Network Penetration

Lesson 2: Scanning + Enumeration

Program

- Scanning
  - Intro
  - Live systems
  - Scanning types
  - OS fingerprinting
  - Vulnerabilities
  - Network mapping
  - Proxies
- Enumeration
  - Intro
  - Windows basics
  - Linux basics
  - SNMP
  - Unix/Linux enumeration
  - LDAP
  - NTP
  - SMTP
- Exercises

Introduction to scanning

- Engaging and probing a network
- Creating a more finely grained picture of target
- Uses footprinting information, network fundamentals and a scanner
- Types of scan:
  - Port scan
    - Probing ports to reveal info on hosts
  - Network scan
    - Mapping the network, find live hosts
  - Vulnerability scan
    - Check for potential vulnerabilities

Introduction to scanning

- Information uncovered using scanning:
  - Live hosts on a network
  - Information on the open/closed ports on a host
  - Information on the operating system(s) and the system architecture
  - Services or processes running on hosts
  - Types and seriousness of vulnerabilities
  - Information about patches present on a system
  - Presence of firewalls
  - Addresses of routers and other devices

Live systems

- Checking for live systems
    - Wardialing
        - Dialing up ranges of phone numbers, hoping to reach modems
    - Ping
        - Using Internet Control Message Protocol (ICMP)
    - Port scan
        - Crafting packages to see response

Live systems

- Simple listing of live host on network: arp –a (address resolution protocol)
- Ping
  - Simple ping commands:
    - ping <target IP> or ping <target host – name>
      - Check if live
  - Using nmap:
    - nmap –sP –v <target IP address>
    - Check if IP address is up
    - Provides the media access control (MAC) address, maybe even vendor
    - Ping sweep:
      - nmap –sP –PE –PA<port numbers> <starting IP/ending IP>
      - E.g. nmap –sP –PE –PA21,23,80,3389 <192.168.10.1-50>
      - I needed to remove <> on addresses for this to work
  - Hping3
    - hping3 -1 <domain name>
    - Firewall check: hping3 -c 1 -V -p 80 -s 5050 -A <domain name>
      - -A for ACK, -V for verbose, -p followed by a target port number, and –s for the port on the source

Port status

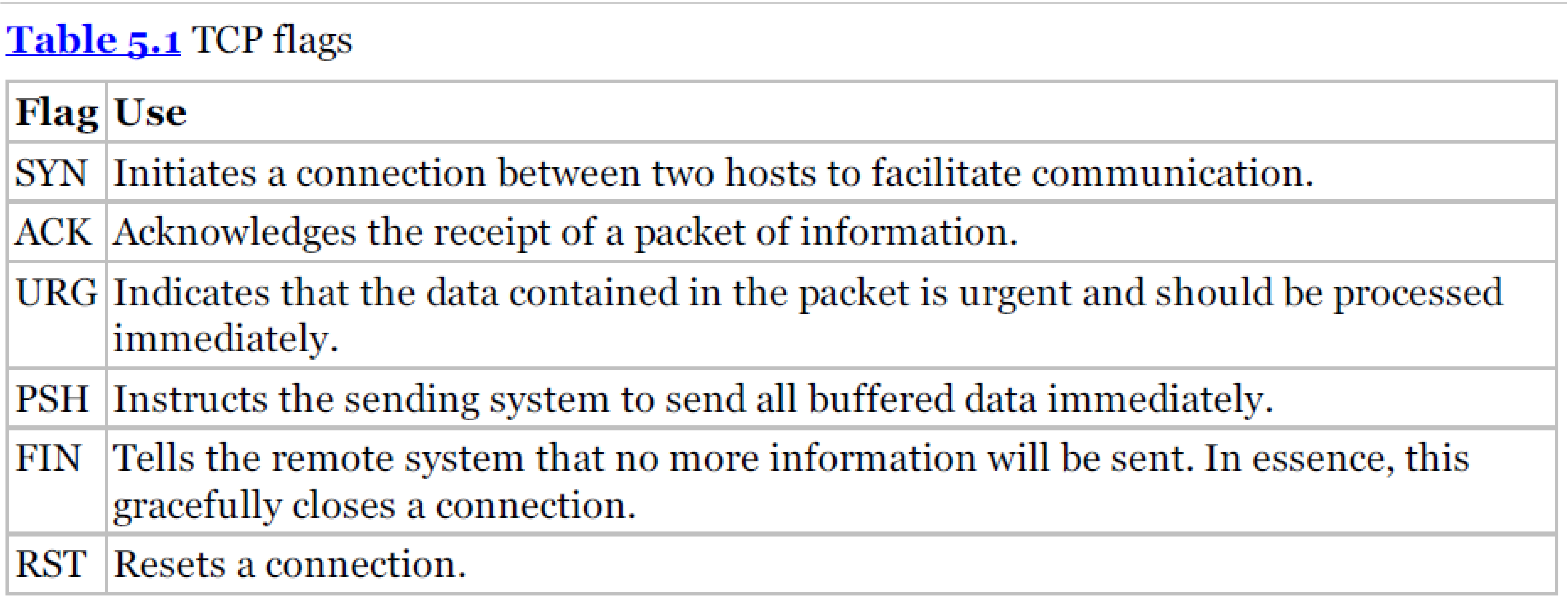


Table 5.1 TCP flags

Flag	Use
SYN	Initiates a connection between two hosts to facilitate communication.
ACK	Acknowledges the receipt of a packet of information.
URG	Indicates that the data contained in the packet is urgent and should be processed immediately.
PSH	Instructs the sending system to send all buffered data immediately.
FIN	Tells the remote system that no more information will be sent. In essence, this gracefully closes a connection.
RST	Resets a connection.

