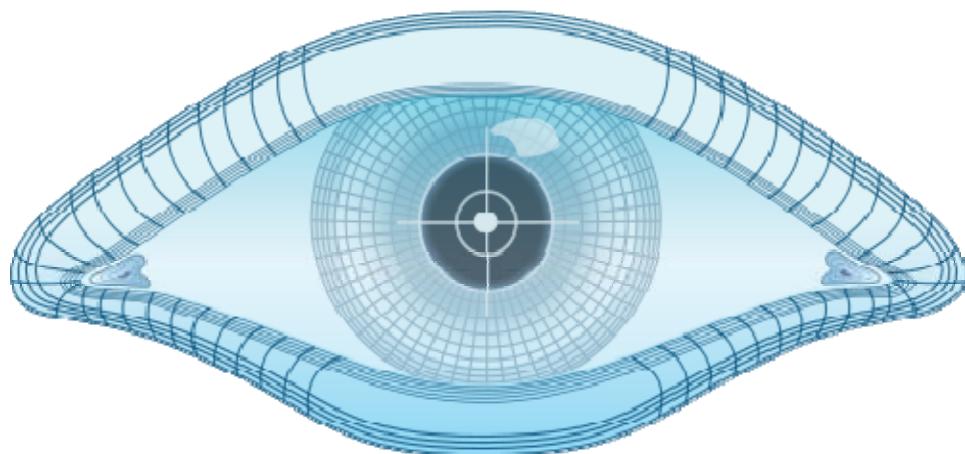


CSCE 629

Cyber Attack

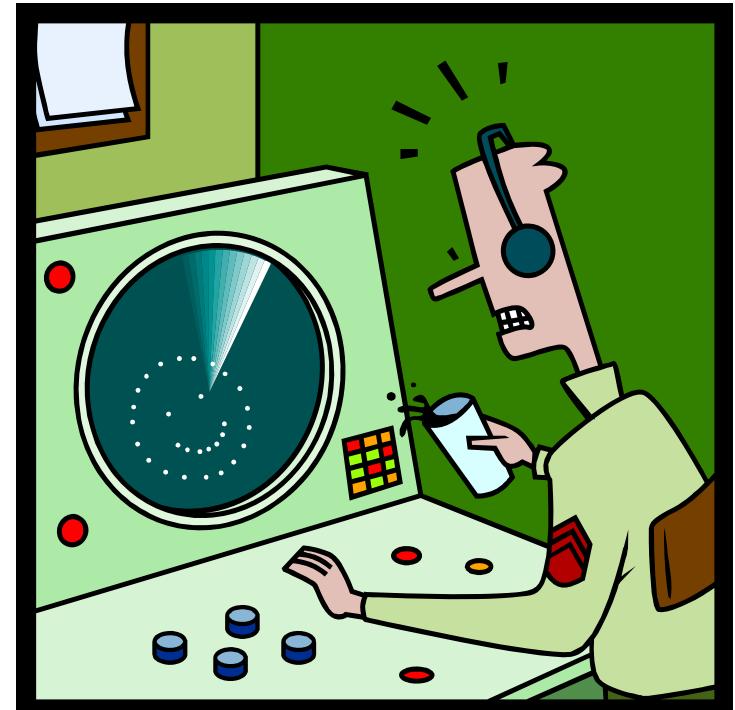
Scanning



Dr. Barry Mullins
AFIT/ENG
Bldg 642
Room 209
255-3636 x7979

define: Scanning

- Recon → searching for **information** about target
- Scanning → searching for
 - ❖ **Systems / computers (IPs) and services / openings (ports)**
- Together, they
 - ❖ Are a critical first step
 - ❖ Identify available avenues of entry / attack vectors

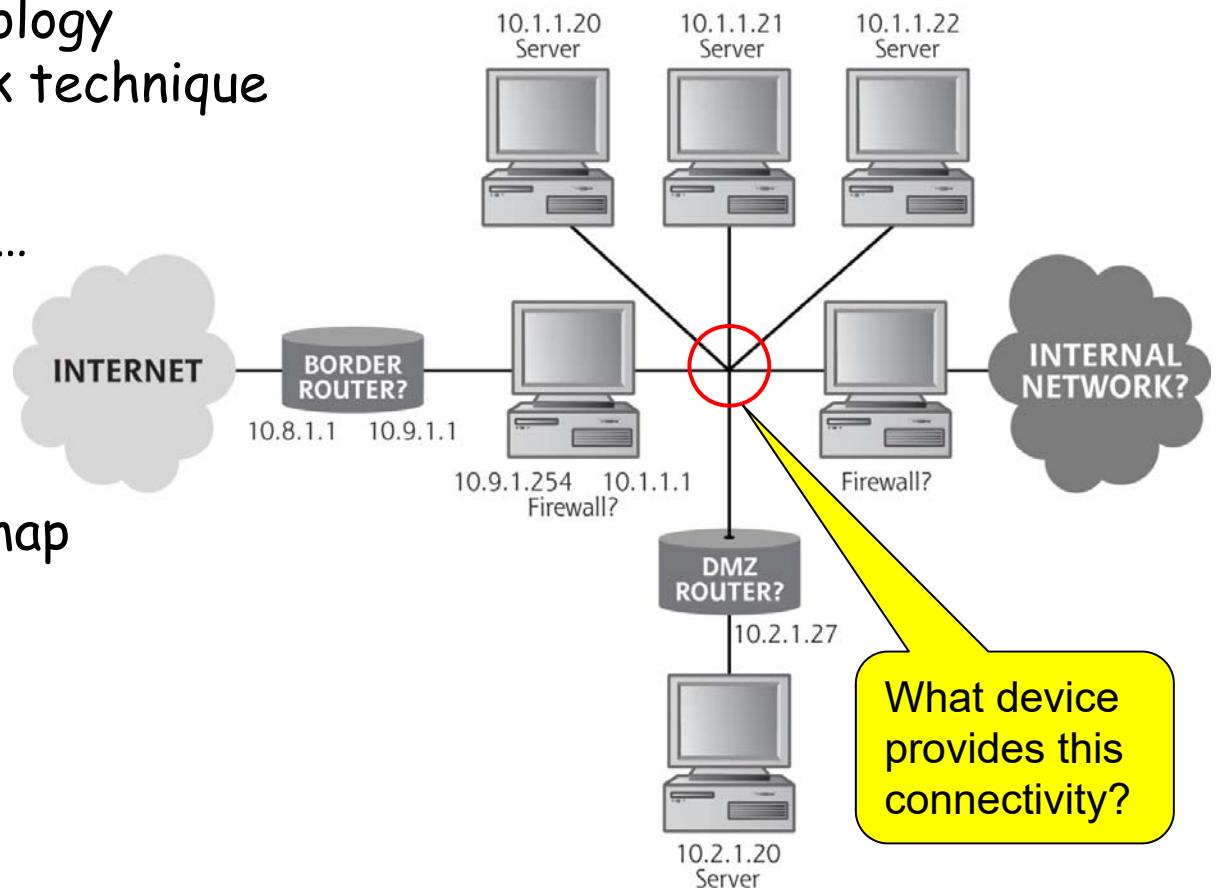


Computer and Network Hacker Exploits

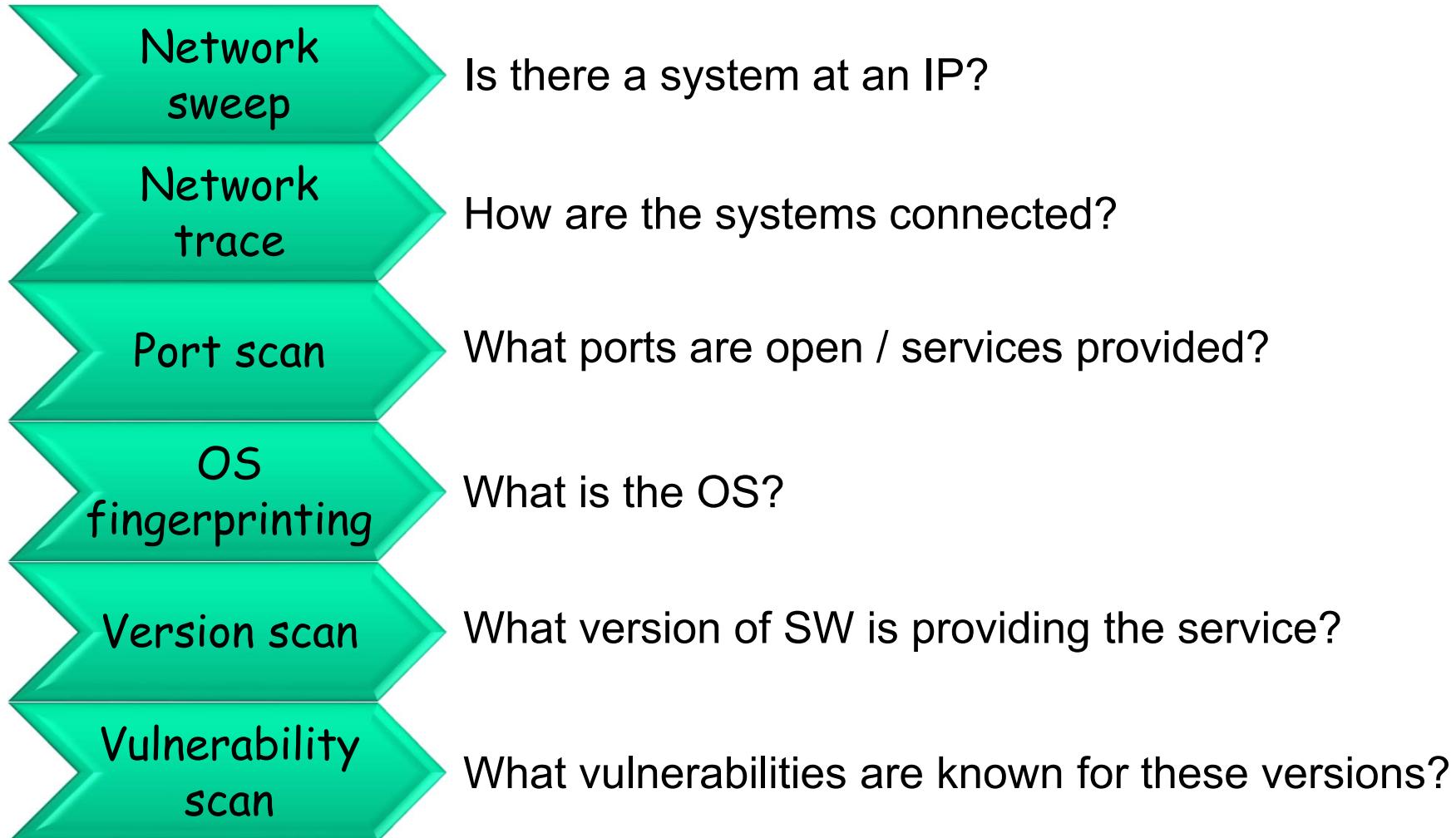
- Step 1: Reconnaissance
- **Step 2: Scanning**
 - ❖ Network Mapping
 - ❖ Determining Open Ports Using Port Scanners
 - ❖ Vulnerability-Scanning Tools
 - ❖ Intrusion Detection System and Intrusion Prevention System Evasion
 - ❖ Shares
- Step 3: Gaining Access
 - ❖ Application and Operating System Attacks
 - ❖ Network Attacks
 - ❖ Denial of Service Attacks
- Step 4: Maintaining Access
- Step 5: Covering Tracks and Hiding

define: "Network Mapping"

- Probe systems to understand the Internet perimeter and topology (the layout of routers and hosts) of the target network
 - ❖ How is the target interfacing with the Internet?
 - ❖ Understanding topology helps decide attack technique
- Looking for addresses...
... and how they are interconnected
- Goal is to generate a map of the network



