

THOMSON



COURSE TECHNOLOGY

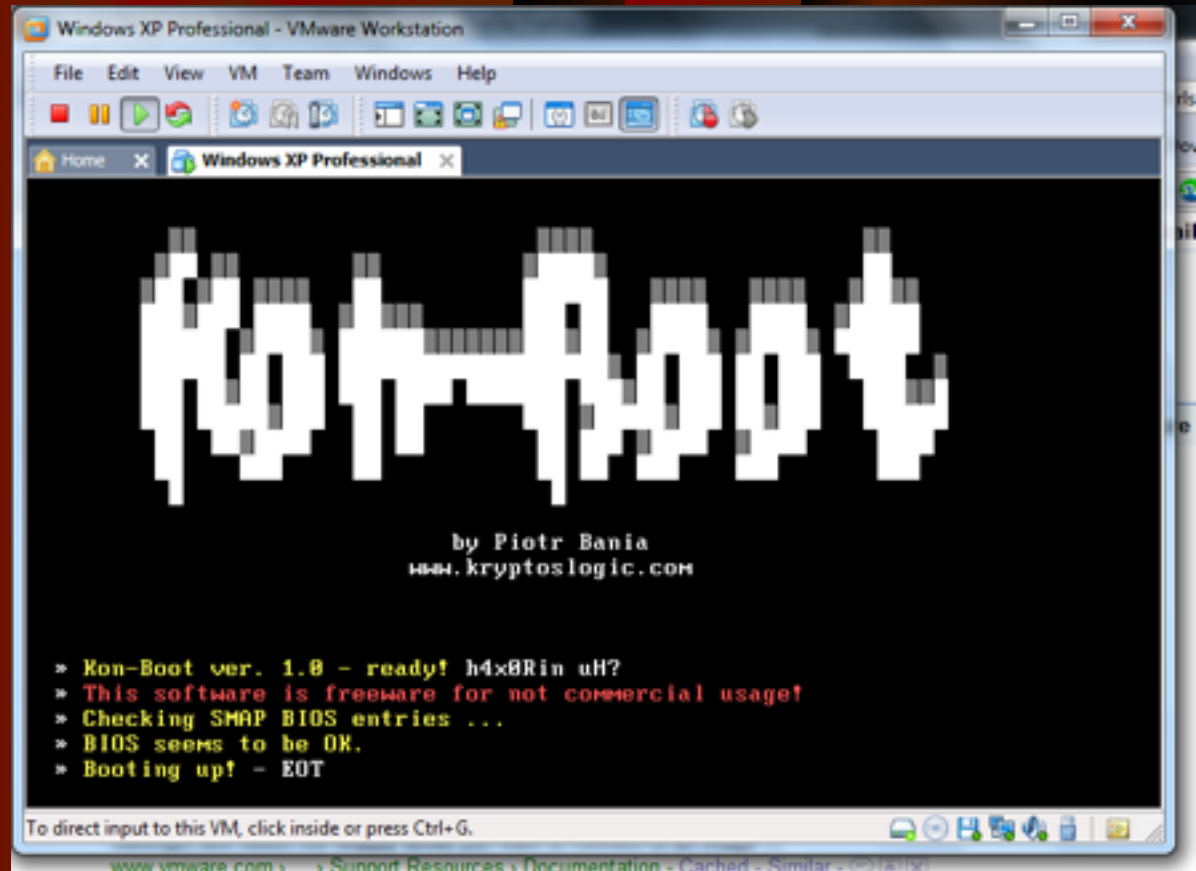
Hands-On Ethical Hacking and Network Defense

Chapter 5 Port Scanning

Last revised
10-4-17

KonBoot

- Get into any account without the password
- Works on Windows and Linux
- No longer free
- Link Ch 5r



From the Projects: UBCD



- Proj 13
- Create new administrator user on a Windows computer
- Based on Win XP Pre-Boot Environment; causes BSOD on some modern systems

Linux-Based UBCD

```
Ultimate Boot CD V5.3.2 http://www.ultimatebootcd.com
BIOS
CPU
HDD
Memory
Others
Peripherals
System
Parted Magic 2013_08_01_i586 - Press F1 for more information
UBCD FreeDOS R1.51 (Based on MWDsk V3.48)
User-defined
```

- Proj X7
- Promote normal user to administrator user on a Windows computer
- Works well on modern systems

Objectives

- Describe port scanning
- Describe different types of port scans
- Describe various port-scanning tools
- Explain what ping sweeps are used for
- Explain how shell scripting is used to automate security tasks

Introduction to Port Scanning

- Port Scanning
 - Finds out which services are offered by a host
 - Identifies vulnerabilities
- Open services can be used on attacks
 - Identify a vulnerable port
 - Launch an exploit
- Scan all ports when testing
 - Not just well-known ports

angryip.org/about/



Angry IP Scanner

Fast and friendly network scanner

About

Screenshots

About

Angry IP scanner is a very fast IP address and port scanner.