Port status

- Crafting packages using hping3:
  - Create an ACK packet and send it to port 80 on the victim:
    - hping3 –A <target IP address> -p 80
  - Create a SYN scan against different ports on a victim:
    - hping3 -8 50-56 –s <target IP address> -v
  - Create a packet with FIN, URG, and PSH flags set and send it to port 80 on the victim:
    - hping3 –F –P -U <target IP address> -p 80

Scanning types – full open

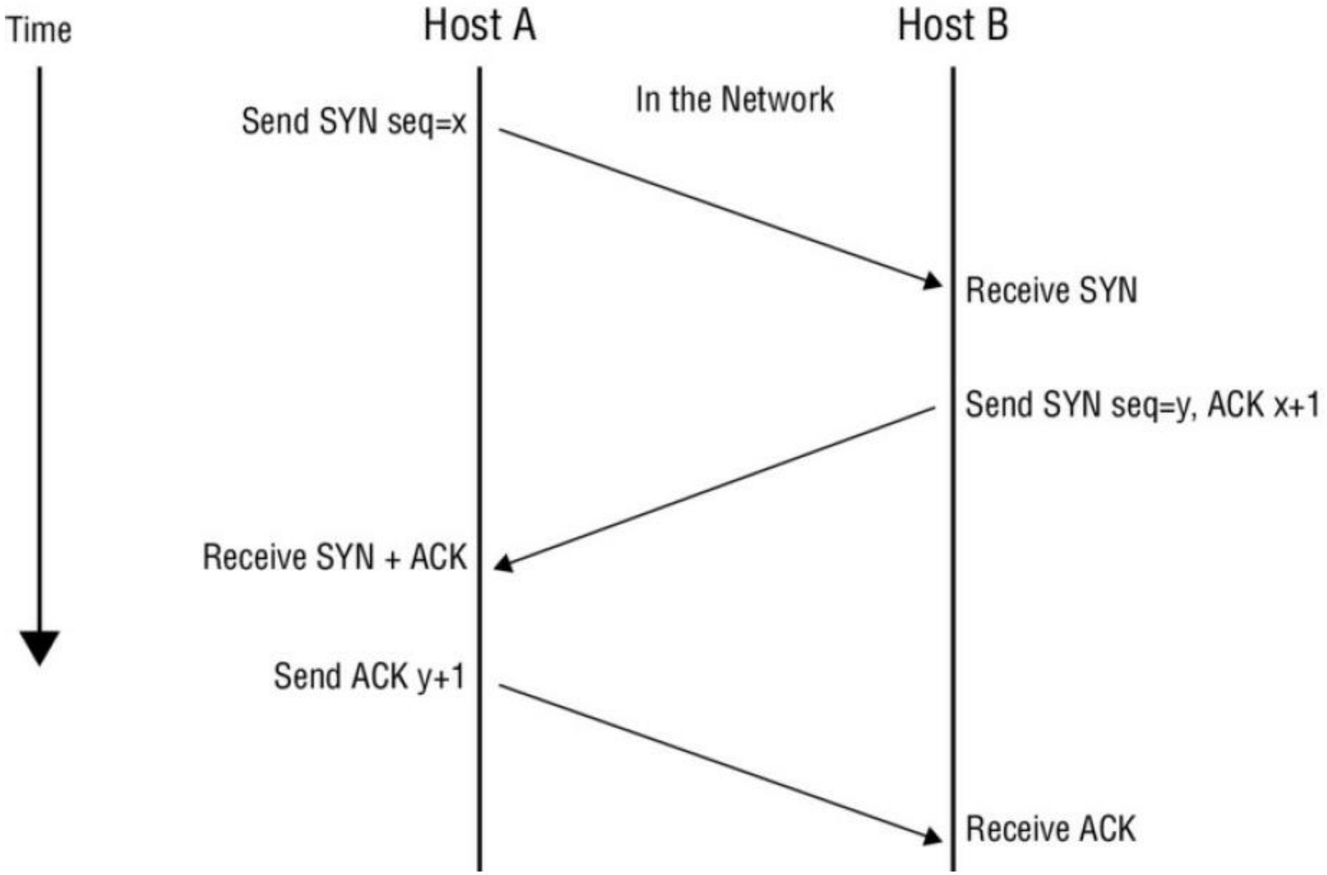


Figure 5.1 The three-way handshake

Scanning types – half open

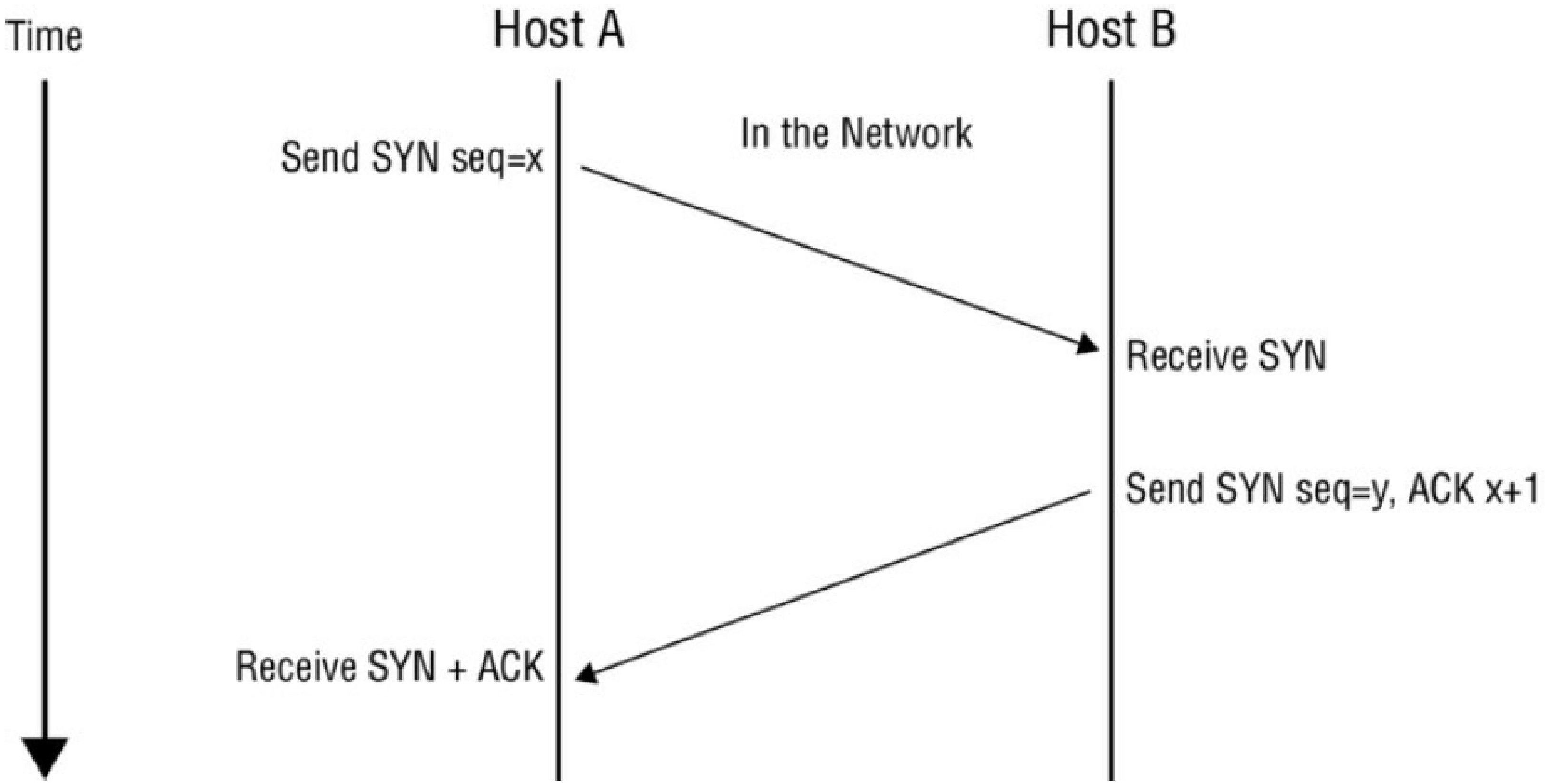


Figure 5.2 Half-open scan against closed and open ports

Scanning types – FIN + NULL

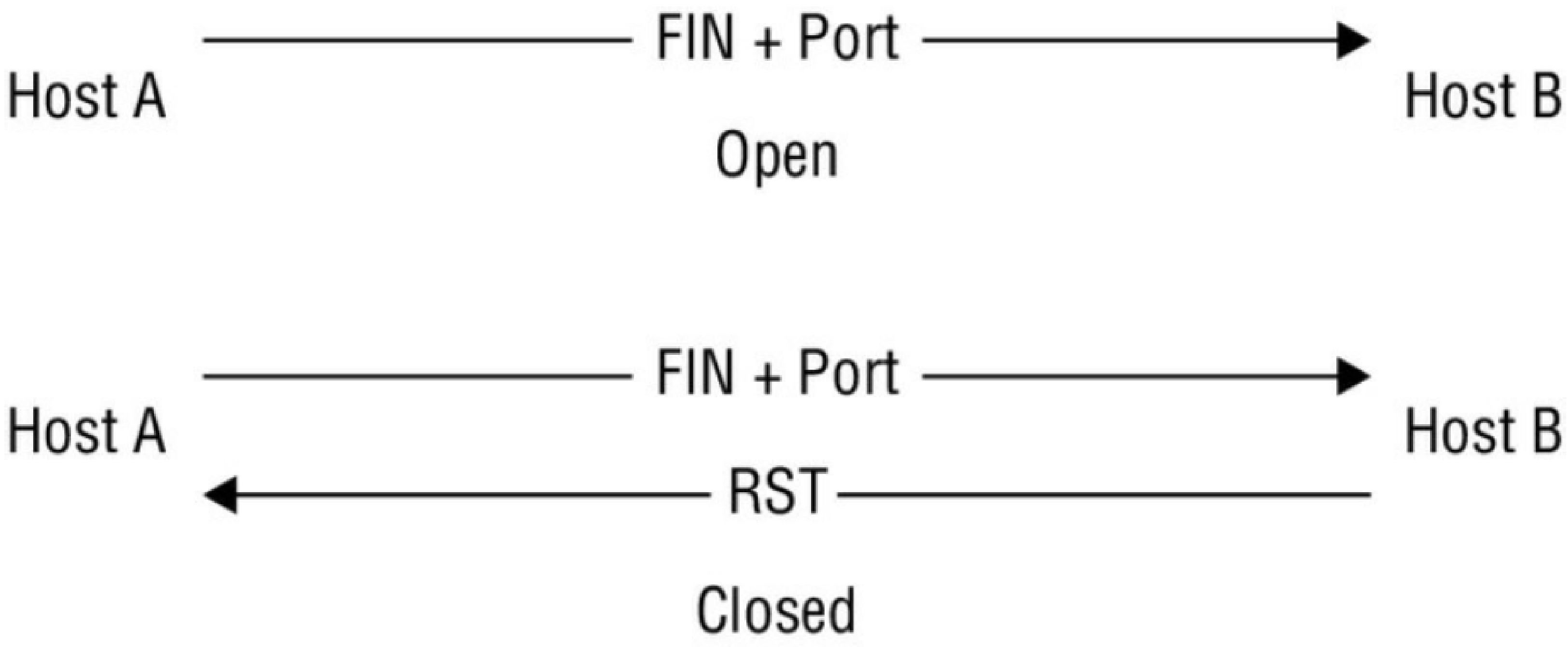


Figure 5.5 A NULL scan against a closed and an open port