Scanning Process



Network Mapping Using arp-scan

- Sends ARP request and listens for response

Vmware_3b:d4:e3	Broadcast	ARP	42 Who has 10.1.0.0? Tell 10.1.0.8
Vmware_3b:d4:e3	Broadcast	ARP	42 Who has 10.1.0.1? Tell 10.1.0.8
Dell_b2:c6:60	Vmware_3b:d4:e3	ARP	60 10.1.0.1 is at 00:23:ae:b2:c6:60
Vmware_3b:d4:e3	Broadcast	ARP	42 Who has 10.1.0.2? Tell 10.1.0.8
Adastra_6e:3b:8c	Vmware_3b:d4:e3	ARP	60 10.1.0.2 is at 00:20:0c:6e:3b:8c
Vmware_3b:d4:e3	Broadcast	ARP	42 Who has 10.1.0.3? Tell 10.1.0.8

```
root@kali:~# arp-scan --localnet
```

```
Interface: eth0, datalink type: EN10MB (Ethernet)
Starting arp-scan 1.9 with 2048 hosts (http://www.nta-monitor.org)
10.1.0.1      00:23:ae:b2:c6:60      Dell Inc.
10.1.0.2      00:20:0c:6e:3b:8c      ADASTRA SYSTEMS CORP.
10.1.0.3      48:0f:cf:50:38:bd      (Unknown)
10.1.0.4      2c:41:38:4f:3d:ce      Hewlett-Packard Company
10.1.0.5      48:0f:cf:50:38:cc      (Unknown)
                                <<snip>>
10.1.5.91     dc:4a:3e:70:27:89      (Unknown)
10.1.5.98     80:2a:a8:1d:b7:72      (Unknown)
10.1.5.99     08:00:27:a5:b4:f8      CADMUS COMPUTER SYSTEMS
10.1.5.102    48:0f:cf:50:19:7b      (Unknown)
10.1.6.25     08:00:27:dc:a6:21      CADMUS COMPUTER SYSTEMS
```

192 packets received by filter, 0 packets dropped by kernel

Ending arp-scan 1.9: 2048 hosts scanned in 9.129 seconds (224.34 hosts/sec). 192 responded

Effective beyond the subnet?
No. Why?

Network Mapping using Ping Sweeps

- Packet InterNet Groper (PING)
 - ❖ Sends an ICMP echo request (type 8, code 0)
 - ❖ Waits for an ICMP echo reply (type 0 , code 0)
- Also great for resolving an IP address from hostname

```
C:\Users\bmullins.CDN>ping fs-cdn-01
```

```
Pinging fs-cdn-01.CDN.LOCAL [10.1.2.7] with 32 bytes of data:  
Reply from 10.1.2.7: bytes=32 time<1ms TTL=64  
Reply from 10.1.2.7: bytes=32 time<1ms TTL=64
```

- Ping sweeps can be defeated by blocking incoming ICMP messages

Ping Sweeps With Scapy

sr() function sends layer 3 packets and receives answers

Send an IP packet containing an ICMP PING (default) payload

ans,unans=sr(IP(dst="10.1.0.1-254")/ICMP(),timeout=1)

sr returns ans → list of couples (packet sent, answer)
unans → list of unanswered packets

Print the received packet's IP source address

ans.summary(lambda (s,r): r.printf("%IP.src% is alive"))

lambda (s,r) is an anonymous function accepting sent (s) and received (r) packets

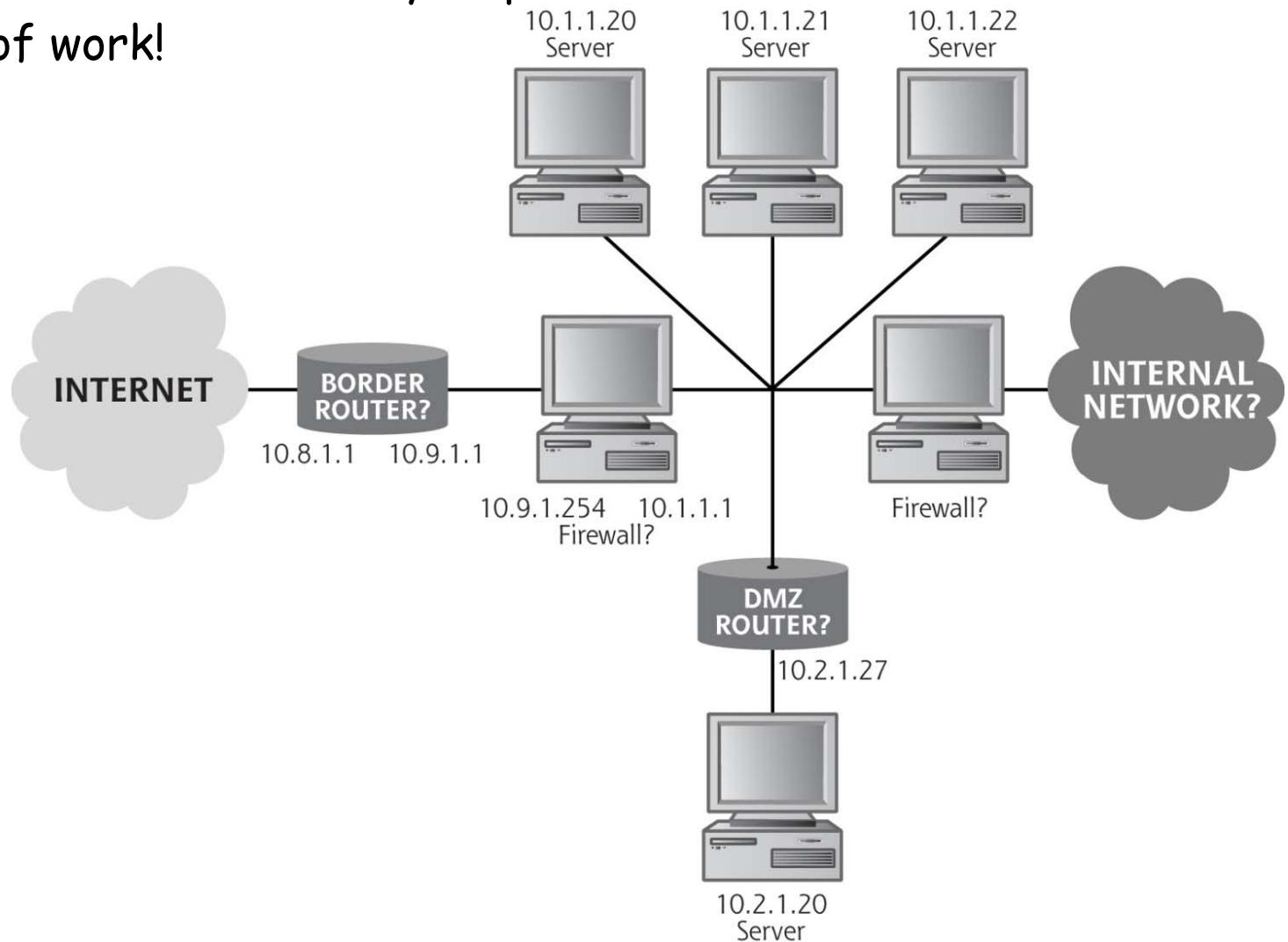
```
>>> ans.summary(lambda (s,r): r.printf("%IP.src% is alive"))
10.1.0.1 is alive
10.1.0.3 is alive
10.1.0.2 is alive
10.1.0.4 is alive
```

Network Mapping using TCP / UDP

- Send TCP SYN packet to a port commonly open (e.g., 80)
 - ❖ `ans,unans=sr(IP(dst="10.1.0.*")/TCP(dport=80,flags="S"),timeout=1)`
 - ❖ `ans.summary(lambda (s,r): r.printf("%IP.src% is alive"))`
 - ❖ Target listening on that port → attacker receives SYN-ACK
 - There is a machine at that address
- Send a UDP packet to an unlikely port
 - ❖ `ans,unans=sr(IP(dst="10.1.1-7.1-10")/UDP(dport=0),timeout=1)`
 - ❖ `ans.summary(lambda (s,r): r.printf("%IP.src% is alive"))`
 - ❖ Target responds with ICMP port unreachable message
 - There is a machine at that address
- For both above,
 - if I get ANY response, there is a machine at that address

Network Mapping using Traceroute

- Can use traceroute to manually map a network
 - ❖ A LOT of work!



Computer and Network Hacker Exploits

- Step 1: Reconnaissance
- **Step 2: Scanning**
 - ❖ Network Mapping
 - ❖ Determining Open Ports Using Port Scanners
 - ❖ Vulnerability-Scanning Tools
 - ❖ Intrusion Detection System and Intrusion Prevention System Evasion
 - ❖ Shares
- Step 3: Gaining Access
 - ❖ Application and Operating System Attacks
 - ❖ Network Attacks
 - ❖ Denial of Service Attacks
- Step 4: Maintaining Access
- Step 5: Covering Tracks and Hiding

Port Scanners

- Now we have
 - ❖ IP addresses of systems
 - ❖ Very basic understanding of the topology
- Still need
 - ❖ What ports (processes/services) are listening on these IPs?
 - Attacker can focus attack based on open ports
- Port scanners send packets to ports to determine what's listening
 - ❖ If a system responds,
 - that port is listening and
 - associated service is available

Nmap by Fyodor (Gordon Lyon)

- "Network exploration tool and security / port scanner"



Title : The Art of Scanning

Author : Fyodor

---[Phrack Magazine Volume 7, Issue 51 September 01, 1997, article 11 of 17

-----[The Art of Port Scanning

-----[Fyodor <fyodor@dhp.com>

[Abstract]

This paper details many of the techniques used to determine what ports (or similar protocol abstraction) of a host are listening for connections. These ports represent potential communication channels. Mapping their existence facilitates the exchange of information with the host, and thus it is quite useful for anyone wishing to explore their networked environment, including hackers. Despite what you have heard from the media, the Internet is NOT all about TCP port 80. Anyone who relies exclusively on the WWW for information gathering is likely to gain the same level of proficiency as your average AOLer, who does the same. This paper is also meant to serve as an introduction to and ancillary documentation for a coding project I have been working on. It is a full featured, robust port scanner which (I hope) solves some of the problems I have encountered when dealing with other scanners and when working to scan massive networks. The tool, nmap, supports the following:

Nmap by Fyodor

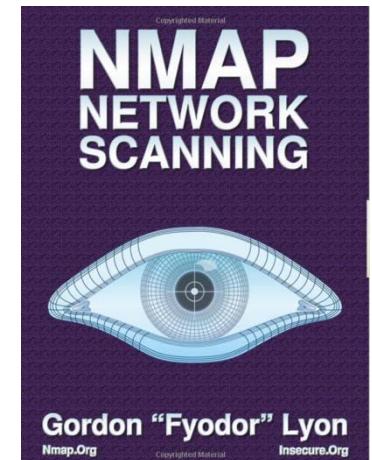


- GUI version available (Zenmap) in Unix or Windows
 - ❖ Basically generates command line from GUI inputs
- nmap.org
- Featured in The Matrix Reloaded



```
1/tcp      nmap      host<2-ns      [mobile]
0: [ ] Starting nmap 0.2.54BETA25
1: Insufficient responses for TCP sequencing (3), OS detection may be less
2: accurate
3: Interesting ports on 10.2.2.2:
3: (The 1539 ports scanned but not shown below are in state: closed)
4: Port      State      Service
4: 22/tcp    open       ssh
1:
1: No exact OS matches for host
8:
8: Nmap run completed -- 1 IP address (1 host up) scanned
8: # sshnuke 10.2.2.2 -rootpw="210N0101"
4: Connecting to 10.2.2.2:ssh ... successful.
0: Attempting to exploit SSHv1 CRC32 ... successful.
Resetting root password to "210N0101".
System open: Access Level <9>
P: # ssh 10.2.2.2 -l root
root@10.2.2.2's password:
1: PRE_CONTROL > disable grid nodes 21 - 48
```

nmap.org/book/toc.html



Nmap in The Bourne Ultimatum



The screenshot shows a terminal window with several panes. The main pane displays Nmap version 4.01 output for the host guardian.telservice.net (IP 205.217.10.14). It lists open ports 22/tcp (ssh), 25/tcp (smtp), and 53/tcp (domain).