IP Range - Angry IP Scanner

Scan Go to Commands Favorites Tools Help

IP Range: 195.80.116.0 to 195.80.116.255

IP Range



Hostname: e-estonia.com

IP1 /24

Start



IP	Ping	Hostname	Ports [3+]	Web detect
195.80.116.226	[n/a]	[n/s]	[n/s]	[n/s]
195.80.116.227	9 ms	[n/a]	80,443	Resin/4.0.37
195.80.116.228	10 ms	[n/a]	80,443	[n/a]
195.80.116.229	9 ms	[n/a]	80,443	Apache
195.80.116.230	13 ms	mx3.rmke.ee	[n/a]	[n/a]
195.80.116.231	10 ms	mx4.rmke.ee	[n/a]	[n/a]
195.80.116.232	[n/a]	[n/s]	[n/s]	[n/s]
195.80.116.233	[n/a]	[n/s]	[n/s]	[n/s]
195.80.116.234	[n/a]	[n/s]	[n/s]	[n/s]
195.80.116.235	9 ms	[n/a]	80,443	[n/a]
195.80.116.236	[n/a]	[n/s]	[n/s]	[n/s]
195.80.116.237	[n/a]	[n/s]	[n/s]	[n/s]

Ready

Display: All

Threads: 0


```
root@kali:~/romance# netdiscover -h
Netdiscover 0.3-pre-beta7 [Active/passive arp reconnaissance tool]
Written by: Jaime Penalba <jpenalbae@gmail.com>

Usage: netdiscover [-i device] [-r range | -l file | -p] [-m file] [-s time] [-n node] [-c count] [-f] [-d] [-S] [-P] [-c]
  -i device: your network device
  -r range: scan a given range instead of auto scan. 192.168.6.0/24,/16,/8
  -l file: scan the list of ranges contained into the given file
  -p passive mode: do not send anything, only sniff
  -m file: scan the list of known MACs and host names
  -F filter: Customize pcap filter expression (default: "arp")
  -s time: time to sleep between each arp request (milliseconds)
  -n node: last ip octet used for scanning (from 2 to 253)
  -c count: number of times to send each arp request (for nets with packet loss)
  -f enable fastmode scan, saves a lot of time, recommended for auto
  -d ignore home config files for autoscan and fast mode
  -S enable sleep time suppression between each request (hardcore mode)
  -P print results in a format suitable for parsing by another program
  -N Do not print header. Only valid when -P is enabled.
  -L in parsable output mode (-P), continue listening after the active scan is completed

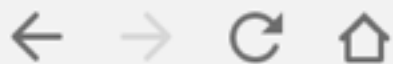
If -r, -l or -p are not enabled, netdiscover will scan for common lan addresses.
root@kali:~/romance#
```

```
root@kali:~/romance# netdiscover -r 172.16.1.0/24
```

```
Currently scanning: Finished! | Screen View: Unique Hosts
```

```
4 Captured ARP Req/Rep packets, from 4 hosts. Total size: 240
```

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
172.16.1.1	00:50:56:c0:00:08	1	60	Unknown vendor
172.16.1.2	00:50:56:f0:8a:91	1	60	Unknown vendor
172.16.1.206	00:0c:29:dd:64:1c	1	60	Unknown vendor
172.16.1.254	00:50:56:ec:f2:9c	1	60	Unknown vendor



Secure

https://nmap.org



NMAP.ORG

Zenmap

Scan Tools Profile Help

New Scan Command Wizard Save Scan Open Scan Report a bug Help

Intense Scan on scanme.nmap.org 171.67.22.3 10.0.0.10 wap.yuma.net zardoz.yuma.net X

Target: .10 wap.yuma.net zardoz.yuma.net Profile: Intense Scan Scan

Command: nmap -T Aggressive -A -v scanme.nmap.org 171.67.22.3 10.0.0.10 wap.yuma.net zardoz.yuma.net

Hosts Services Ports / Hosts Nmap Output Host Details Scan Details

OS	Host
	scanme.nmap.org
	171.67.22.3
	10.0.0.10
	wap.yuma.net 192
	zardoz.yuma.net 1

Host Status

State: up

Open ports: 3

Filtered ports: 0

Closed ports: 2

Scanned ports: 5

Up time: 3916956

Last boot: Sat Oct 27 10:38:07 2007

Addresses

IPv4: 205.217.153.62

IPv6:

MAC:

Hostnames

Name - Type: scanme.nmap.org - PTR

Operating System

Name: Linux 2.6.20-1 (Fedora Core 5)

Accuracy: 100%

Introduction to Port Scanning (continued)

- Port scanning programs report
 - Open ports
 - Closed ports
 - Filtered ports
 - Best-guess assessment of which OS is running

Is Port Scanning Legal?

- The legal status of port scanning is unclear
 - If you have permission, it's legal
 - If you cause damage of \$5,000 or more, it may be illegal
 - For more, see links Ch 5a and Ch 5b

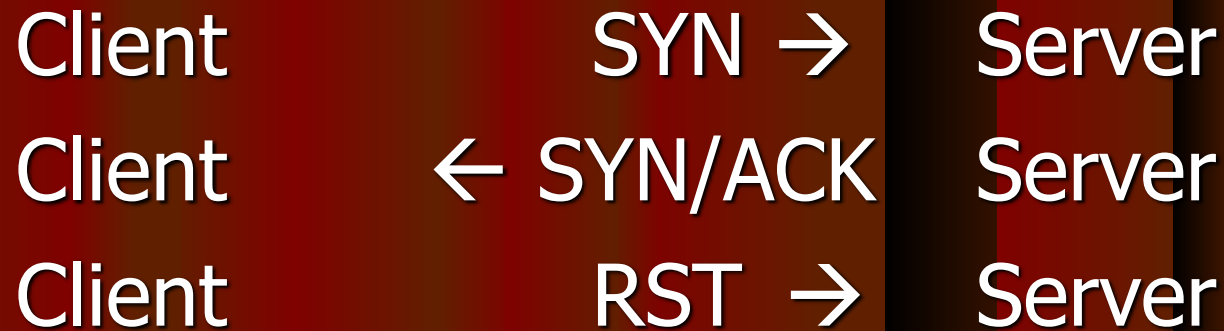
Normal TCP Handshake

Client SYN → Server
Client ← SYN/ACK Server
Client ACK → Server

```
1461 > http [SYN] seq=0  
http > 1461 [SYN, ACK]  
1461 > http [ACK] seq=1
```