Scanning types - Xmas

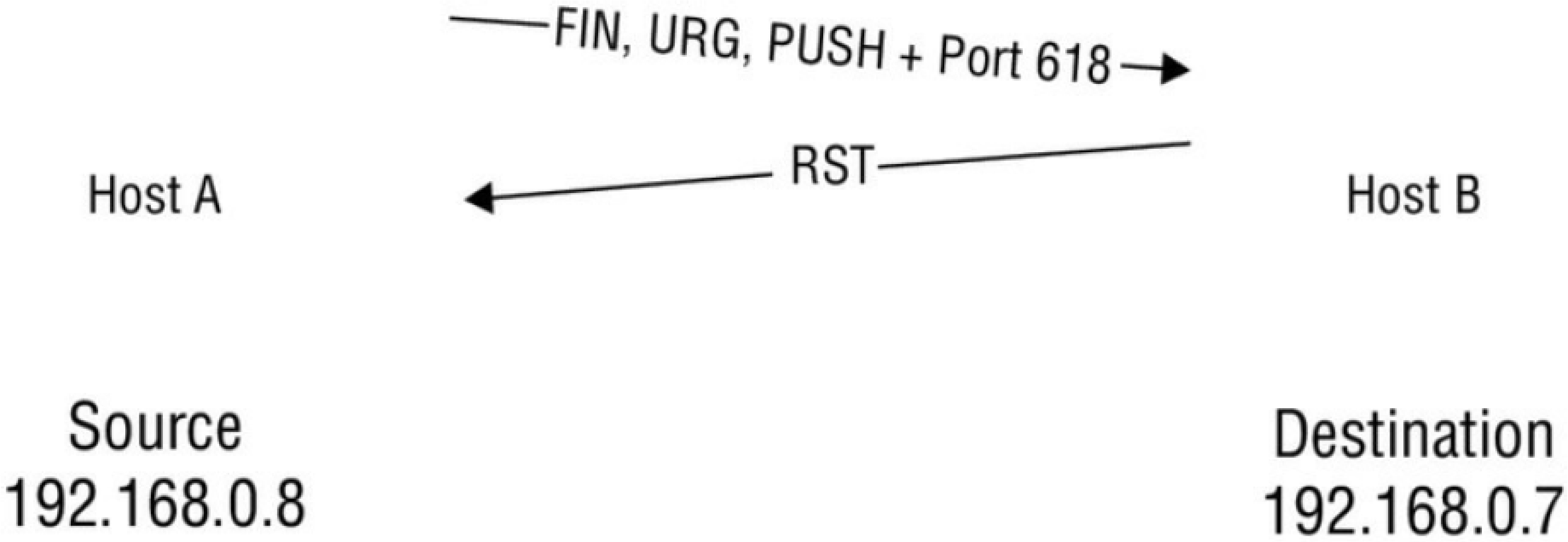


Figure 5.3 Xmas tree scan

Scanning types – further scans

- Idle scan
  - Bounce of helper host (zombie) to hide identity
- ACK scan
  - Check for reach (RST) or no reach (no message or error message)
  - Checks for Stateful Packet Inspection (SPI) in firewall
- Blocked
  - Can help to fragment packages