Port	State	Service	Version
22/tcp	open	ssh	SSH 3.9.1 (proto 2.0)
25/tcp	open	smtp	Postfix smtpd
53/tcp	open	domain	

Below the Nmap output, a "Bash Terminal" pane shows a login session:

```
Lost login:19:01:41 on console
Welcome to CRI!
SECOM Interagency Contract Network 6674
Mark-Coleron:- mcoleron$ show tog 443 -loading....
```

On the left side of the interface, there are two vertical panes labeled "HOSTS" and "SERVICES". The "HOSTS" pane lists IP ranges and their status (e.g., 192.168.1.0/24, 192.168.1.219, 192.168.1.220-221). The "SERVICES" pane lists various services like ssh, smtp, and domain.

On the right side, there is a "Bash Terminal" pane showing an email inbox:

```
loading...
Chain 14, L File 23
From: adr...
Subject: f1...
Date: 17:51
To: simon...
Return-Path: ...
Delivery-Date: ...
Received: ...
id 1D3Nwf-0...
Envelope-To: ...
Message-ID: ...
Ross, Simon...
Flight-(K50...
Outbound...
Flight 253...
Status: ...
Class of Ser...
Depart: ...
Arrive: ...
```

Nmap in Ocean's 8



Nmap



I know you're what you're thinking...
This movie stuff is a fantasy world. Why should I care about nmap?



President George W. Bush visited the NSA headquarters at Fort Meade in January 2006

nmap [Scan Type ...] [Options] {target specification }

Nmap GUI (aka Zenmap)

Built into Kali or install in Windows (nmap.org/download.html)

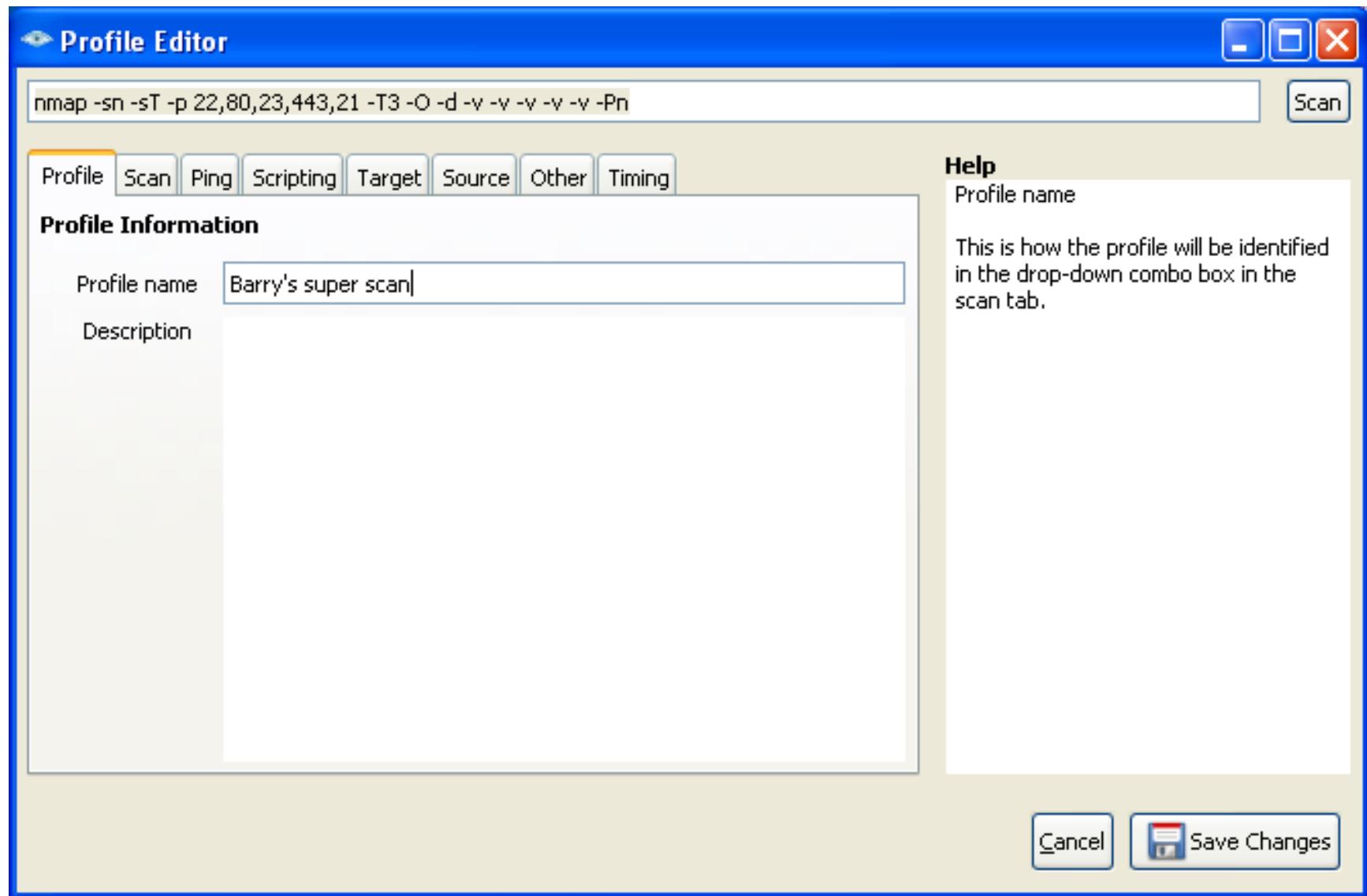
The screenshot shows the Zenmap interface. At the top, there's a menu bar with Scan, Tools, Profile, and Help. A yellow callout points to the Profile menu item with the text "Create a Profile first as shown on next slide". Below the menu is a toolbar with Target, Profile, Scan, and Cancel buttons. The Target dropdown is set to 10.1.3.1-10, and the Profile dropdown is set to Barry's super scan. A yellow callout points to the Command field below, which contains the command nmap -T4 -A -v 10.1.3.1-10, with the text "Command line is shown and editable". The main window has tabs for Hosts, Services, Nmap Output (which is selected), Ports / Hosts, Topology, Host Details, and Scans. The Nmap Output tab displays a table of results:

Port	Protocol	State	Service	Version
135	tcp	open	msrpc	Microsoft Windows RPC
139	tcp	open	netbios-ssn	Microsoft Windows 98 netbios-
445	tcp	open	microsoft-ds	Microsoft Windows 10 microsof
903	tcp	open	vmware-auth	VMware Authentication Daemo
1025	tcp	open	msrpc	Microsoft Windows RPC
1026	tcp	open	msrpc	Microsoft Windows RPC
1027	tcp	open	msrpc	Microsoft Windows RPC
1028	tcp	open	msrpc	Microsoft Windows RPC
1141	tcp	open	msrpc	Microsoft Windows RPC
5432	tcp	open	postgresql	PostgreSQL DB

A yellow callout at the bottom right of the table area says "Nmap sends packets to the target looking for a response". At the bottom of the interface are buttons for Filter Hosts and a scroll bar.

nmap [Scan Type ...] [Options] {target specification }

Nmap GUI (aka Zenmap)



Nmap - Scan Types

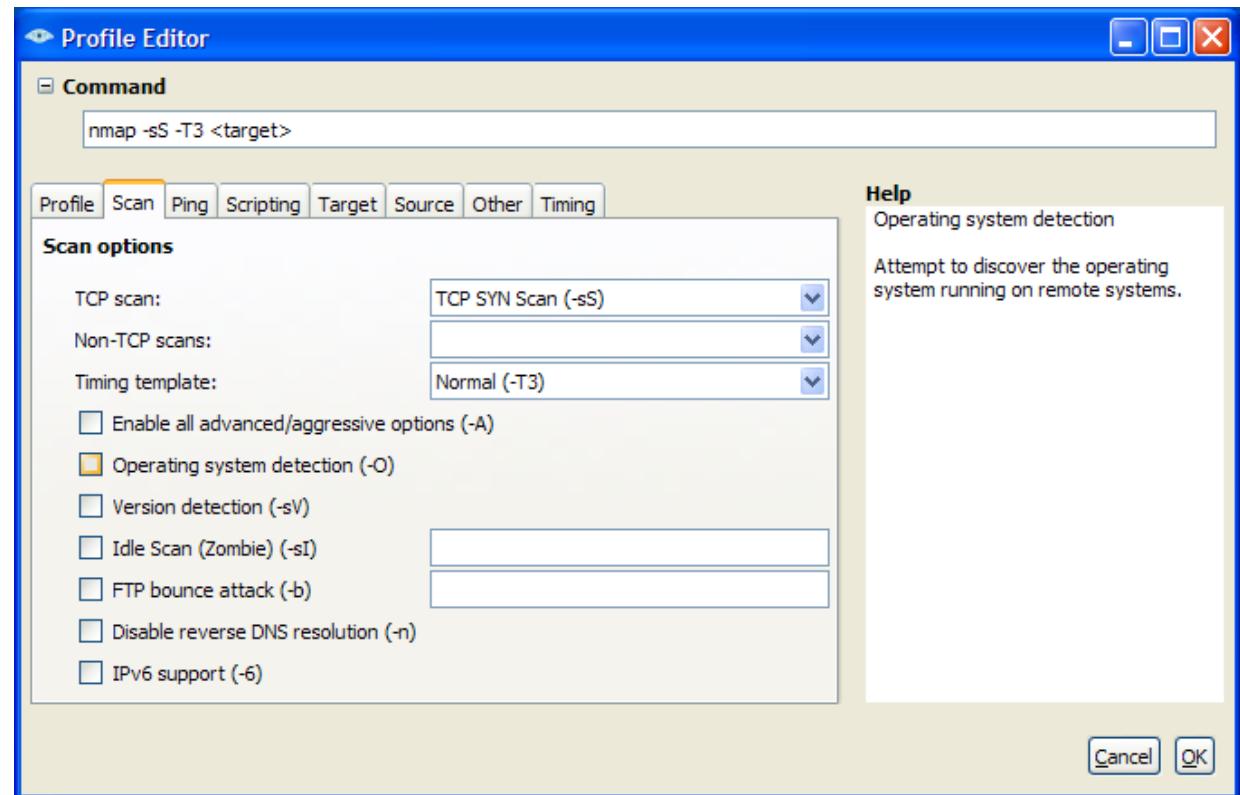
- TCP Connect scan
 - ❖ Completes three-way handshake
 - ❖ Not stealthy
- TCP SYN scan ("half-open" scans)
 - ❖ Only send initial SYN
 - ❖ Receive SYN-ACK → Port is open
 - ❖ Stealthier than connect scan
 - Still can ID the attacker using IP addr of SYN pkt
 - ❖ Faster than connect scan
- TCP FIN scan
 - ❖ Send FIN to ports
 - ❖ Receive RESET → closed
 - ❖ Receive nothing → probably open
 - ❖ Stealthier than connect scan