After this, you are ready to send data

SYN Port Scan



The server is ready, but the client decided not to complete the handshake

Types of Port Scans

- SYN scan
 - Stealthy scan, because session handshakes are never completed
 - That keeps it out of some log files
 - Three states
 - Closed
 - Open
 - Filtered

```
44393 > 5001 [SYN] Seq=0
5001 > 44393 [RST, ACK]
```

```
38194 > netbios-ssn [SYN] Seq=0
netbios-ssn > 38194 [SYN, ACK]
38194 > netbios-ssn [RST] Seq=1
```

```
60313 > 203 [SYN]
```


Types of Port Scans

- Connect scan
 - Completes the three-way handshake
 - Not stealthy--appears in log files
 - Three states

- Closed

```
54353 > 5001 [SYN] Seq=  
5001 > 54353 [RST, ACK]
```

- Open

```
39582 > netbios-ssn [SYN] Seq=  
netbios-ssn > 39582 [SYN, ACK]  
39582 > netbios-ssn [ACK] Seq=  
39582 > netbios-ssn [RST, ACK]
```

- Filtered

```
46863 > 5007 [SYN]
```

Types of Port Scans

- NULL scan
 - All the packet flags are turned off
 - Two results:
 - Closed ports reply with RST
 - Open or filtered ports give no response

```
35745 > 4 [] Seq=0 Len=0
4 > 35745 [RST, ACK]
```

```
46854 > netbios-ssn [] Seq=0 Len=0
```

Types of Port Scans

- XMAS scan
 - FIN, PSH and URG flags are set
 - Works like a NULL scan – a closed port responds with an RST packet
- FIN scan
 - Only FIN flag is set
 - Closed port responds with an RST packet

Windows Machines

- NULL, XMAS and FIN scans don't work on Windows machines
 - Win 2000 Pro and Win Server 2003 shows all ports closed
 - Win XP Pro all ports open/filtered
 - See the NMAP tutorial ([link Ch 5c](#))

Types of Port Scans

- Ping scan
 - Simplest method sends ICMP ECHO REQUEST to the destination(s)
 - TCP Ping sends SYN or ACK to any port (default is port 80 for Nmap)
 - Any response shows the target is up

Types of Port Scans (continued)

- ACK scan
 - Used to get information about a firewall
 - Stateful firewalls track connection and block unsolicited ACK packets
 - Stateless firewalls just block incoming SYN packets, so you get a RST response
- UDP scan
 - Closed port responds with ICMP "Port Unreachable" message
 - Rarely used--but much improved in latest Nmap version (2010)

Using Port-Scanning Tools

- Nmap
- Nessus and OpenVAS (the GPL-licensed fork of Nessus)
 - A complete vulnerability scanner, more than a port scanner

Nmap

- Originally written for Phrack magazine
- One of the most popular tools
- GUI versions
 - Xnmap and Ubuntu's NmapFE
- Open source tool
- Standard tool for security professionals

The Matrix Reloaded

- Trinity uses Nmap
- Video at link Ch 4e



Trinity Nmap Hack - Matrix Reloaded

```
Port      State  Service
22/tcp    open  ssh

No exact OS matches for host

Nmap run completed -- 1 IP address (1 host up) scanned
# sshnuke 10.2.2.2 -rootpw="210N0101"
Connecting to 10.2.2.2:ssh ... successful.
Attempting to exploit SSHv1 CRC32 ... successful.
Reseting root password to "210N0101".
System open: Access Level (9)
# ssh 10.2.2.2 -l root
```

Kahoot!

Nessus

- First released in 1998
- No longer free, free version is called OpenVAS(GreenBone)
- Uses a client/server technology
- Can conduct tests from different locations
- Can use different OSs for client and network

Nessus (continued)

- Finds services running on ports
- Finds vulnerabilities associated with identified services