Scanning types - UDP

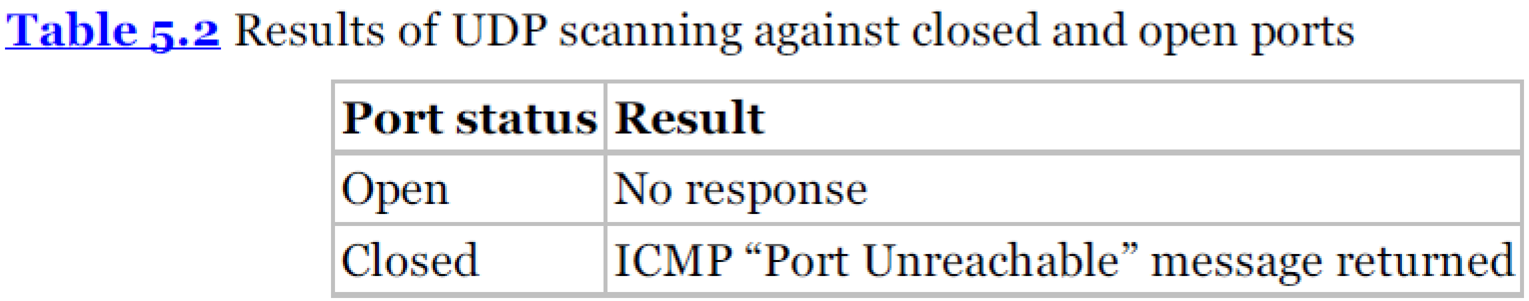


Table 5.2 Results of UDP scanning against closed and open ports

Port status	Result
Open	No response
Closed	ICMP “Port Unreachable” message returned

OS fingerprinting

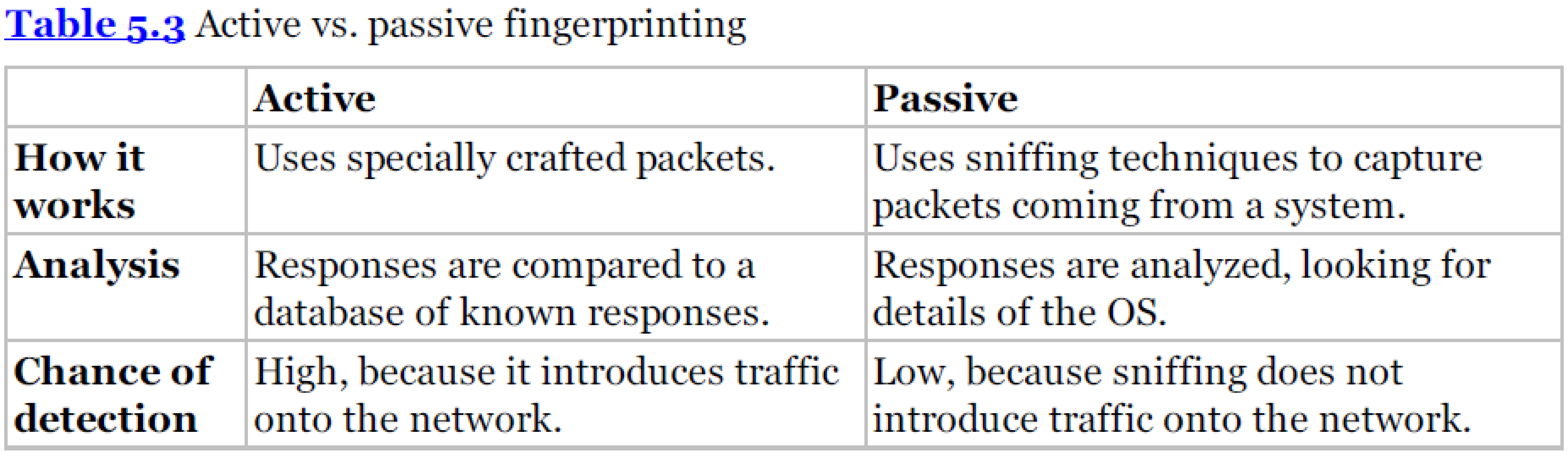


Table 5.3 Active vs. passive fingerprinting

	Active	**Passive**
How it works	Uses specially crafted packets.	Uses sniffing techniques to capture packets coming from a system.
Analysis	Responses are compared to a database of known responses.	Responses are analyzed, looking for details of the OS.
Chance of detection	High, because it introduces traffic onto the network.	Low, because sniffing does not introduce traffic onto the network.

OS fingerprinting

- Based on:
  - IP TTL values
  - IP ID values
  - TCP Window size
  - TCP options (generally, in TCP SYN and SYN+ACK packets)
  - DHCP requests
  - ICMP requests
  - HTTP packets (generally, the User-Agent field)
  - Running services
  - Open port patterns