Nmap - Scan Types

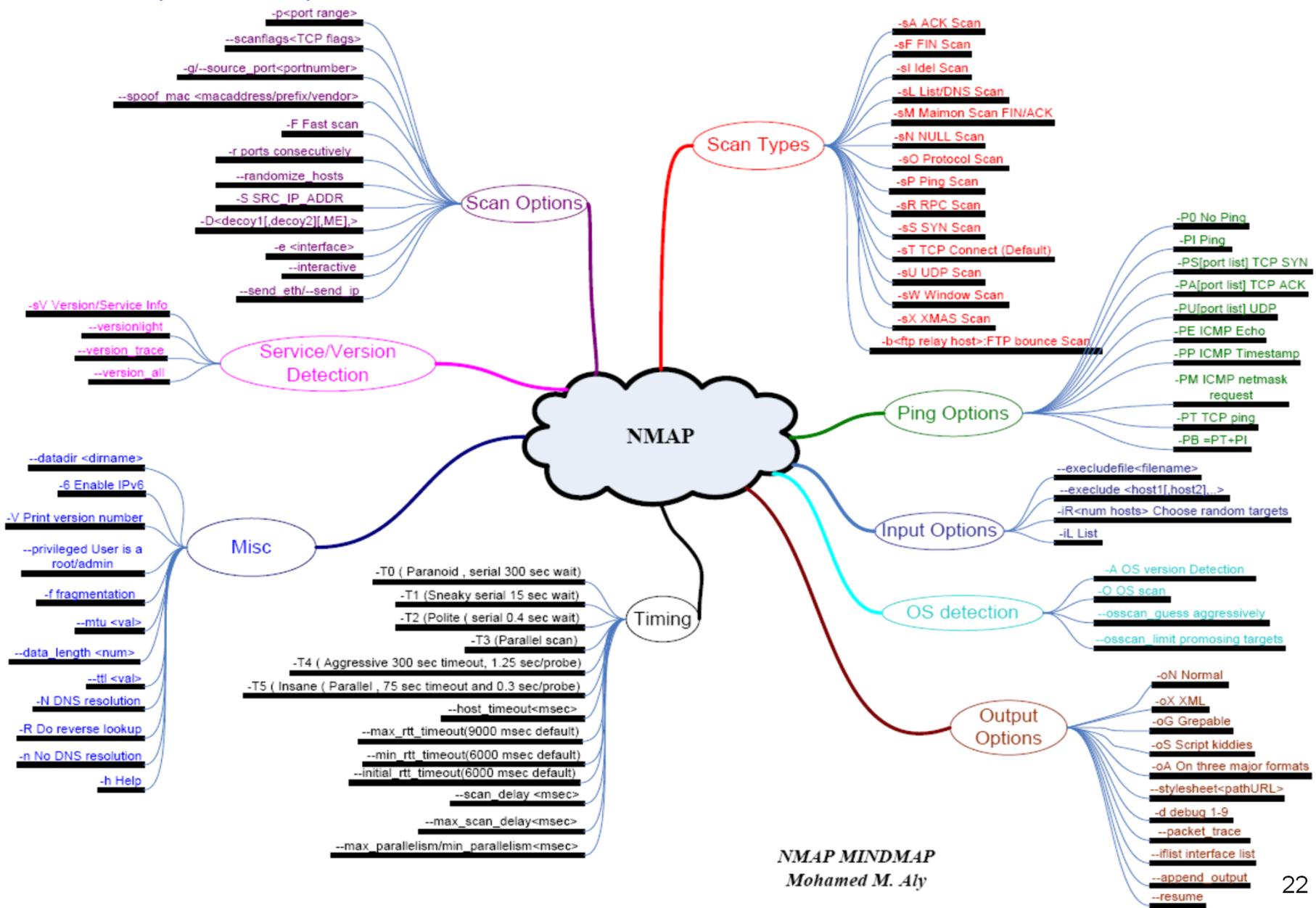
- ❑ TCP Xmas tree scan → Send a packet with **all** control bits set
- ❑ TCP null scan → Send a packet with **no** control bits set
 - ❖ Receive RESET → closed
 - ❖ Receive nothing → probably open

- ❑ Discussed later
 - ❖ "Idle" Scanning
 - ❖ Version Scanning



nmap [Scan Type ...] [Options] {target specification }

Nmap - Options Galore



Nmap Command Line Examples

nmap [Scan Type ...] [Options] {target specification }

```
root@kali:~/Desktop# nmap fs-cdn-01
```

Run a default TCP connect scan against target

```
Starting Nmap 7.70 ( https://nmap.org ) at 2019-01-07 14:41 EST
```

```
Nmap scan report for fs-cdn-01 (10.1.2.7)
```

```
Host is up (0.015s latency).
```

```
Not shown: 990 closed ports
```

PORT	STATE	SERVICE
------	-------	---------

80/tcp	open	http
--------	------	------

111/tcp	open	rpcbind
---------	------	---------

139/tcp	open	netbios-ssn
---------	------	-------------

443/tcp	open	https
---------	------	-------

445/tcp	open	microsoft-ds
---------	------	--------------

548/tcp	open	afp
---------	------	-----

2049/tcp	open	nfs
----------	------	-----

3261/tcp	open	winshadow
----------	------	-----------

5000/tcp	open	upnp
----------	------	------

5001/tcp	open	commplex-link
----------	------	---------------

```
MAC Address: 00:11:32:32:6F:61 (Synology Incorporated)
```

Any host running logging software will easily detect this type of scan

```
Nmap done: 1 IP address (1 host up) scanned in 5.51 seconds
```

```
root@kali:~/Desktop#
```

Nmap Command Line Examples

nmap [Scan Type ...] [Options] {target specification }

nmap -A -Pn -p 1-65535 -oN <filename> <ip address>

- Use TCP connect scan (default)
- **-A** → Performs OS fingerprinting, version scan, script scan, and traceroute
- **-Pn** → nmap will not ping the machine before scanning it
 - ❖ Useful if target blocks ICMP pings. Without this option, if the remote machine does not respond to pings, nmap will report that the machine is down and not scan.
- **-p 1-65535** → ports to scan **-p-** → Shorthand for scan all ports
 - ❖ If time permits, scan all 65,535 ports (1-65535)
 - ❖ Single port: 80 (nmap -A -p 80)
 - ❖ List of ports: 135,137-139,445 (nmap -A -p 135,137-139,445)
- **-oN <filename>** → Sends scan output to a file. Depending on number of machines, sending scan output to a text file is recommended.
- **<ip address>** → Scan single IP address or range of IP addresses
 - ❖ Single: nmap -A -p 1-65535 **10.1.1.1**
 - ❖ Range: nmap -A -p 1-65535 **10.1.1.1-254**
 - ❖ Range: nmap -A -p 1-65535 **fs-cdn-01/24**
 - ❖ List: nmap -A -p 1-65535 **10.1.1.2,4,8,16,32,64,128**

Nmap Command Line Examples

- **nmap -sV -p- 198.116.0-255.1-127**
 - ❖ **-sV** → version / service information
 - If any port is found open, version detection is used to determine what application is running
 - ❖ **-p-** → Scan all ports
 - ❖ Target IPs → first half of each of the 255 possible subnets in the 198.116. address space
- **nmap -v -iR 100000 -Pn -p 80**
 - ❖ **-v** → enables verbose mode
 - ❖ **-iR 100000** → Asks nmap to choose 100,000 IPs at random
 - ❖ **-p 80** → scan hosts for web servers (port 80)
 - ❖ **-Pn** → no ping
- **nmap -p 80 --open 192.168.1.0/24**
 - ❖ **--open** → only display IPs with port 80 open

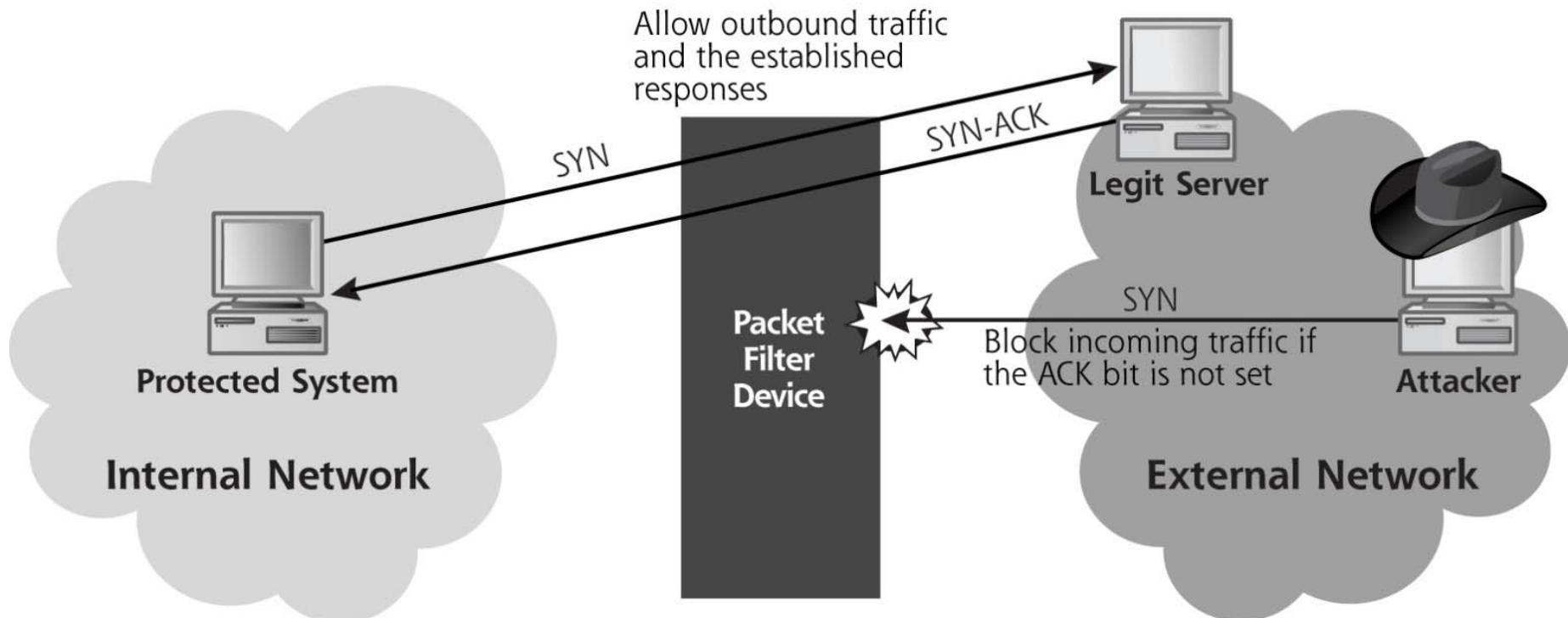
Firewalls - Review



- Packet Filtering
 - ❖ Inspects each packet individually
 - ❖ Packets allowed through based on this single packet
- Stateful packet filtering
 - ❖ Remembers previous packets and tries to correlate new packets with previous traffic in order to make filtering decision
 - ACK packet will be allowed only if destined for an IP/port number used by an earlier SYN sent out of the network
- Proxy firewalls (application layer)
 - ❖ First, sender makes a connection to the proxy
 - ❖ Then, proxy makes a separate connection to destination
 - ❖ Packet header information is modified

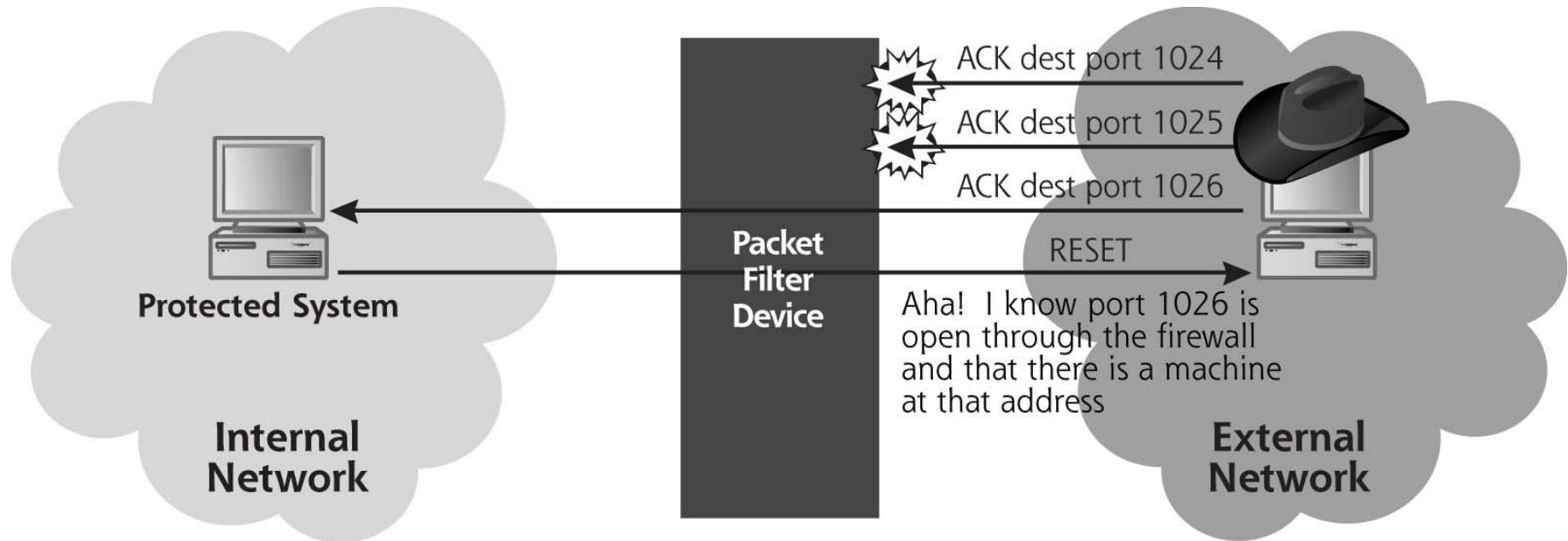
Firewalls - Review

- Suppose firewall allows outgoing connections, but blocks incoming
 - ❖ Allow outgoing SYNs
 - ❖ Allow incoming connections (packets) only if ACK bit is set
 - ❖ Blocks connection attempts from the outside