Nessus

https://172.20.10.60/

admin | Help | About | Log out

Policies Reports Scans Policies Users

➤ Add Policy

General
 Credentials
Plugins
 Preferences

Families	Plugins
<input type="radio"/> AIX Local Security Checks	<input type="radio"/> 34195 DB2 8 < Fix Pack 17 Multiple Vulnerabilities
<input type="radio"/> Backdoors	<input type="radio"/> 40662 DB2 8.1 < Fix Pack 18 Multiple Vulnerabilities
<input type="radio"/> CGI abuses	<input checked="" type="radio"/> 34475 DB2 9.1 < Fix Pack 6 Multiple Vulnerabilities
<input type="radio"/> CGI abuses : XSS	<input type="radio"/> 36216 DB2 9.1 < Fix Pack 7 Multiple Vulnerabilities
<input type="radio"/> CISCO	<input type="radio"/> 42044 DB2 9.1 < Fix Pack 8 Multiple Vulnerabilities
<input type="radio"/> CentOS Local Security Checks	<input type="radio"/> 34056 DB2 9.5 < Fix Pack 2 Multiple Vulnerabilities
<input type="radio"/> DNS	<input type="radio"/> 15486 DB2 < 8 Fix Pack 7a Multiple Vulnerabilities
<input checked="" type="radio"/> Databases	<input type="radio"/> 23935 DB2 < 8.1 FixPak 12 EXCSAT Long MGRLVLLS M
<input type="radio"/> Debian Local Security Checks	<input type="radio"/> 23936 DB2 < 8.1 FixPak 13 CONNECT Processing Unspe
<input type="radio"/> Default Unix Accounts	<input type="radio"/> 23937 DB2 < 8.1 FixPak 14 Multiple Vulnerabilities

Plugin Description

DB2 9.1 < Fix Pack 6 Multiple Vulnerabilities

Synopsis
 The remote database server is affected by multiple issues.

Description
 According to its version, the installation of DB2 9.1 on the remote host is affected by one or more of the following issues :

Enabled Families: 42 Enabled Plugins: 31443 Enable All Disable All

Cancel Back Next

OpenVAS (Greenbone)

Applications Places Mon Apr 27, 11:34 AM root

Greenbone Security Assistant - Iceweasel

Greenbone Security ...

https://127.0.0.1:9392/omp?r=1&token=62f51749-c006-44fd-8998-78855555 Google

Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB

Greenbone Security Assistant Logged in as Admin **admin** | Logout
Mon Apr 27 15:33:31 2015 UTC

Scan Management Asset Management SecInfo Management Configuration Extras Administration Help

Tasks (total: 0)

Filter:


apply_overrides=1 rows=10 first=1 sort=name

Name	Status	Reports		Severity	Trend	Actions
		Total	Last			

(Applied filter: apply_overrides=1 rows=10 first=1 sort=name) (total: 0)

Welcome dear new user!
To explore this powerful application and to have a quick start for doing things the first time, I am here to assist you with some hints and short-cuts.

I will appear automatically in areas where you have created no or only a few objects. And disappear when you have more than 3 objects. You can call me with this icon any time later on.



Quick start: Immediately scan an IP address
IP address or hostname:

For this short-cut I will do the following for you:

1. Create a new Target with default Port List
2. Create a new Task using this target with default Scan Configuration
3. Start this scan task right away
4. Switch the view to reload every 30 seconds so you can learn

root@kali: - [root@kali: ~] Greenbone Security A...

Greenbone Security Assistant - Firefox

File Edit View History Bookmarks Tools Help

Greenbone Security Assi...

https://192.168.201.250/omsp

Wikipedia (en)

Greenbone Security Assistant

Logged in as User demouser | Logout

Tue Jul 15 10:52:34 2014 UTC

Scan Management Asset Management Sec Info Management Configuration Extras Help

Tasks 1 - 11 of 11 (total: 11) Refresh every 10 Sec

Filter: apply_overrides=1 rows=20 permission=any owner=any first=1 sort Tasks Filter

Name	Status	Reports		Severity	Trend	Actions
		Total	Last			
Alterable Task (All assigned elements in this task: can be modified)	Stopped at 20 %	4 (5)	Jul 4 2014	0.0 (Log)		
Container Task (This does contain several imported reports)	Container	2 (2)	Jun 20 2014			
Deep Scan Linux (This does a deep scan of our linux test-system)	Done	2 (2)	Jun 25 2014	N/A	↓	
Deep Scan Windows (This does a deep scan of our Windows lab test-machines)	Done	1 (1)	Jun 20 2014	18.0 (High)		
Discovery Scan (This Scan Configuration applies any NVTs that discover as many details about the target system)	Requested	7 (9)	Jul 15 2014	0.0 (Log)	↔	
IT-Grundschutz Scan (Tests for Compliance with IT-Grundschutz, 12. EL)	Paused at 1 %	2 (4)	Jun 24 2014	2.8 (Low)	↔	
Nightly Scan with Schedule (This scan does a nightly scan of the entire network: and sends a mail if the threat level increases)	Done	1 (1)	Jun 21 2014	2.8 (Low)		
Quick Scan Linux (This does a quick: scan of our GNU/Linux lab machine)	Done	2 (4)	Jun 20 2014	4.3 (Medium)	↑	
Quick Scan Linux Clone 1 (This does a quick: scan of our GNU/Linux lab machine)	New					
Quick Scan Test Network (This does a deep scan of our test network:)	Done	1 (1)	Jun 24 2014	18.0 (High)		
Scan for Heartbleed (This does a scan for heartbleed vulnerability on our test-machines)	50 %	8 (16)	Jul 8 2014	0.0 (Log)		

(Applied filter: apply_overrides=1 rows=20 permission=any owner=any first=1 sort=name)

1 - 11 of 11 (total: 11)

Greenbone Security Assistant (GSA) Copyright 2009-2014 by Greenbone Networks GmbH, www.greenbone.net

Greenbone Security Assistant - Firefox

File Edit View History Bookmarks Tools Help

Greenbone Security Assi...

https://192.168.201.250/omp/token=ad5e35de-0c0d-11e4-8974-0f... W wikipedia (en)