OS fingerprinting

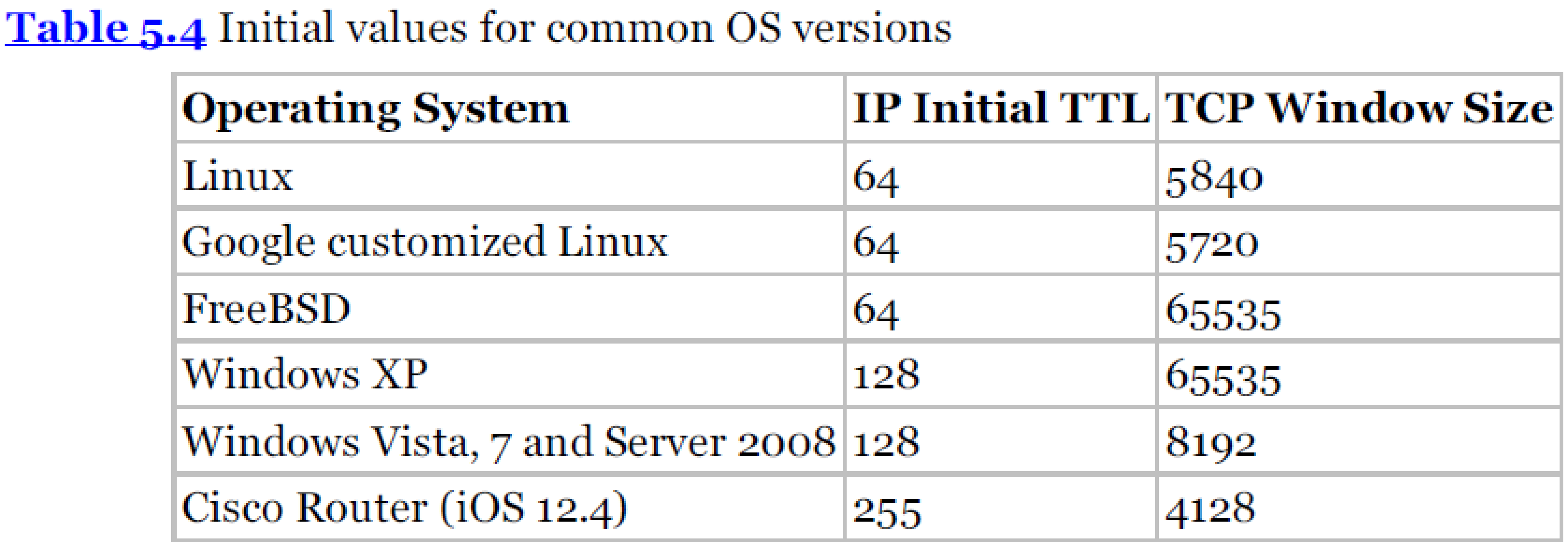


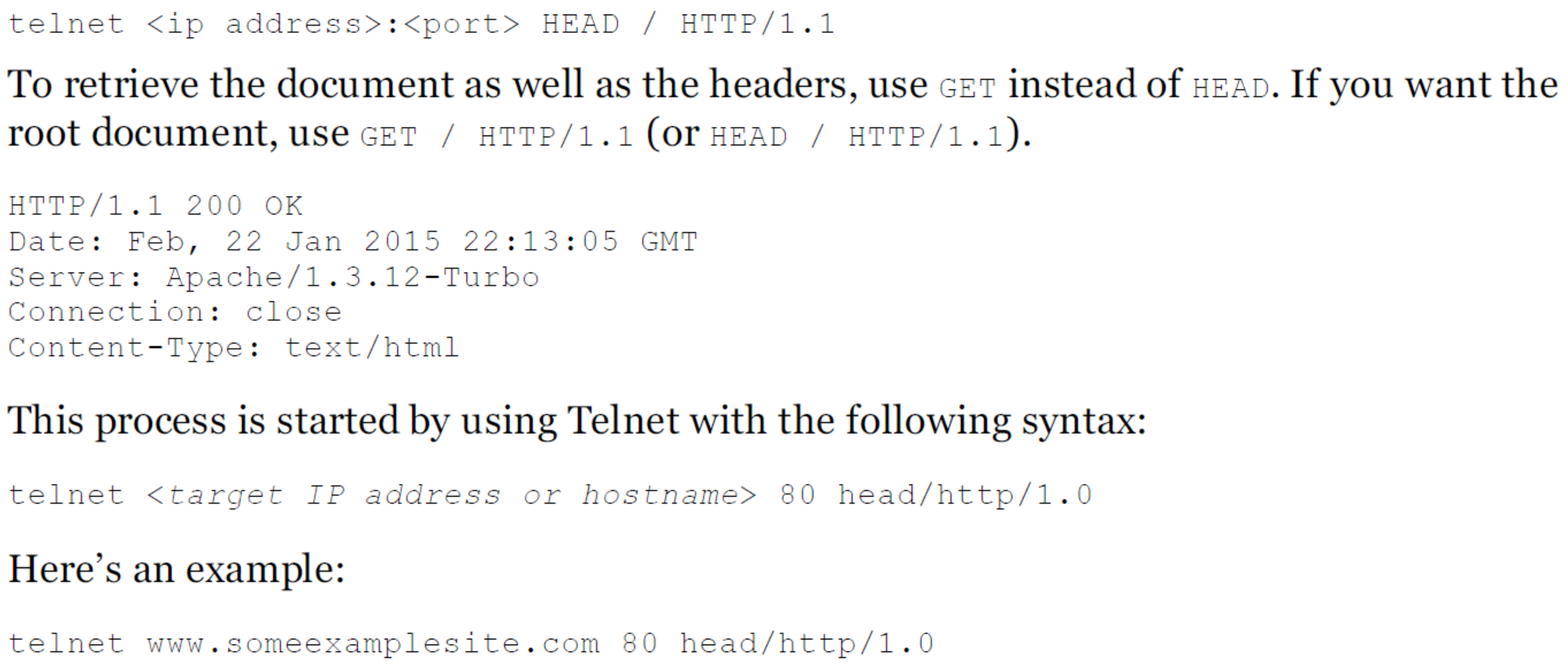
Table 5.4 Initial values for common OS versions