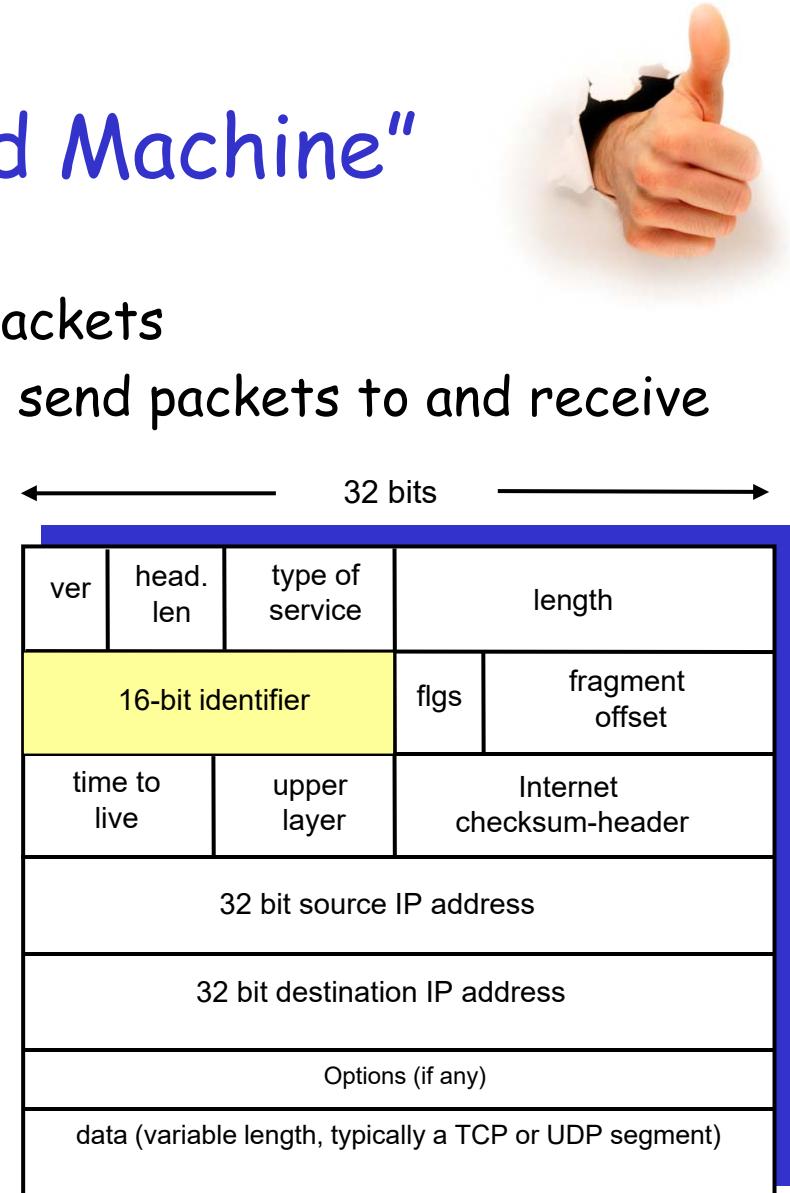
Nmap - ACK Scanning

- ❑ ACK Scan → used to map out firewall rule sets
 - ❖ Will firewall allow outbound connections on port 1026?

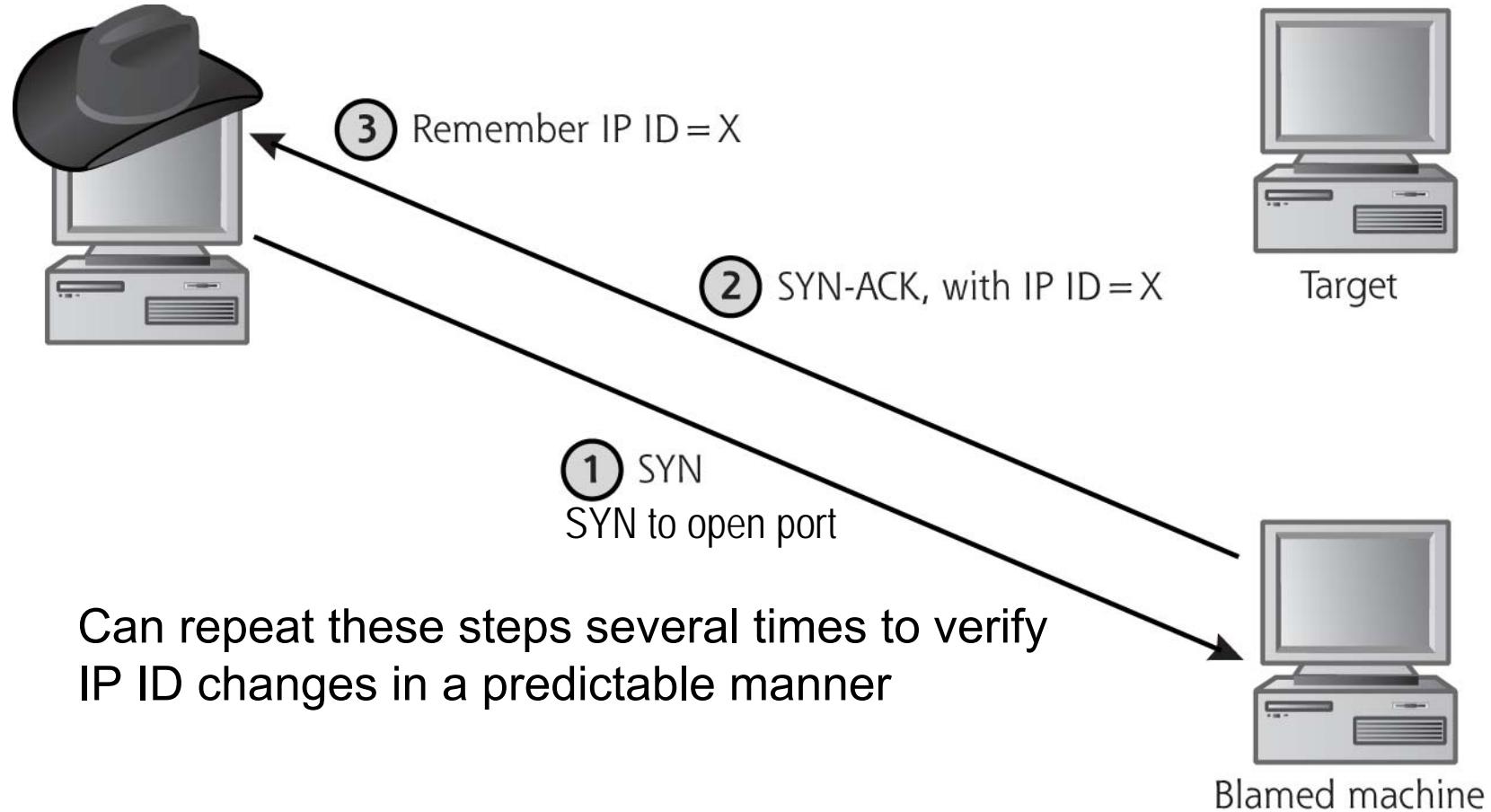


Idle Scans in Nmap - First Step: Pick a "Blamed Machine"

- Find a machine that is relatively idle
 - ❖ Machine that generates very few packets
- Could be any system that attacker can send packets to and receive packets from
 - ❖ Web server
 - ❖ Client connected to cable modem
- Must have a predictable IP ID field
 - ❖ IP ID used to group all fragments together for packet reassembly
 - ❖ Each packet assigned an IP ID value incremented by one