Greenbone Security Assistant

Logged in as User demouser | Logout

Tue Jul 15 11:06:58 2014 UTC

Scan Management Asset Management Sec Info Management Configuration Extras Help

NVTs 230 - 239 of 35902 (total: 35902)

Filter: sort-reverse=created rows=10 first=230

Name	Family	Created	Modified	Version	CVE	Severity
Fedora Update for openssh FEDORA-2014-6569	Fedora Local Security Checks	Tue Jun 17 2014	Fri Jun 20 2014	\$Revision: 517 \$	CVE-2014-2653 CVE-2014-2532	5.8
Fedora Update for mingw-readline FEDORA-2014-6820	Fedora Local Security Checks	Tue Jun 17 2014	Fri Jun 20 2014	\$Revision: 517 \$	CVE-2014-2524	7.8
Fedora Update for mingw-libtiff FEDORA-2014-6831	Fedora Local Security Checks	Tue Jun 17 2014	Fri Jun 20 2014	\$Revision: 517 \$	CVE-2013-4231 CVE-2013-4232 CVE-2013-4243 CVE-2013-4244 CVE-2012-4447 CVE-2012-4564 CVE-2013-1960 CVE-2013-1961	9.3
Fedora Update for chkrootkit FEDORA-2014-7071	Fedora Local Security Checks	Tue Jun 17 2014	Fri Jun 20 2014	\$Revision: 517 \$	CVE-2014-0476	6.8
Fedora Update for gnutils FEDORA-2014-6881	Fedora Local Security Checks	Tue Jun 17 2014	Fri Jun 20 2014	\$Revision: 517 \$	CVE-2014-3466 CVE-2014-0092 CVE-2014-1959 CVE-2013-4466	6.8
Fedora Update for nspr FEDORA-2014-7279	Fedora Local Security Checks	Tue Jun 17 2014	Fri Jun 20 2014	\$Revision: 517 \$	CVE-2013-5607	7.5
Fedora Update for mingw-freetype FEDORA-2014-6830	Fedora Local Security Checks	Tue Jun 17 2014	Fri Jun 20 2014	\$Revision: 517 \$	CVE-2014-2240 CVE-2014-2241	7.5
Fedora Update for check-mk FEDORA-2014-6810	Fedora Local Security Checks	Tue Jun 17 2014	Fri Jun 20 2014	\$Revision: 517 \$	CVE-2014-2330 CVE-2014-2331 CVE-2014-2329 CVE-2014-2332 CVE-2014-0243	7.8
Fedora Update for mingw-libjpeg-turbo FEDORA-2014-6870	Fedora Local Security Checks	Tue Jun 17 2014	Fri Jun 20 2014	\$Revision: 517 \$	CVE-2013-6629 CVE-2013-6630	5.8
Fedora Update for mingw-icu FEDORA-2014-6828	Fedora Local Security Checks	Tue Jun 17 2014	Fri Jun 20 2014	\$Revision: 517 \$	CVE-2013-2924	7.5

(Applied filter: sort-reverse=created rows=10 first=230)

230 - 239 of 35902 (total: 35902)

Greenbone Security Assistant (GSA) Copyright 2009-2014 by Greenbone Networks GmbH, www.greenbone.net

Conducting Ping Sweeps

- Ping sweeps
 - Identify which IP addresses belong to active hosts
 - Ping a range of IP addresses
- Problems
 - Computers that are shut down cannot respond
 - Networks may be configured to block ICMP Echo Requests
 - Firewalls may filter out ICMP traffic

FPing

- Ping multiple IP addresses simultaneously
- www.fping.com/download
- Command-line tool
- Input: multiple IP addresses
 - To enter a range of addresses
 - -g option
 - Input file with addresses
 - -f option
- See links Ch 5k, 5l

```
File Edit View Terminal Go Help
Usage: fping [options] [targets...]
  -a          show targets that are alive
  -A          show targets by address
  -b n        amount of ping data to send, in bytes (default 56)
  -B f        set exponential backoff factor to f
  -c n        count of pings to send to each target (default 1)
  -C n        same as -c, report results in verbose format
  -e          show elapsed time on return packets
  -f file     read list of targets from a file ( - means stdin) (only if no -g specified)
  -g          generate target list (only if no -f specified)
              (specify the start and end IP in the target list, or supply a IP netmask)
              (ex. fping -g 192.168.1.0 192.168.1.255 or fping -g 192.168.1.0/24)
  -i n        interval between sending ping packets (in millisec) (default 25)
  -l          loop sending pings forever
  -m          ping multiple interfaces on target host
  -n          show targets by name (-d is equivalent)
  -p n        interval between ping packets to one target (in millisec)
              (in looping and counting modes, default 1000)
  -q          quiet (don't show per-target/per-ping results)
  -Q n        same as -q, but show summary every n seconds
  -r n        number of retries (default 3)
  -s          print final stats
  -t n        individual target initial timeout (in millisec) (default 500)
  -u          show targets that are unreachable
  -v          show version
  targets    list of targets to check (if no -f specified)

[root@localhost root]#
```

