAA

41 41 41 41 41 41 41 41 41 41 41 41 41 00 00 21 00 01 AAAAAAAAAAAAA..!..

EVENT1: [SMB:NAME-WILDCARD] (udp,dp=137,sp=137)

dragon (Towards) 00:21:53

SOURCE: 209.64.117.215 209-64-117-215.mastercard.com

DEST: 192.168.1.68 openbsd.evilscan.com

45 00 00 4e 74 07 00 00 71 11 b7 4c d1 40 75 d7 c7 ef 0f 44 E..Nt...q..L.@u....D

00 89 00 89 00 3a b7 f4 e9 ee 00 00 00 01 00 00 00 00 00 00 .....:..............

20 43 4b 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 CKAAAAAAAAAAAAAAAA

41 41 41 41 41 41 41 41 41 41 41 41 41 00 00 21 00 01 AAAAAAAAAAAAA..!..

EVENT1: [SMB:NAME-WILDCARD] (udp,dp=137,sp=137)

dragon (Towards) 00:21:54

SOURCE: 209.64.117.215 209-64-117-215.mastercard.com

DEST: 192.168.1.68 openbsd.evilscan.com

45 00 00 4e 75 07 00 00 71 11 b6 4c d1 40 75 d7 c7 ef 0f 44 E..Nu...q..L.@u....D

00 89 00 89 00 3a b7 f2 e9 f0 00 00 00 01 00 00 00 00 00 00 .....:..............

20 43 4b 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 CKAAAAAAAAAAAAAAAA

41 41 41 41 41 41 41 41 41 41 41 41 41 00 00 21 00 01 AAAAAAAAAAAAA..!..

EVENT1: [SMB:NAME-WILDCARD] (udp,dp=137,sp=137)

dragon (Towards) 00:21:51

SOURCE: 209.64.117.215 209-64-117-215.mastercard.com

DEST: 192.168.1.68 openbsd.evilscan.com

45 00 00 4e 73 07 00 00 71 11 b8 4c d1 40 75 d7 c7 ef 0f 44 E..Ns...q..L.@u....D

00 89 00 89 00 3a b7 f6 e9 ec 00 00 00 01 00 00 00 00 00 00 .....:..............

20 43 4b 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 CKAAAAAAAAAAAAAAAA

41 41 41 41 41 41 41 41 41 41 41 41 41 00 00 21 00 01 AAAAAAAAAAAAA..!..
```

```
EVENT1: [SMB:NAME-WILDCARD] (udp,dp=137,sp=137)
dragon (Towards) 00:21:53
SOURCE: 209.64.117.215 209-64-117-215.mastercard.com
DEST: 192.168.1.68 openbsd.evilscan.com
45 00 00 4e 74 07 00 00 71 11 b7 4c d1 40 75 d7 c7 ef 0f 44 E..Nt...q..L.@u....D
00 89 00 89 00 3a b7 f4 e9 ee 00 00 00 01 00 00 00 00 00 00 .....:..............
20 43 4b 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 CKAAAAAAAAAAAAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 41 00 00 21 00 01 AAAAAAAAAAAAA..!..
EVENT1: [SMB:NAME-WILDCARD] (udp,dp=137,sp=137)
dragon (Towards) 00:21:54
SOURCE: 209.64.117.215 209-64-117-215.mastercard.com
DEST: 192.168.1.68 openbsd.evilscan.com
45 00 00 4e 75 07 00 00 71 11 b6 4c d1 40 75 d7 c7 ef 0f 44 E..Nu...q..L.@u....D
00 89 00 89 00 3a b7 f2 e9 f0 00 00 00 01 00 00 00 00 00 00 .....:..............
20 43 4b 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 CKAAAAAAAAAAAAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 41 00 00 21 00 01 AAAAAAAAAAAAA..!..
EVENT1: [SMB:NAME-WILDCARD] (udp,dp=137,sp=137)
dragon (Towards) 00:21:51
SOURCE: 209.64.117.215 209-64-117-215.mastercard.com
DEST: 192.168.1.68 openbsd.evilscan.com
45 00 00 4e 73 07 00 00 71 11 b8 4c d1 40 75 d7 c7 ef 0f 44 E..Ns...q..L.@u....D
00 89 00 89 00 3a b7 f6 e9 ec 00 00 00 01 00 00 00 00 00 00 .....:..............
20 43 4b 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 CKAAAAAAAAAAAAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 41 00 00 21 00 01 AAAAAAAAAAAAA..!..
EVENT1: [SMB:NAME-WILDCARD] (udp,dp=137,sp=137)
dragon (Towards) 00:21:53
SOURCE: 209.64.117.215 209-64-117-215.mastercard.com
DEST: 192.168.1.68 openbsd.evilscan.com
45 00 00 4e 74 07 00 00 71 11 b7 4c d1 40 75 d7 c7 ef 0f 44 E..Nt...q..L.@u....D
```

```
00 89 00 89 00 3a b7 f4 e9 ee 00 00 00 01 00 00 00 00 00 00 .....:..............

20 43 4b 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 CKAAAAAAAAAAAAAAAA

41 41 41 41 41 41 41 41 41 41 41 41 41 00 00 21 00 01 AAAAAAAAAAAAA..!..

EVENT1: [SMB:NAME-WILDCARD] (udp,dp=137,sp=137)

dragon (Towards) 00:21:54

SOURCE: 209.64.117.215 209-64-117-215.mastercard.com

DEST: 192.168.1.68 openbsd.evilscan.com

45 00 00 4e 75 07 00 00 71 11 b6 4c d1 40 75 d7 c7 ef 0f 44 E..Nu...q..L.@u....D

00 89 00 89 00 3a b7 f2 e9 f0 00 00 00 01 00 00 00 00 00 00 .....:..............

20 43 4b 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 CKAAAAAAAAAAAAAAAA

41 41 41 41 41 41 41 41 41 41 41 41 41 00 00 21 00 01 AAAAAAAAAAAAA..!..

EVENT1: [SMB:NAME-WILDCARD] (udp,dp=137,sp=137)
```

Return to Detect 10