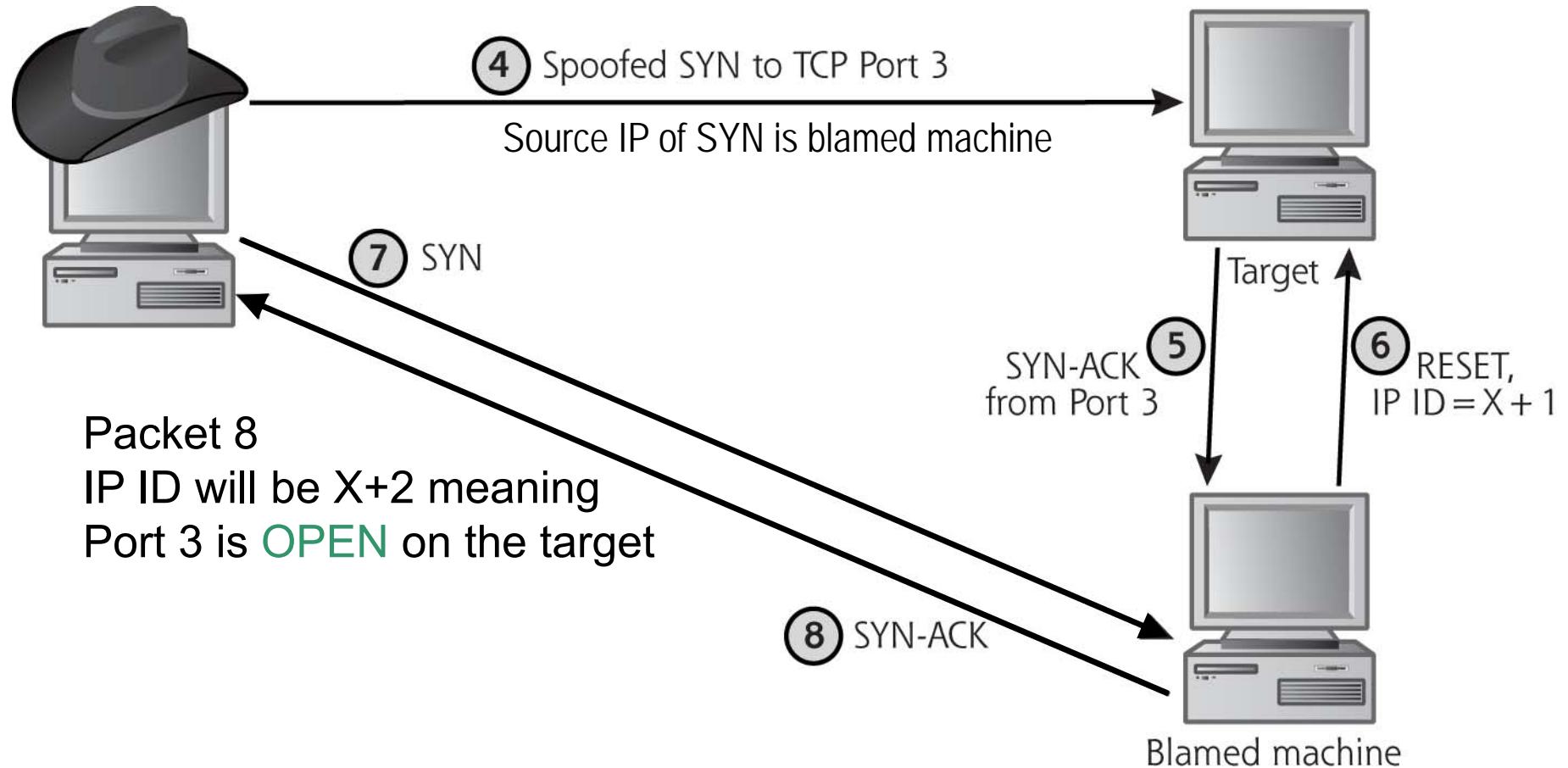


Idle Scans in Nmap - Prep For Attack



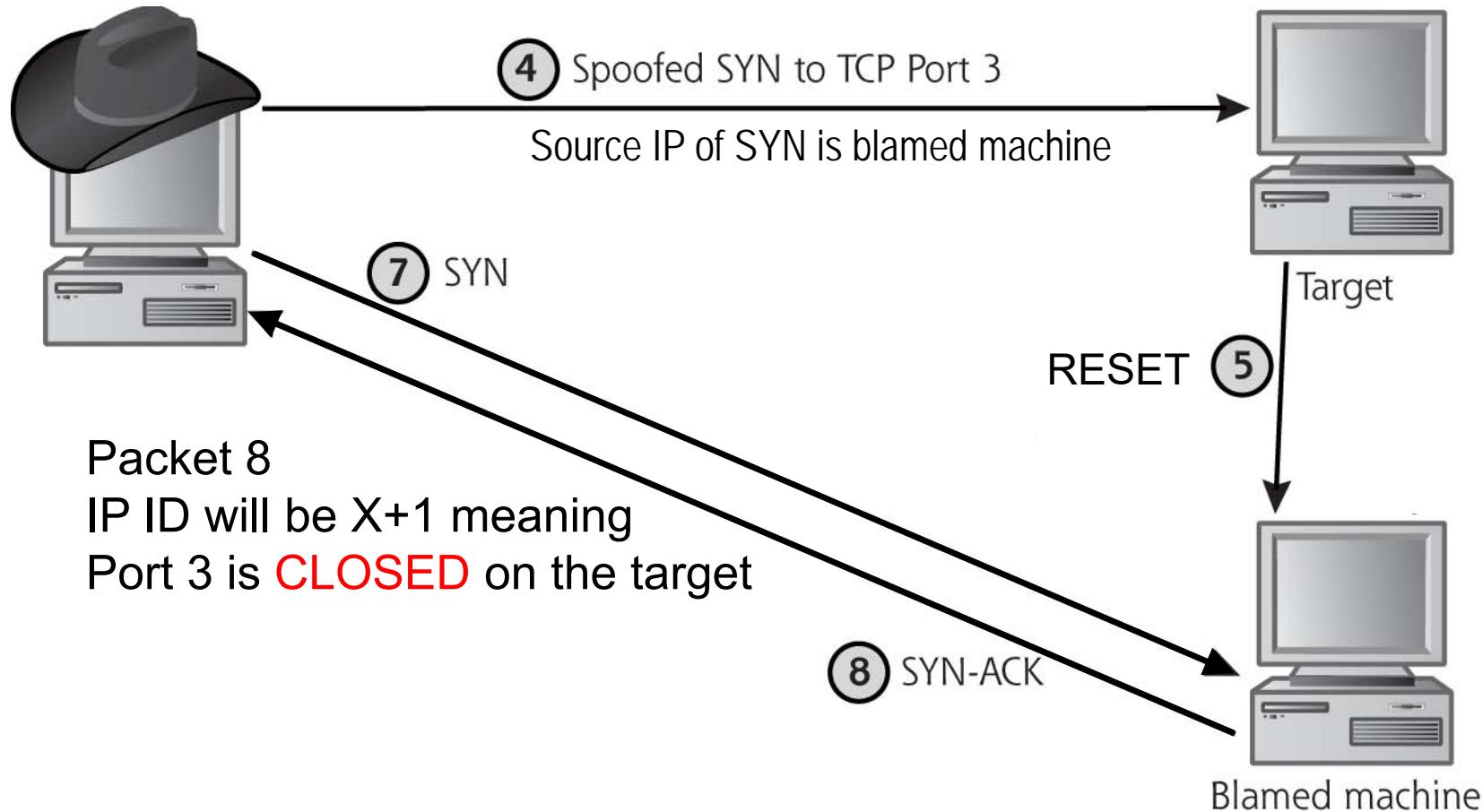
IP ID Scanning (aka Idle Scan)

Open Port



IP ID Scanning (aka Idle Scan)

Closed Port



Version Scanning

- Detects what service and **software version** is running on a port
 - ❖ Will find all services even if the service is listening on an unconventional port
 - I can place a web server on port 12345
- Nmap compares banner information presented after a three-way handshake to its internal database



A screenshot of a Windows-style Telnet window titled "Telnet ftp1.FreeBSD.org". The window displays the following banner text:

```
220----- Welcome to Pure-FTPd [TLS] -----
220-You are user number 23 of 100 allowed.
220-Local time is now 19:04. Server port: 21.
220-Only anonymous FTP is allowed here
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 2 minutes of inactivity.
```

- If no banner returned, nmap probes more to elicit some response

Setting Source Ports

- You want your scanning traffic to blend in with other network traffic
- Use common port numbers as the **source**
 - ❖ TCP port 25 - appears to be SMTP email traffic
 - ❖ UDP port 53 - appears to be a DNS response
 - ❖ TCP port 80 - appears to be a web server response



Profile Editor

```
nmap -sn -sT -p 22,80,23,443,21 -T3 -O -d -v -v -v -v -v -Pn
```

Source

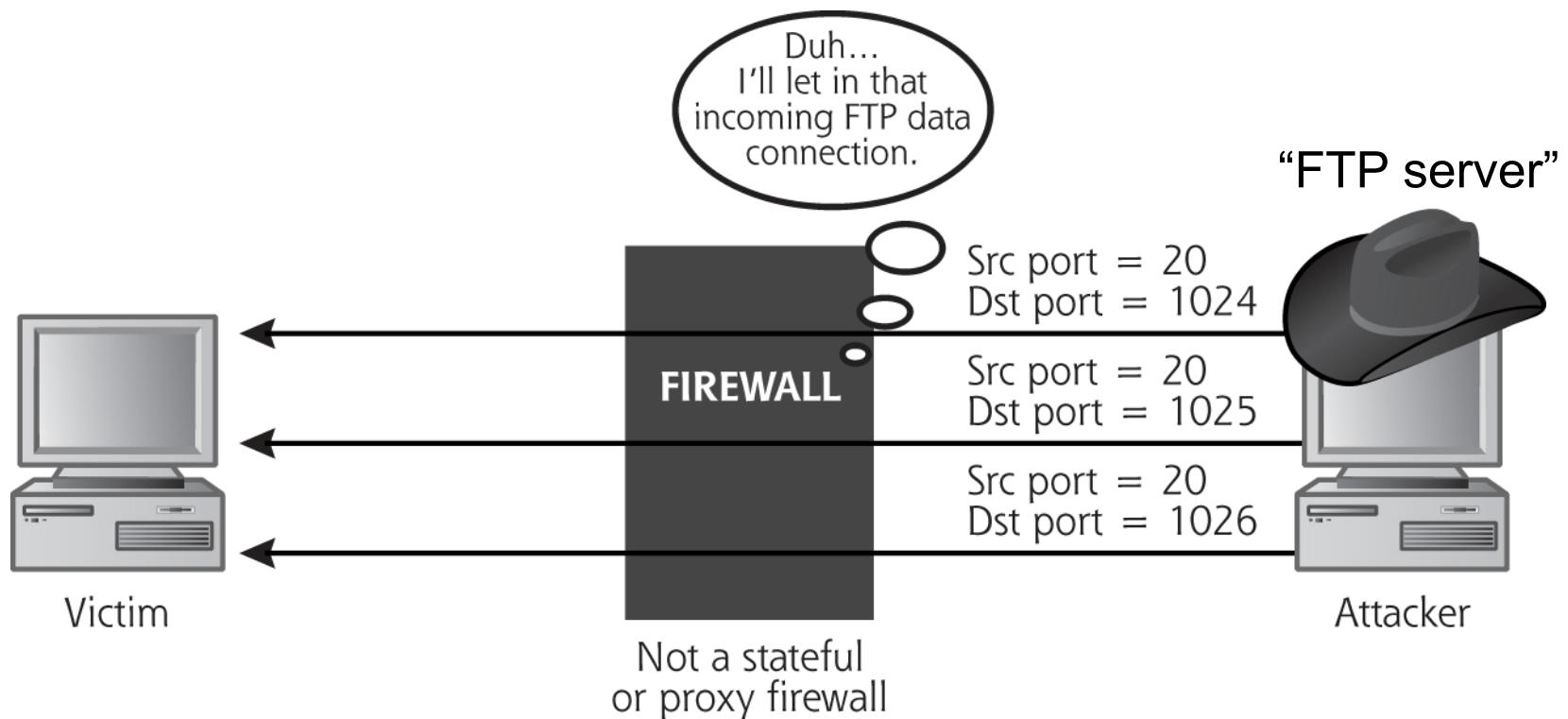
Source options

- Use decoys to hide identity (-D)
- Set source IP address (-S)
- Set source port (--source-port)
- Set network interface (-e)

Help
Set source port
Provide a port number and Nmap will send packets from that port where possible.
Example input:
53

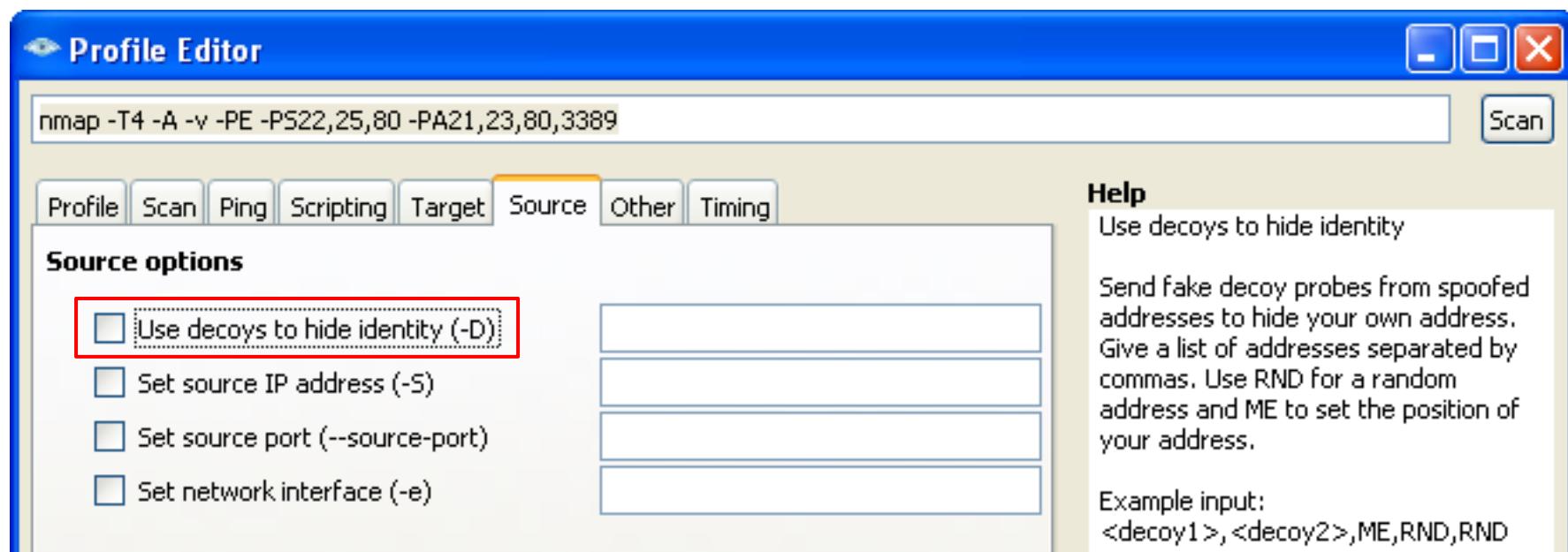
Use FTP as a Source Port

- Remember FTP uses two connections
 - ❖ FTP control connection - TCP port 21
 - ❖ FTP data connection - TCP port 20 (on FTP server - Active)
 - ❖ Port 20 very useful as source port
- Stateful packet filter or proxy firewall will catch this



