---

# „Shall We Play A Game?” - Active defense against port scanning

**Author:**
Piotr Duszyński
Twitter: @drk1wi
e-mail: piotr [at] duszynski.eu

**Project website:**
http://portspoof.duszynski.eu
https://github.com/drk1wi/portspoof

---

Table of contents:

***Intro:*** ***2***

***Description:*** ***2***

***Briefly about the Portspoof*** ***3***

***How to configure Portspoof on your system*** ***5***

***:: Author comments ::*** ***5***

 

**Intro:**

I assume that the reader of this paper is familiar with basic technical concepts related to networking and ethical hacking (especially port scanning techniques as part of the reconessaince phase).

Therefore without any additional digression I go to the main topic of this paper. Mainly: how to make life of a port scanner user miserable and daunting...

**Description:**

Maybe lets express the whole concept in a bit more appealing way. We want to change **this**:

```
Starting Nmap 6.01 ( http://nmap.org ) at 2012-10-17 19:52 CEST
Stats: 0:00:01 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 100.00% done; ETC: 19:52 (0:00:00 remaining)
Nmap scan report for 192.168.97.130
Host is up (0.0051s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     ProFTPD 1.3.2c
22/tcp open  ssh     OpenSSH 5.3p1 Debian 3ubuntu6 (protocol 2.0)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:kernel

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.87 seconds
```

Note:
Yes, there are two legitimate services here.
into **this**:

```
Host is up (0.00057s latency).
PORT     STATE SERVICE           VERSION
1/tcp    open  4d-server         4th Dimension database server
3/tcp    open  compressnet?
4/tcp    open  afsmain           Code-Crafters Ability FTP Server afsmain admin
6/tcp    open  aperio-aaf        Aperio Algorithm Framework
7/tcp    open  aplus             Cleo A+ (API 237592289; CSS 3612)
9/tcp    open  arkeia            Arkeia Network Backup
13/tcp   open  backdoor          Jeem backdoor (**BACKDOOR**)
17/tcp   open  backdoor          Subseven backdoor (**BACKDOOR**)
19/tcp   open  backdoor          NerdBot backdoor (**BACKDOOR**)
20/tcp   open  backdoor          Darkmoon backdoor "reptile" ftpd (**BACKDOOR**)
21/tcp   open  ftp?
22/tcp   open  backdoor          dhcpse.exe (**BACKDOOR**)
23/tcp   open  backdoor          Haxdoor trojan (**BACKDOOR**)
24/tcp   open  priv-mail?
25/tcp   open  smtp?
26/tcp   open  bandwidth-test    Mikrotik bandwidth-test server
30/tcp   open  bruker-axs        Bruker AXS X-ray controller status (X-rays: Off)
32/tcp   open  burk-autopilot    Burk AutoPilot Plus remote management
33/tcp   open  bzfs              BZFlag game server
37/tcp   open  chat              AIM or ICQ server
42/tcp   open  citrix-ima        Citrix Metaframe XP IMA
43/tcp   open  clsbd             Cadence IC design daemon
49/tcp   open  crestron-control  Crestron Terminal Console
53/tcp   open  domain?
70/tcp   open  gopher?
79/tcp   open  ftp               Microsoft IIS ftpd MrBjGBQbX
80/tcp   open  ftp               IronPort mail appliance ftpd Q
81/tcp   open  ftp               IronPort firewall ftpd TgRTfdUju
82/tcp   open  ftp               Texas Imperial Software WFTPD 9lVt
83/tcp   open  ftp               Heimdal Kerberized ftpd 9vT
84/tcp   open  ftp               vsftpd (broken: could not bind listening IPv4 socket)
85/tcp   open  ftp               vsftpd (broken: j*)
88/tcp   open  kerberos-sec?
89/tcp   open  ftp               FileZilla ftpd .K..e% `.
90/tcp   open  ftp               FileZilla ftpd
```

 

