



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

Port Scanning

Lecture 3

Trawsnewid Addysg; Trawsnewid Bywydau
Transforming Education; Transforming Lives



www.uwtsd.ac.uk

LEARNING OUTCOMES

After you complete today's class, you will be able to:

- Describe port scanning and types of port scans
- Describe 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

- Method of finding which services are offered by a host
- Identifies vulnerabilities
- Common Vulnerabilities and Exposures: <http://cve.mitre.org/index.html>
- National Vulnerabilities Database (USA) : <https://nvd.nist.gov/vuln/full-listing>

Open services can be used on attacks

- Identify vulnerable port and launch exploit

Scans all ports when testing

- Not just well-known ports

Open, Closed, and Filtered Ports

- Port scanning programs report:
 - **Open ports**
 - Allows access to applications and can be vulnerable to attack
 - **Closed ports**
 - Doesn't allow entry or access to a service
 - **Filtered ports**
 - Might indicate that a firewall allows specified traffic into or out of the network

TYPES OF PORT SCANS

- SYN scan
 - Stealthy scan
 - If port is closed RTS/ACK packet
 - Close connection quickly so no full TCP connection made
- Connect scan
 - Completes three-way handshake
 - Could be tracked
- NULL scan
 - Packet flags are turned off
 - Response to a Null scan could be RST packet, meaning closed port, no packet could mean an open port
- XMAS scan
 - FIN, PSH and URG flags are set, closed port response would be RST packet else it could be open

TYPES OF PORT SCANS

- **ACK scan**
 - Used to get past firewall, if anACK packet is sent and an RTS is returned, it is likely there is no-packet filtering device
- **FIN scan**
 - Closed port responds with an RST packet
- **UDP scan**
 - Closed port responds with ICMP “Port Unreachable” message, means closed port

USING PORT-SCANNING TOOLS

- **Port-scanning tools**
 - Hundreds available
 - Not all are accurate
 - Be familiar with a variety of tools
 - Practice often to gain proficiency
 - Do not use one tool exclusively
- **Some tools include:**
 - Nmap
 - Nessus and OpenVAS

CONDUCTING PING SWEEPS

- **Ping sweeps**
 - Identify which IP addresses belong to active hosts
 - Ping a range of IP addresses to see what type of response is returned
- **Problems**
 - Shut down computers cannot respond
 - Networks may be configured to block ICMP Echo Requests
 - Firewalls may filter out ICMP traffic

ANGRY IP

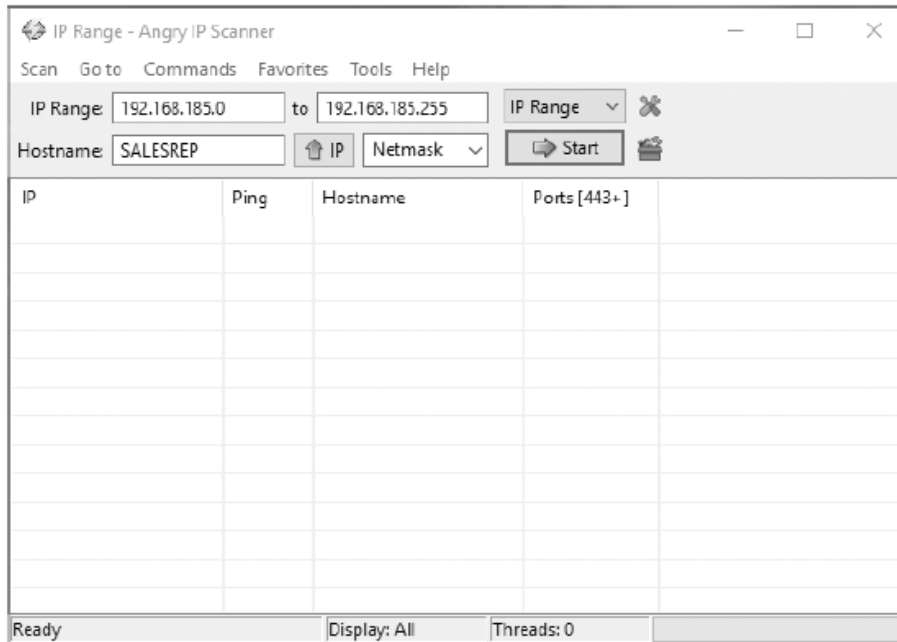


Figure 5-1 The Angry IP port scanner interface

Source: GNU General Public License

PRACTICAL1: Try Angry IP Scanner and record results (Runs on Windows, Mac or Linux)