Nmap Decoys (-D option)

- ❑ Nmap can send multiple copies of its scans using spoofed (decoy) IP addresses
- ❑ Target must sift through bogus IPs
- ❑ <decoy1>,<decoy2>,ME,RND,RND
- ❑ RND = random address and ME=attacker



Timing Options (-T)

- Paranoid (-T0) → serial; 300 sec between probes
 - Sneaky (-T1) → serial; 15 sec between probes
 - Polite (-T2) → serial; 0.4 sec between probes
 - Normal (-T3) (Default)
 - ❖ parallel
 - ❖ send as quickly as possible
 - Aggressive (-T4)
 - ❖ parallel
 - ❖ send as quickly as possible
 - ❖ only spend 300 sec on one host then move to next
 - ❖ wait no more than 1.25 sec for response
 - Insane (-T5)
 - ❖ parallel
 - ❖ send as quickly as possible
 - ❖ only spend 75 sec on one host then move to next
 - ❖ wait no more than 0.3 sec for response
-
- Stealthy.
Less likely
to be
noticed
- Likely to
miss traffic

Nmap Active OS Fingerprinting

Scanning More Than Once

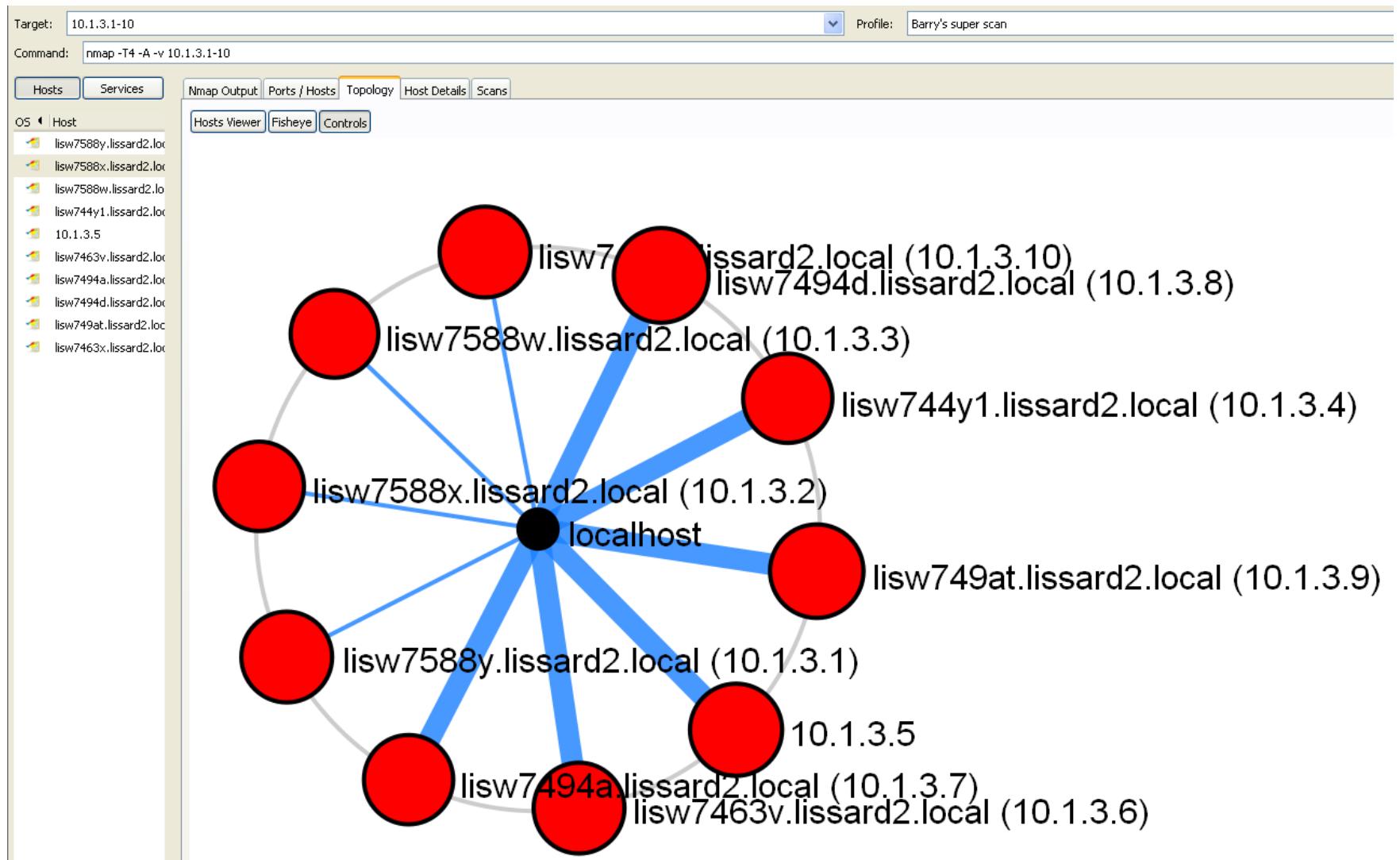
- You may have to run nmap more than once with different settings to achieve your goal

Scenario: What is the host name of a machine listening on port 8888

- First find the IP address
 - ❖ **nmap -p 8888 --open 10.1.1.0/24**
 - Assume there was a hit on 10.1.1.88
- Now find the host name
 - ❖ **nmap --script nbstat 10.1.1.88**
 - ❖ **nmap -A 10.1.1.88**
- If you try to scan and fingerprint using one nmap command, it will likely not give you the host name since it is only scanning port 8888

Nmap GUI - Topology Tab

Announced at DEFCON 2008



Some ports are filtered

Passive OS Fingerprinting

- Covered on pages 446-448, but I discuss it here
- How do operating systems populate various fields?
 - ❖ Initial sequence number
 - ❖ Initial TTL
 - ❖ IP ID
- Technique can identify the operating system on **machines whose communications you can observe**
 - ❖ machines that connect to your box (SYN mode)
 - ❖ machines you connect to (SYN+ACK mode)
 - ❖ machines you **cannot** connect to (RST mode)

POF3 - Totally Passive!

- **Passive** sniffer and database for determining system type
 - ❖ Does not generate traffic
- Determines the type of system that generated the packet based solely on sniffed packets
- Can also detect or measure
 - ❖ firewall presence
 - ❖ NAT use
 - ❖ the distance to the remote system and its uptime
 - ❖ target's network hookup (DSL, OC3, avian carriers) and ISP
- lcamtuf.coredump.cx/p0f3/

Determining Firewall Filter Rules - Firewalking

- Allows an attacker to determine which packets are allowed through a packet filtering device
- Firewalk is based on ideas originally used in traceroute
 - ❖ Works with both TCP or UDP since TTL is in the IP header
 - ❖ Works with firewalls or routers
 - ❖ Does not work with proxies since the TTL is reset by proxy

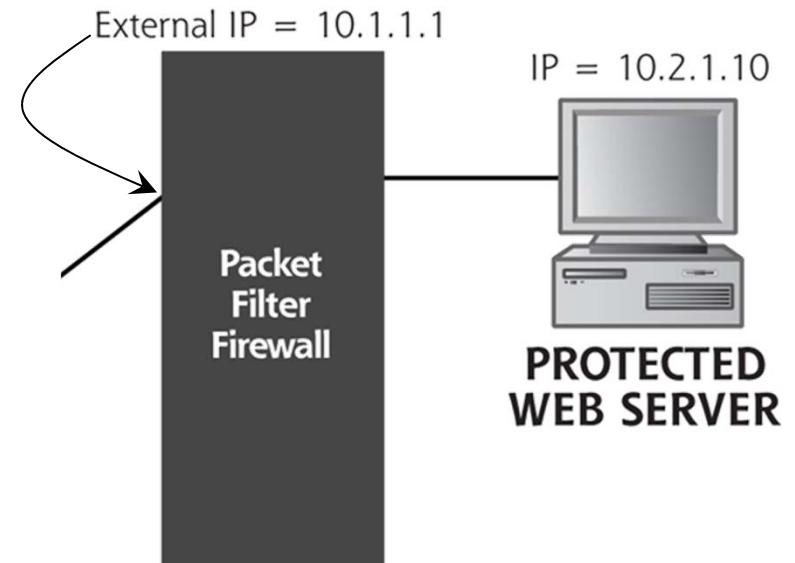
Determining Firewall Filter Rules - Firewalking

- Different than nmap ACK scan
 - ❖ Firewalking tells us that the firewall allows **new** connections from **outside to inside** (SYN bit set)
 - ❖ Nmap ACK scan tells us which ports allow **established** connections from **inside to outside** (ACK bit set)
- Nmap has a firewalking script → --script=firewalk
- packetfactory.openwall.net/projects/firewalk/
 - ❖ Kali: `apt-get install firewalk`
- Tutorial → <https://www.hackingloops.com/firewalk/>

Firewalk Operation

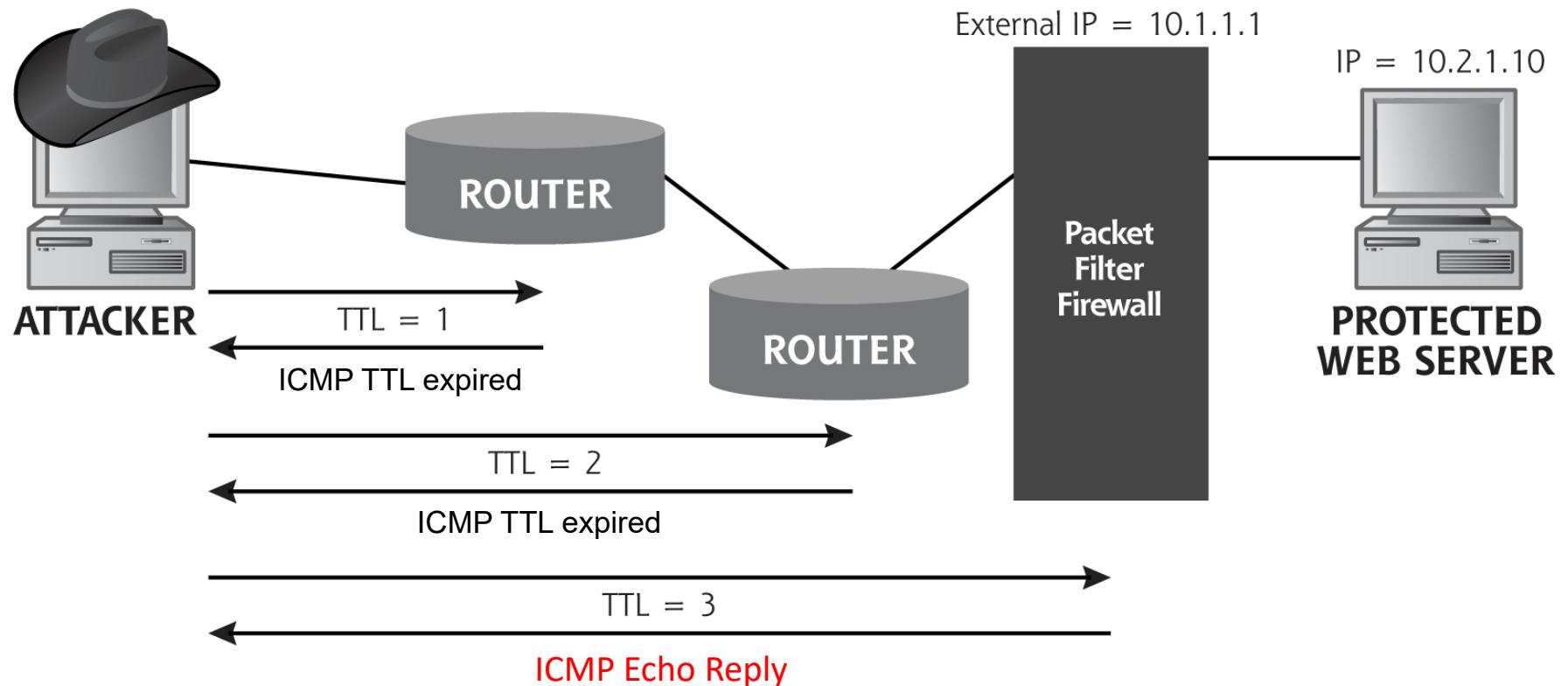
- Requires 2 IP addresses:
 - ❖ Network hop just before filtering takes place
 - Typically external address of packet-filtering device (e.g., 10.1.1.1)
 - ❖ Destination machine on the other side of packet-filtering device (e.g., 10.2.1.10)