Figure 5-7 Fping parameters

```
Session Edit View Bookmarks Settings Help
[root@localhost fping-2.4b2_to]# fping -g 193.145.85.201 193.145.85.220
193.145.85.201 is alive
193.145.85.202 is alive
193.145.85.206 is alive
193.145.85.207 is alive
193.145.85.208 is alive
193.145.85.209 is alive
193.145.85.210 is alive
193.145.85.203 is alive
193.145.85.204 is unreachable
193.145.85.205 is unreachable
193.145.85.211 is unreachable
193.145.85.212 is unreachable
193.145.85.213 is unreachable
193.145.85.214 is unreachable
193.145.85.215 is unreachable
193.145.85.216 is unreachable
193.145.85.217 is unreachable
193.145.85.218 is unreachable
193.145.85.219 is unreachable
193.145.85.220 is unreachable
[root@localhost fping-2.4b2_to]#
```

Figure 5-8 Results of an Fping command

Hping

- Used to bypass filtering devices
 - Allows users to fragment and manipulate IP packets
- www.hping.org/download
- Powerful tool
 - All security testers must be familiar with tool
- Supports many parameters (command options)
 - See links Ch 5m, Ch 5n

```

File Edit View Terminal Go Help
usage: hping host [options]
-h --help      show this help
-v --version   show version
-c --count     packet count
-i --interval  wait (uX for X microseconds, for example -i u1000)
               --fast      alias for -i u10000 (10 packets for second)
-n --numeric   numeric output
-q --quiet     quiet
-I --interface interface name (otherwise default routing interface)
-V --verbose   verbose mode
-D --debug     debugging info
-z --bind      bind ctrl+z to ttl                (default to dst port)
-Z --unbind    unbind ctrl+z

Mode
default mode   TCP
-0 --rawip     RAW IP mode
-1 --icmp      ICMP mode
-2 --udp       UDP mode
-8 --scan      SCAN mode.
               Example: hping --scan 1-30,70-90 -S www.target.host
-9 --listen    listen mode

IP
-a --spoofer   spoof source address
--rand-dest    random destination address mode. see the man.
--rand-source  random source address mode. see the man.
-t --ttl       ttl (default 64)
-N --id        id (default random)
-W --winid     use win* id byte ordering
-r --rel       relativize id field                (to estimate host traffic)
-f --frag      split packets in more frag.      (may pass weak acl)
-x --morefrag  set more fragments flag
-y --dontfrag  set dont fragment flag
-g --fragoff   set the fragment offset
-m --mtu       set virtual mtu, implies --frag if packet size > mtu
-o --tos       type of service (default 0x00), try --tos help
-G --rroute    includes RECORD_ROUTE option and display the route buffer
--lsrr         loose source routing and record route
--ssrr         strict source routing and record route
-H --ipproto   set the IP protocol field, only in RAW IP mode
:

```

Figure 5-9 Hping help, page 1

```
File Edit View Terminal Go Help
ICMP
-C --icmp-type icmp type (default echo request)
-K --icmp-code icmp code (default 0)
--force-icmp send all icmp types (default send only supported types)
--icmp-gw set gateway address for ICMP redirect (default 0.0.0.0)
--icmp-ts Alias for --icmp --icmp-type 13 (ICMP timestamp)
--icmp-addr Alias for --icmp --icmp-type 17 (ICMP address subnet mask)
--icmp-help display help for others icmp options
UDP/TCP
-s --baseport base source port (default random)
-p --destport [+] [+]<port> destination port(default 0) ctrl+z inc/dec
-k --keep keep still source port
-w --win winsize (default 64)
-o --tcpoff set fake tcp data offset (instead of tcphdrLen / 4)
-Q --seqnum shows only tcp sequence number
-b --badcksum (try to) send packets with a bad IP checksum
many systems will fix the IP checksum sending the packet
so you'll get bad UDP/TCP checksum instead.
-M --setseq set TCP sequence number
-L --setack set TCP ack
-F --fin set FIN flag
-S --syn set SYN flag
-R --rst set RST flag
-P --push set PUSH flag
-A --ack set ACK flag
-U --urg set URG flag
-X --xmas set X unused flag (0x40)
-Y --ynas set Y unused flag (0x80)
--tcpexitcode use last tcp->th_flags as exit code
--tcp-timestamp enable the TCP timestamp option to guess the HZ/uptime
Common
-d --data data size (default is 0)
-E --file data from file
-e --sign add 'signature'
-j --dump dump packets in hex
-J --print dump printable characters
-B --safe enable 'safe' protocol
-u --end tell you when --file reached EOF and prevent rewind
-T --traceroute traceroute mode (implies --bind and --ttl 1)
:
```