<https://angryip.org/>

NMAP

- Originally written for *Phrack* magazine
 - One of the most popular port scanning tools
 - New features frequently added
- GUI front end
 - Zenmap
 - Makes working with complex options easier
- Standard tool for security professionals
 - Command: `nmap 193.145.85.201`
 - Scans every port on computer with this IP address

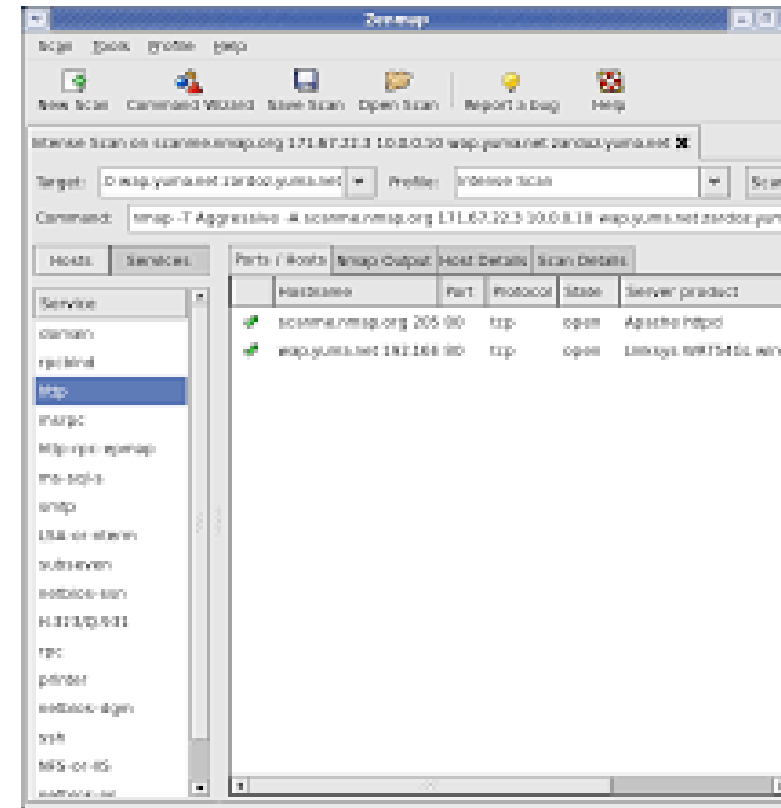
Nmap and Zenmap

```
# nmap -iL scanme.nmap.org -oXc

Starting Nmap 4.01 ( http://www.insecure.org/nmap/ ) at 2006-02-20 15:53 PST
Interesting ports on scanme.nmap.org (205.217.153.62):
(The 1647 ports scanned but not shown below are in state: filtered)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 3.9p1 (protocol 1.99)
25/tcp    open  smtp     Postfix smtpd
53/tcp    open  domain   ISC BIND 9.2.1
80/tcp    closed gopher-
88/tcp    open  http     Apache httpd 2.0.52 ((Ubuntu))
113/tcp   closed auth
Service type: general purpose
Running: Linux 2.6.8
OS details: Linux 2.6.8 - 2.6.11
Uptime: 26.177 days 44secs Mon Feb 22 11:39:16 2006

Interesting ports on d8aa.internal (192.168.12.30):
(The 1647 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      Serv-U ftpd 4.0
25/tcp    open  smtp     Mail M-CRIMP 7.15 2005-2
88/tcp    open  http     Microsoft IIS webserver 5.0
110/tcp   open  pop3     Mail pop3d 7.15 2005-4
135/tcp   open  msrpc    Microsoft msrpc Task server - c:\winnt\system32\
139/tcp   open  netbios-ssn
145/tcp   open  microsoft-ds Microsoft Windows XP microsoft-ds
1625/tcp  open  wsrpc    Microsoft Windows XP
5000/tcp  open  vnc-bdts UltraVNC Ovation 1024x800: VNC RDP port: 5000
NMC Address: 00:00:0C:00:17:2E 0-Lite-on Communications
Service type: general purpose
Running: Microsoft Windows NT/2000/XP
OS details: Microsoft Windows 2000 Professional
Service Info: OS: Windows

Nmap finished: 2 IP addresses (2 hosts up) scanned in 42.291 seconds
file:///home/fjoder/nmap-misc/Screenshots/042906a1
```