Operating System	IP Initial TTL	TCP Window Size
Linux	64	5840
Google customized Linux	64	5720
FreeBSD	64	65535
Windows XP	128	65535
Windows Vista, 7 and Server 2008	128	8192
Cisco Router (iOS 12.4)	255	4128

- Using nmap:
  - nmap -O <ip address>
- Using p0f
  - p0f –i eth0 (Exercise)

Banner grap

- Banner
  - Returned by service to provide information about itself
  - Can reveal information about host to be exploited
  - Use telnet:



```
telnet <ip address>:<port> HEAD / HTTP/1.1
```

To retrieve the document as well as the headers, use `GET` instead of `HEAD`. If you want the root document, use `GET / HTTP/1.1` (or `HEAD / HTTP/1.1`).

```
HTTP/1.1 200 OK
Date: Feb, 22 Jan 2015 22:13:05 GMT
Server: Apache/1.3.12-Turbo
Connection: close
Content-Type: text/html
```

This process is started by using Telnet with the following syntax:

```
telnet <target IP address or hostname> 80 head/http/1.0
```

Here's an example:

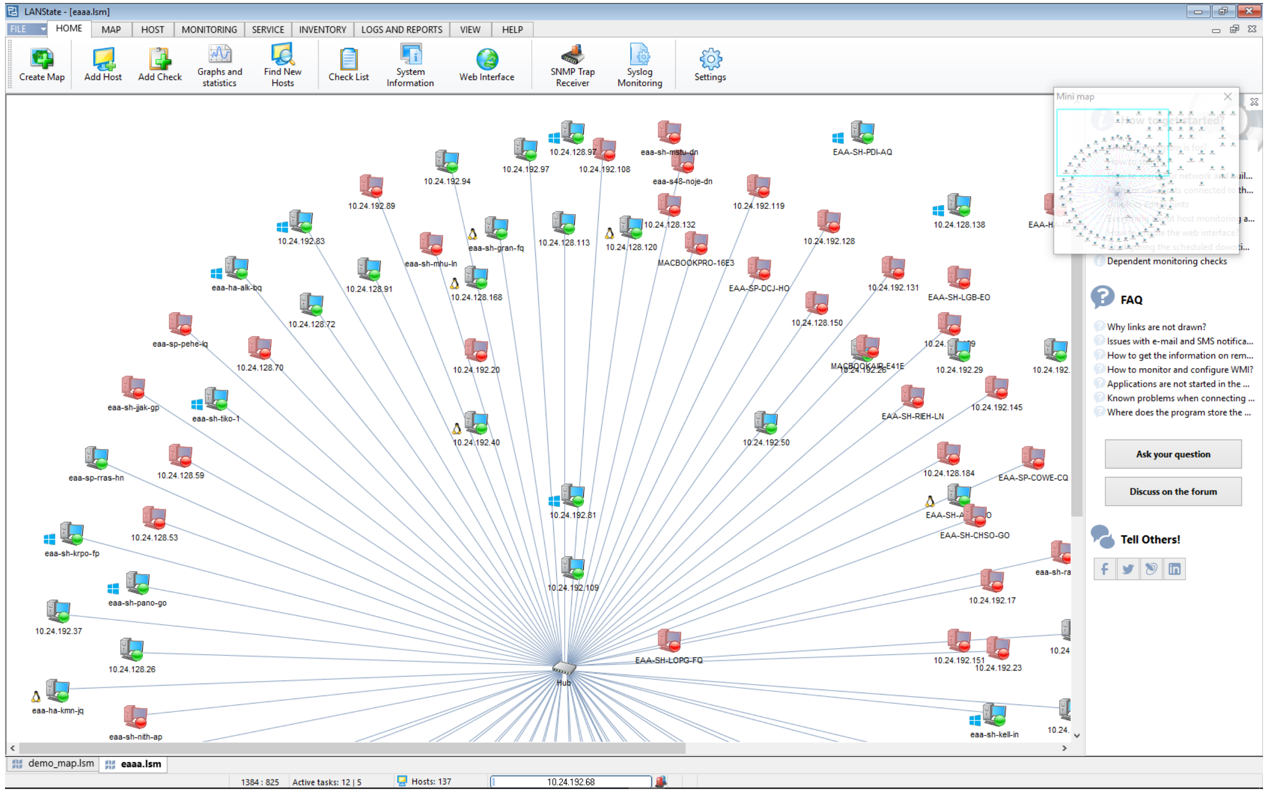
```
telnet www.someexamplesite.com 80 head/http/1.0
```

Vulnerabilities

- Vulnerability:
  - Weakness, with a potential to be exploited
  - E.g. outdates patches
  - Drawback with scanners: Only looks for know problems
  - Tools:
    - Nessus, OpenVAS, Nexpose, Retina
    - Microsoft Baseline Security Analyzer

Network mapping

- Map network
  - Network topology
  - Live/connected hosts
  - Live hardware, e.g. routers, switches
  - Several programs, e.g. LANState



Using proxies

- Stand-in between scanner and target
- Several functions:
  - Filtering traffic in and out of the network
  - Anonymizing web traffic
  - Providing a layer of protection between the outside world and the internal network
- Can be created using whatismyip and public proxy
- Can be created using the TOR network

Scanning

- Tools:
  - Nmap
  - Telnet
  - Netcraft
  - P0f
  - Maltego
  - LANstate

Break

Introduction to enumeration

- Extracting information about:
  - Network resources and shares
  - Users and groups
  - Routing tables
  - Auditing and service settings
  - Machine names
  - Applications and banners
  - SNMP and DNS details