Figure 5-10 Hping help, page 2

```

File Edit View Terminal Go Help
--icmp-ts Alias for --icmp --icmptype 13 (ICMP timestamp)
--icmp-addr Alias for --icmp --icmptype 17 (ICMP address subnet mask)
--icmp-help display help for others icmp options
UDP/TCP
-s --baseport base source port (default random)
-p --destport [+] [+]<port> destination port(default 0) ctrl+z inc/dec
-k --keep keep still source port
-w --win winsize (default 64)
-O --tcpoff set fake tcp data offset (instead of tcphdrlen / 4)
-Q --seqnum shows only tcp sequence number
-b --badcksum (try to) send packets with a bad IP checksum
many systems will fix the IP checksum sending the packet
so you'll get bad UDP/TCP checksum instead.
-M --setseq set TCP sequence number
-L --setack set TCP ack
-F --fin set FIN flag
-S --syn set SYN flag
-R --rst set RST flag
-P --push set PUSH flag
-A --ack set ACK flag
-U --urg set URG flag
-X --xmas set X unused flag (0x40)
-Y --ynas set Y unused flag (0x80)
--tcpexitcode use last tcp->th_flags as exit code
--tcp-timestamp enable the TCP timestamp option to guess the HZ/uptime
Common
-d --data data size (default is 0)
-E --file data from file
-e --sign add 'signature'
-j --dump dump packets in hex
-J --print dump printable characters
-B --safe enable 'safe' protocol
-u --end tell you when --file reached EOF and prevent rewind
-T --traceroute traceroute mode (implies --bind and --ttl 1)
--tr-stop Exit when receive the first not ICMP in traceroute mode
--tr-keep-ttl Keep the source TTL fixed, useful to monitor just one hop
--tr-no-rtt Don't calculate/show RTT information in traceroute mode
ARS packet description (new, unstable)
--apd-send Send the packet described with APD (see docs/APD.txt)
(END)

```

Figure 5-11 Hping help, page 3

Broadcast Addresses

- If you PING a broadcast address, that can create a lot of traffic
- Normally the broadcast address ends in 255
- But if your LAN is subnetted with a subnet mask like 255.255.255.192
 - There are other broadcast addresses ending in 63, 127, and 191

Smurf Attack

- Pinging a broadcast address on an old network resulted in a lot of ping responses
- So just put the victim's IP address in the "From" field
 - The victim is attacked by a flood of pings, none of them directly from you
- Modern routers don't forward broadcast packets, which prevents them from amplifying smurf attacks
- Windows XP and Ubuntu don't respond to broadcast PINGs
- See links Ch 5o, 5p

Broadcast Ping at CCSF

```
~: sam@Sam-Bownes-MacBook-Air.local: ~ — bash — 80x24 11:15:26
sam@Sam-Bownes-MacBook-Air:~$ ping 147.144.207.255
PING 147.144.207.255 (147.144.207.255): 56 data bytes
64 bytes from 147.144.205.105: icmp_seq=0 ttl=64 time=0.127 ms
64 bytes from 147.144.207.114: icmp_seq=0 ttl=63 time=6.004 ms
64 bytes from 147.144.204.1: icmp_seq=0 ttl=64 time=36.508 ms
64 bytes from 147.144.192.1: icmp_seq=0 ttl=255 time=46.509 ms
64 bytes from 147.144.200.95: icmp_seq=0 ttl=64 time=61.198 ms
64 bytes from 147.144.192.233: icmp_seq=0 ttl=64 time=68.454 ms
64 bytes from 147.144.197.146: icmp_seq=0 ttl=64 time=119.037 ms
64 bytes from 147.144.192.31: icmp_seq=0 ttl=64 time=119.107 ms
64 bytes from 147.144.196.244: icmp_seq=0 ttl=64 time=126.904 ms
64 bytes from 147.144.200.62: icmp_seq=0 ttl=64 time=133.260 ms
64 bytes from 147.144.207.128: icmp_seq=0 ttl=64 time=213.046 ms
64 bytes from 147.144.206.140: icmp_seq=0 ttl=64 time=213.810 ms
64 bytes from 147.144.207.225: icmp_seq=0 ttl=64 time=218.351 ms
64 bytes from 147.144.207.219: icmp_seq=0 ttl=64 time=237.446 ms
64 bytes from 147.144.204.170: icmp_seq=0 ttl=64 time=292.164 ms
64 bytes from 147.144.204.168: icmp_seq=0 ttl=64 time=323.063 ms
64 bytes from 147.144.193.61: icmp_seq=0 ttl=64 time=323.239 ms
64 bytes from 147.144.201.156: icmp_seq=0 ttl=64 time=331.565 ms
64 bytes from 147.144.194.46: icmp_seq=0 ttl=64 time=332.753 ms
64 bytes from 147.144.197.242: icmp_seq=0 ttl=64 time=451.780 ms
64 bytes from 147.144.197.125: icmp_seq=0 ttl=64 time=453.995 ms
```

Crafting IP Packets

- Packet components
 - Source IP address
 - Destination IP address
 - Flags
- Crafting packets helps you obtain more information about a service
- Tools
 - Fping
 - Hping

Understanding Shell Scripting

- Modify tools to better suit your needs
- Script
 - Computer program that automates tasks
 - Time-saving solution