■ ■ ■ **90/tcp -> 49161/tcp ;)**

```
49161/tcp open  righteous-backup  R1Soft Righteous Backup
49163/tcp open  rpd               Remote Play Daemon 1003002
49165/tcp open  scalix-ual        Scalix UAL
49167/tcp open  sieve             Cyrus timsieved Murder kSm
49175/tcp open  sharefolder       Public ShareFolder mailbox synchronization
49176/tcp open  shell             HP-UX Remshd (Kerberos disabled)
49400/tcp open  ssh               OpenSSH UheUAe (gssapi; protocol 81011)
49999/tcp open  telnet            Welltech Wellgate VoIP adapter telnetd
50000/tcp open  telnet            Toshiba print server telnetd
50001/tcp open  telnet            IPSentry telnetd
50002/tcp open  telnet            EMULEX NetQue print server telnetd
50003/tcp open  telnet            Cisco telnetd
50006/tcp open  telnet            Philips D-BOX2 telnetd (Linux kernel gxpWKz)
50300/tcp open  netbios-ssn       Brother MFC-820CW printer smbd
50389/tcp open  aplus             Cleo A+ (API 237592289; CSS 3612)
50500/tcp open  ftp
50636/tcp open  ftp-proxy         AVM KEN! ftp proxy
50800/tcp open  unknown
51103/tcp open  smtp              Lotus Notes SMTP
51493/tcp open  telnet            Actiontec DSL router
52673/tcp open  mysql             MySQL
52822/tcp open  pop3              Classic Hamster pop3d (Permission denied)
52848/tcp open  pop3-proxy        AVG pop3 proxy 084628630 Beta
52869/tcp open  pop3pw            poppassd
54045/tcp open  postgresql        PostgreSQL DB
54328/tcp open  ftp               Savin 8055 printer ftpd wtyIj
55055/tcp open  ssh               (protocol 476)
55056/tcp open  ssh               (protocol 639)
55555/tcp open  pop3              hMailServer pop3d
55600/tcp open  telnet            EMULEX NetQue print server telnetd
56737/tcp open  smtp              JAMES 3 M3 smtpd
56738/tcp open  smtp
57294/tcp open  keriopfservice    Kerio PF 4 Service (maybe 4.0.2-11)
57797/tcp open  X11               StarNet X-Win32 (Only accepting connections from net 28215)
58080/tcp open  ftp               Nucleus ftpd SAivAXt
60020/tcp open  imap              Microsoft Exchange Server 2003 imapd begQlrBzZ (Spanish)
60443/tcp open  smtp              eMail Sentinel smtpd 6
61532/tcp open  giop              CORBA naming service
61900/tcp open  imap              Binc imapd
62078/tcp open  pop3              MS Exchange 2003 pop3d 86869 (Chinese)
63331/tcp open  smtp-proxy        Tumbleweed Email Firewall smtp proxy
64623/tcp open  telnet            Bintec X2301 ADSL modem telnetd atm_+l8 (Name mDYF)
64680/tcp open  unknown
65000/tcp open  http              IronPort Mailflow http config (Python 48573925)
65129/tcp open  echo
65389/tcp open  ftp               Microsoft IIS ftpd MrBjGBQbX
Service Info: Hosts: quU, YXoSyi, Zscj, -IdqKFf, wODFXR; OSs: Windows, Unix, NetWare, AIX, Linux; Devices: specialized, remote management, game
 console, printer, security-misc; CPE: cpe:/o:microsoft:windows, cpe:/o:novell:netware, cpe:/o:ibm:aix, cpe:/o:redhat:linux, cpe:/o:apple:mac_o
s_x

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 530.31 seconds
```

Note:
Can you find all of the legitimate services without running the range of 1-65535 without the knowledge of particular protocol and sending additional packets?

### Briefly about the Portspoof

The goal of this software can be closed in few sentences:

„The portspoof program is designed to enhance OS security through emulation of legitimate service signatures on otherwise closed ports. It is meant to be a lightweight, fast, portable and secure addition to the any firewall system or security infrastructure.
The general goal of the program is to make the port scanning software (Nmap/Unicornscan/etc) process slow and output very difficult to interpret, thus making the attack reconnaissance phase a challenging and bothersome task....”

Though ... it is going to do much more than that in the nearest future ;) keep track of:
https://github.com/drk1wi/portspoof

It has the following features:

- Fast : Multithreaded (by default 10 threads handle new incoming connections).
- Lightweight : Requires marginal amount of system resources.
- Portable : runs on Linux and on BSD (up to ver. 0.3)
  Note:
  I will resume the BSD support as soon I will find more time.
- Flexible : You can easily use your firewall rules to define ports that are going to be spoofed.
- Effective against popular port scanners ...
- Over **8000** false signatures that will fool port scanners!
- Did I mention it's Open Source?

 

**How to configure Portspoof on your system**

**1. Get the software**

https://github.com/drk1wi/portspoof

**2. Compile it:**

$ ./configure
$ make
# make install (optional)

**3. Configure your firewall rules:**

**IPTABLES (Linux) :**
Add the following rule as your last (instead of DROP):

**# iptables -A PREROUTING -i eth0 -p tcp -m tcp --dport 1:65535 -j REDIRECT --to-ports 4444**

Note:
If you want to access your legitimate services you have to exclude their ports from the REDIRECT statement!

Portspoof by default will listen on port ALL_INTERFACES and port 4444 tcp. This FW rules will result in service obfuscation for port range from 1 to 65535

$ ./portspoof.

**3. Add portspoof invocation to your system's startup scripts.**

Modify other relevant startup scripts.

**:: Author comments ::**

If you would like to submit your ideas, suggestions, comments or additional code, then write to piotr [at] duszynski.eu or post it on:
https://github.com/drk1wi/portspoof/issues