Windows basics

- Guest
  - Mostly not even enabled
  - Very limited capabilities and power
- Administrator
  - Now disabled per default
  - Most accounts are created with admin privileges
    - However, users are prompted when needed (User Account Control)
    - This prevents hidden processes to use the elevated privileges
    - Can be a bit annoying..!
- Processes run under different user contents
- Multiple users can belong to different groups (and privileges)

Windows basics

- Security ID (SID)
  - Whenever an account, a group or computer is created/connected
    - A unique SID is assigned
  - SID’s cannot change, opposed to user names, etc…
  - Guest and Admin accounts have specific SID’s
    - End in 500 for the administrator and 501 for the guest
  - Universal SID’s:
    - S-1-0-0 (Null SID)—This is assigned when the SID value is unknown or for a group without any members.
    - S-1-1-0 (World)—This is a group consisting of every user.
    - S-1-2-0 (Local)—This SID is assigned to users who log on to a local terminal.
- Stored in Security Accounts Manager (SAM)
  - Encrypted and hashed

Linux basics

- Accounts:
  - Username and user ID (UID)
  - Password
  - Primary group name and group ID (GID)
  - Secondary group names and group IDs
  - Location of the home directory
  - Preferred shell
- Stored in format:
  - username:password:UID:GID:name:home directory:shell
  - passwd file:/etc/passwd file or /etc/shadow (root only)
  - Encrypted
- Also provides groups
- Services and ports: See list in the book

Netbios

- Used to access resources on LAN
- Found on port 139
- Tool: nbtstat
    - Name table: nbtstat.exe –a "netbios name of remote system“
    - E.g.: nbtstat -A 192.168.1.10
    - Command line options:
        - -a returns the NetBIOS name table and Media Access Control (MAC) address of the address card for the computer name specified.
        - -A lists the same information as -a when given the target’s IP address.
        - -c lists the contents of the NetBIOS name cache.
        - -n (Names) displays the names registered locally by NetBIOS applications such as the server and redirector.
        - -r (Resolved) displays a count of all names resolved by broadcast or the WINS server.
        - -s (Sessions) lists the NetBIOS sessions table and converts destination IP addresses to computer NetBIOS names.
        - -S (Sessions)

Null session

- Login without giving credentials
- Used only for interprocess communications (IPC) share (internal enumeration)
- May give:
  - List of users and groups
  - List of machines
  - List of shares
  - Users and host SIDs
- Usage:
  - net use \\zelda\ipc$ "" "/user:”
  - net view \\zelda
  - net use s: \\zelda\(shared folder name)
    - Now mapped to S drive

Enumeration tools

- SuperScan
- PsTools
- Finger (unix)

Enumeration with SNMP

- SNMP: Simple Network Management protocol
- SNMP is an Application layer protocol that functions using UDP
- Works through the use of the agent and the management station like so:
  - The SNMP management station sends a request to the agent.
  - The agent receives the request and sends back a reply.
- The messages sent back and forth function by setting or reading variables on a device
- MIB: Management Information Base
  - descriptions of the network objects that can be managed through SNMP

Enumeration with SNMP

- Data, that can be extracted using SNMP:
  - Network resources such as hosts, routers, and devices
  - File shares
  - ARP tables
  - Routing tables
  - Device-specific information
  - Traffic statistics
- Tools:
  - SNMPUtil
  - IP Network Browser
  - SNScan

Unix/Linux enumeration

- Finger (user info):
  - finger <switches> username
- Rpcinfo (remote procedure call info):
  - rpcinfo <switches> hostname
- Showmount (shared directories info):
  - /usr/sbin/showmount [- ade] [hostname]
- Enum4linux (SAMBA info):
  - Group membership information
  - Share information
  - Workgroup or domain membership
  - Remote operating system identification
  - Password policy retrieval

LDAP

- LDAP:
  - Lightweight Directory Access Protocol
  - Used to interact with databases
  - Found on port 389
  - Databases organised in a hierarchical or logical format
  - May use DNS alongside to speed up queries
- Directory services that make use of LDAP:
  - Active Directory
  - Novell eDirectory
  - OpenLDAP
  - Open Directory
  - Oracle iPlanet
- Tools: See list in the book

Enumeration Using NTP

- NTP:
  - Network Time Protocol
  - NTP is used to synchronize the clocks across the hosts on a network
  - Directory services rely on clock settings for logon purposes
  - Uses port 123
  - Commands:
    - ntpdate
    - ntptrace
    - ntpdc
    - Ntpq
  - nmap -sU -pU:123 -Pn -n –script=ntp-monlist <target>
    - –sU defines the scan type, while –pU defines the port for NTP in this case. The –script=ntp-monlist specifies the script being run for NTP enumeration, and the <target> is the IP address of the NTP server

SMTP Enumeration

- SMTP:
  - Simple Mail Transfer Protocol
  - Collect information on mail
- Tools:
  - VRFY – verify existence of email accounts
  - EXPN – return all users on distribution list
  - RCPT TO – identifies recipient of email message
  - Others (non-command prompt):
    - Essential NetTools
    - NetScanTools Pro
- SMTP relay:
  - Send emails through external servers
  - Open relays may be used by spammers