NESSUS

Nessus

- First released in 1998
- No longer under GPL license
 - Still available for download from Tenable Network Security Corporation for noncommercial personal use

OPENVAS

OpenVAS

- Open-source fork of Nessus in 2005
- Now branded as Greenbone Security Assistant
- Capable of updating security check plug-ins
 - Security test programs (scripts)
- Performs complex queries while client interfaces with server
- Can also determine what vulnerabilities are associated with services

CRAFTING IP PACKETS

- Packet components
 - Source IP address
 - Destination IP address
 - Flags
- Helps obtain information about a service
- Tools:
 - Hping
 - Fping
- Both allow ranges of IP addresses to be scanned and you can also use batch files to automate scanning

FPING

- **With the Fping tool you can ping multiple IP addresses simultaneously**
 - Included on the Kali Linux
 - Accepts a range of IP addresses
 - Entered at a command prompt
 - File containing multiple IP addresses
- **Input file**
 - Usually created with a shell-scripting language so you don't need to type thousands of IP addresses needed for a ping sweep

FPING Command Example

- To ping sweep a range of IP addresses without using an input file, use the command:
 - `fping -g BeginningIPAddress EndingIPAddress`
 - The -g parameter is used when no input file is available
 - Example:
 - `fping -g 192.168.185.1 192.168.185.5`

HPING

- Used to:
 - Perform ping sweeps
 - Bypass filtering devices
 - Allows users to inject modified IP packets
- Powerful tool
 - All security testers must be familiar with tool
 - Supports many parameters

UNDERSTANDING SCRIPTING

- Some tools might need to be modified to better suit your needs as a security tester
- Customized scripts
 - Automates tasks
 - Time saving
 - Requires basic programming skills

SCRIPTING BASICS

- Similar to DOS batch programming
- A script or batch file
 - Text file
 - Contains multiple commands that would be entered manually at the command prompt
- If you find that you are using repetitive commands to perform the same task
 - That task is a good candidate for scripting

KEY TERMS (Reconnaissance)

- **Footprinting**
 - Gathering network information with Web tools
- **Competitive intelligence**
 - Gathered through observation and Web tools
- **IP addresses and domain names**
 - Found by using tools (e.g., SamSpade)
- **Cookies and Web bugs**
 - Collect and retrieve user's information
- **Zone transfers**
 - Used to obtain network topologies

KEY TERMS (Social Engineering)

- **Social engineering**
 - Attacks using human nature
 - Many methods
 - Educate personnel
- **Attacker techniques**
 - Shoulder surfing
 - Dumpster diving
 - Piggybacking
 - Phishing

PLEASE NOTE

**SCANNING PRIVATE/PUBLIC NETWORKS WITHOUT
PERMISSION IS ILLEGAL. YOU ARE ADVISED TO USE
THESE TOOLS RESPONSIBLY.**

NEXT WEEK

- **Learn** the core Metasploit commands to navigate, configure, and run exploits with confidence
- **Practice** finding and understanding vulnerabilities using search, info, and help tools
- **Explore** the Armitage GUI to visually manage targets and exploits more efficiently
- **Understand** credential extraction and pivoting to move through networks like a real pen tester



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

Any Questions?

Trawsnewid Addysg; Trawsnewid Bywydau
Transforming Education; Transforming Lives



www.uwtsd.ac.uk