Scripting Basics

- Similar to DOS batch programming
- Script or batch file
 - Text file
 - Contains multiple commands
- Repetitive commands are good candidate for scripting
- Practice is the key

```
File Edit View Terminal Go Help
#!/bin/sh
# Myshell
# This program creates a text file named ip_address.txt that contains 254
# IP addresses using 193.145.85.0 as the network ID. The file created can
# be used as an input file for the fping utility. For example:
#   fping -f ip_address.txt

# Initialize variables

network_id="193.145.85."
count=0

# Stop the loop when count is equal to 254. The 'le' signifies less than
# or equal to 253, so the count variable will be incremented one more
# time after count is equal to 253. We do not want to create an IP
# address of 193.145.85.255 because this would be the broadcast address
# of the 193.145.85.0/24 network. Ping sweeping a broadcast address can
# be problematic.

while [ "$count" -le 253 ]
do

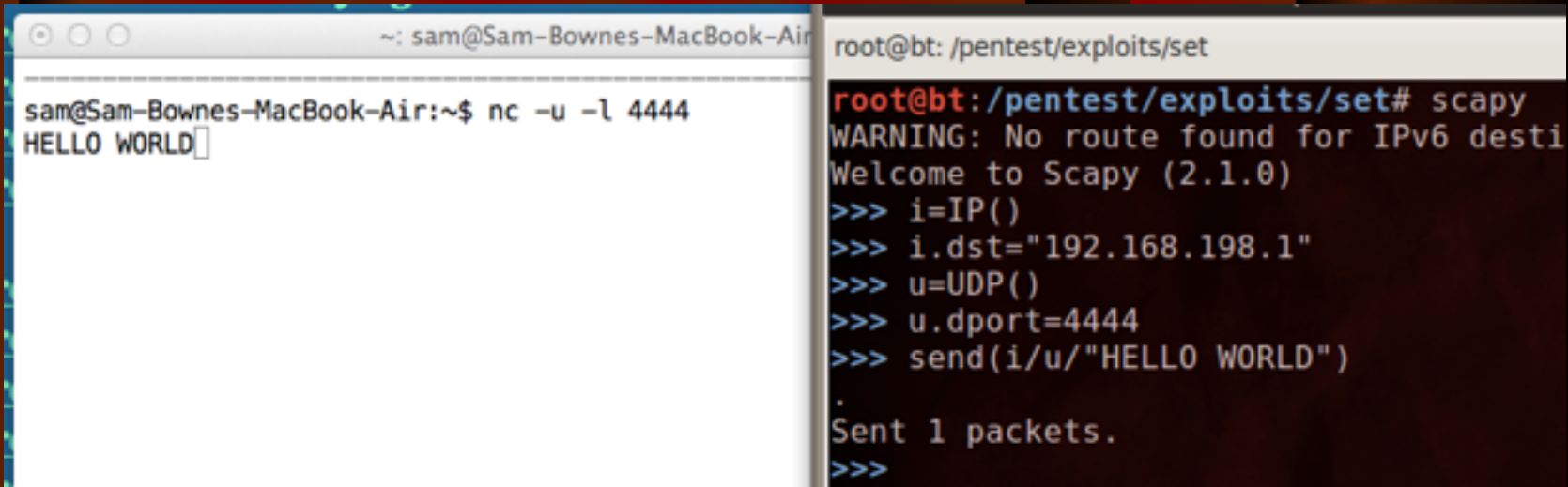
    count=$((count+1))
    printf "%s%s\n" $network_id $count >> ip_address.txt
done

exit 0
~
"Myshell" 27L, 818C written                2,2                All
```

Figure 5-12 A shell script

Scapy

- Packet-crafting python utility
- Proj 9, 10, 17, X11, X12, X13

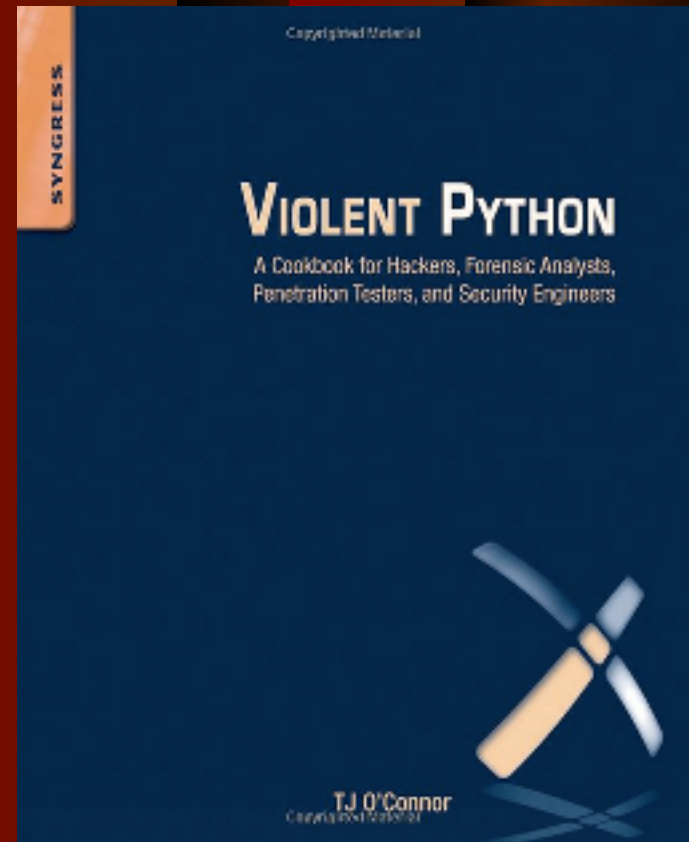


```
~: sam@Sam-Bownes-MacBook-Air
-----
sam@Sam-Bownes-MacBook-Air:~$ nc -u -l 4444
HELLO WORLD

root@bt: /pentest/exploits/set
root@bt:/pentest/exploits/set# scapy
WARNING: No route found for IPv6 destination addresses: dropping (no IPv6 support found)
Welcome to Scapy (2.1.0)
>>> i=IP()
>>> i.dst="192.168.198.1"
>>> u=UDP()
>>> u.dport=4444
>>> send(i/u/"HELLO WORLD")
.
Sent 1 packets.
>>>
```


Python

- Write your own tools
- Using this book in CNIT 124



Kahoot!