- Operates in two phases:
 - ❖ Network Discovery
 - ❖ Scanning



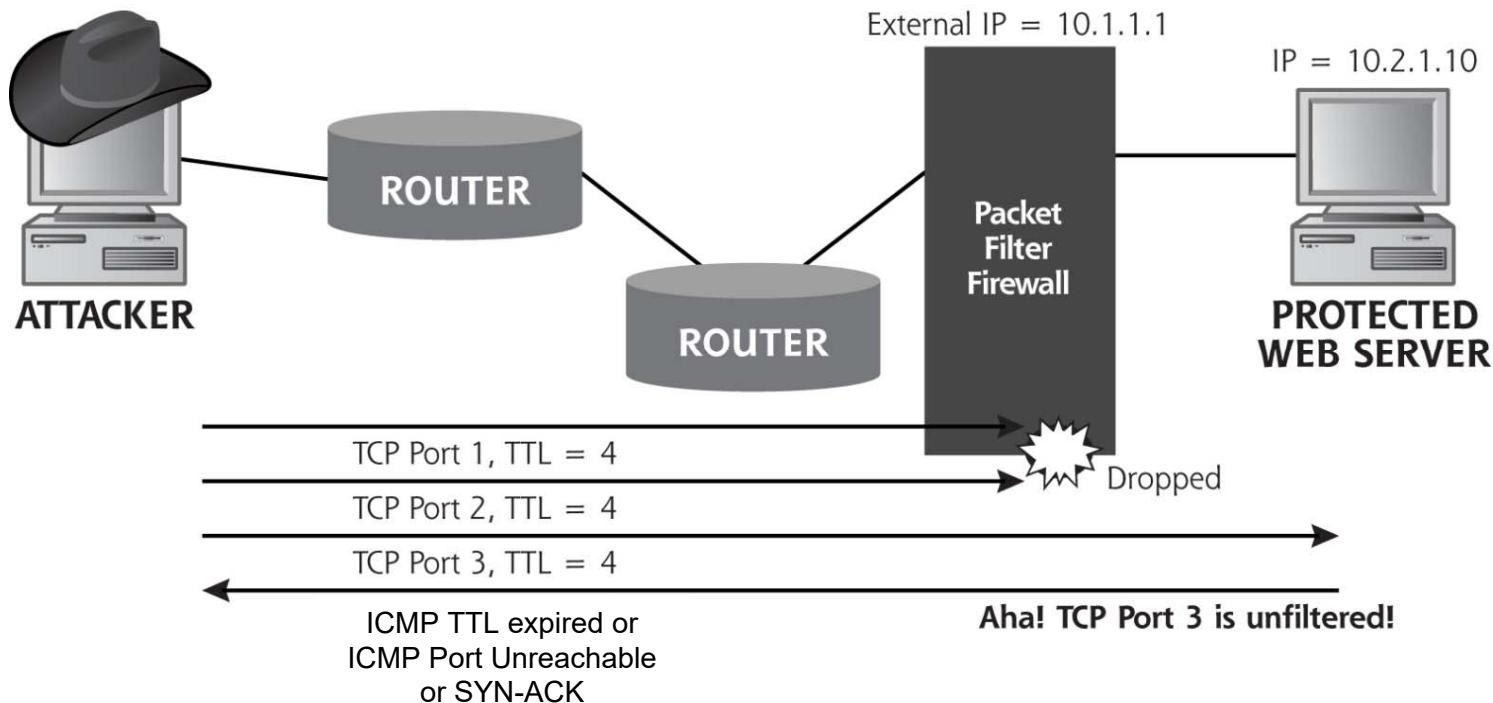
Firewalk Network Discovery Phase

- ❑ Essentially does a traceroute to determine how many network hops (e.g., 3 hops) are between tool and firewall



Firewalk Scanning Phase

- Send packet with TTL = hop_count + 1 (e.g., 4) and start timer
- If filter allows traffic, it forwards packet to next hop where it could generate an ICMP TTL Expired message, an ICMP Port Unreachable message, or SYN-ACK
 - ❖ In all cases we know the port is **not** filtered
- If timer expires and no response means the port **is** filtered



Let's Step Back For A Moment... What Do We Know So Far?

What the attacker knows	Tools used to get the information
List of addresses of live hosts on the network	Arp-scan, Ping, Scapy
General network topology	Traceroute, Nmap
List of open ports on live hosts	Nmap port scan
List of services and versions running on the target ports	Nmap version scan
Operating systems on live hosts	Nmap (active) and P0f3 (passive) operating system fingerprinting
List of ports open through packet filters on target network	Firewalk

Computer and Network Hacker Exploits

- Step 1: Reconnaissance
- **Step 2: Scanning**
 - ❖ Network Mapping
 - ❖ Determining Open Ports Using Port Scanners
 - ❖ **Vulnerability-Scanning Tools**
 - ❖ Intrusion Detection System and Intrusion Prevention System Evasion
 - ❖ Shares
- Step 3: Gaining Access
 - ❖ Application and Operating System Attacks
 - ❖ Network Attacks
 - ❖ Denial of Service Attacks
- Step 4: Maintaining Access
- Step 5: Covering Tracks and Hiding

Vulnerability Scanning Tools

- Automated tool to find target vulnerabilities
 - ❖ We exploit these vulnerabilities to gain access
- Tool maintains list of known vulnerabilities
- Common vulnerabilities include
 - ❖ Configuration / Implementation errors
 - ❖ Default configurations
 - Default accounts and passwords
 - ❖ Well-known security vulnerabilities
 - List grows longer each day
- Tool connects to target and sees if vulnerability is present
 - ❖ Checking for less secure, version of software (e.g., SSH server)

Vulnerability Disclosures

- Bugtraq (www.securityfocus.com)
 - ❖ Discussions about vulnerabilities, vendor security-related announcements, methods of exploitation, and how to fix them

BugTraq

[Back to list](#) | [Post reply](#)

▼ [SQL Injection in LightNEasy](#) Dec 30 2010 09:47AM
advisory htbridge ch

Vulnerability ID: HTB22750
Reference: http://www.htbridge.ch/advisory/sql_injection_in_lightneasy.html
Product: LightNEasy
Vendor: Fernando Baptista ([http://www.lightneeasy.org/](http://www.lightneasy.org/))
Vulnerable Version: 3.2.2
Vendor Notification: 15 December 2010
Vulnerability Type: SQL Injection
Status: Not Fixed, Vendor Alerted, Awaiting Vendor Response
Risk level: High
Credit: High-Tech Bridge SA - Ethical Hacking & Penetration Testing (<http://www.htbridge.ch/>)

Vulnerability Details:
The vulnerability exists due to failure in the "/LightNEasy.php" script to properly sanitize user-supplied input in "handle" variable. Attacker can alter queries to the application SQL database, execute arbitrary queries to the database, compromise the application, access or modify sensitive data, or exploit various vulnerabilities in the underlying SQL database.

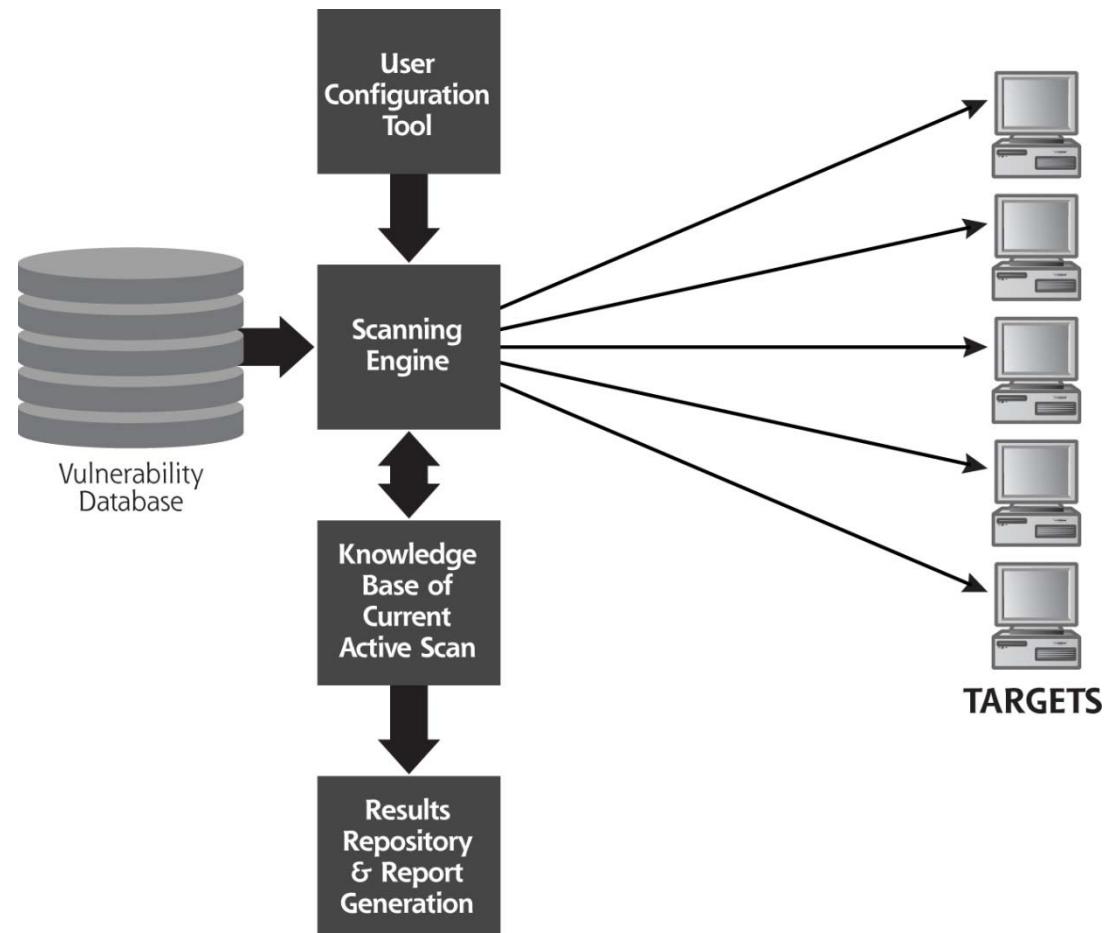
The following PoC is available:

```
<form action="http://[host]/LightNEasy.php?do=login" method="post" name="main" >
<input type="hidden" name="handle" value='123"SQL_CODE_HERE'>
<input type="hidden" name="password" value="1"/>
<input type="hidden" name="do" value="login"/>
<input type="submit" value="submit" name="submit" />
</form>
```

[\[reply \]](#)

A Generic Vulnerability Scanner

- User config tool
 - ❖ Select targets and which vulns to check
- Vulnerability database
 - ❖ List of vulns and how to check for them
- Scanning engine
 - ❖ Creates and sends packets to targets
- Knowledge base of current active scan
 - ❖ Short term memory
- Results repository & report generation
 - ❖ Lists vulns on targets and recommends COA



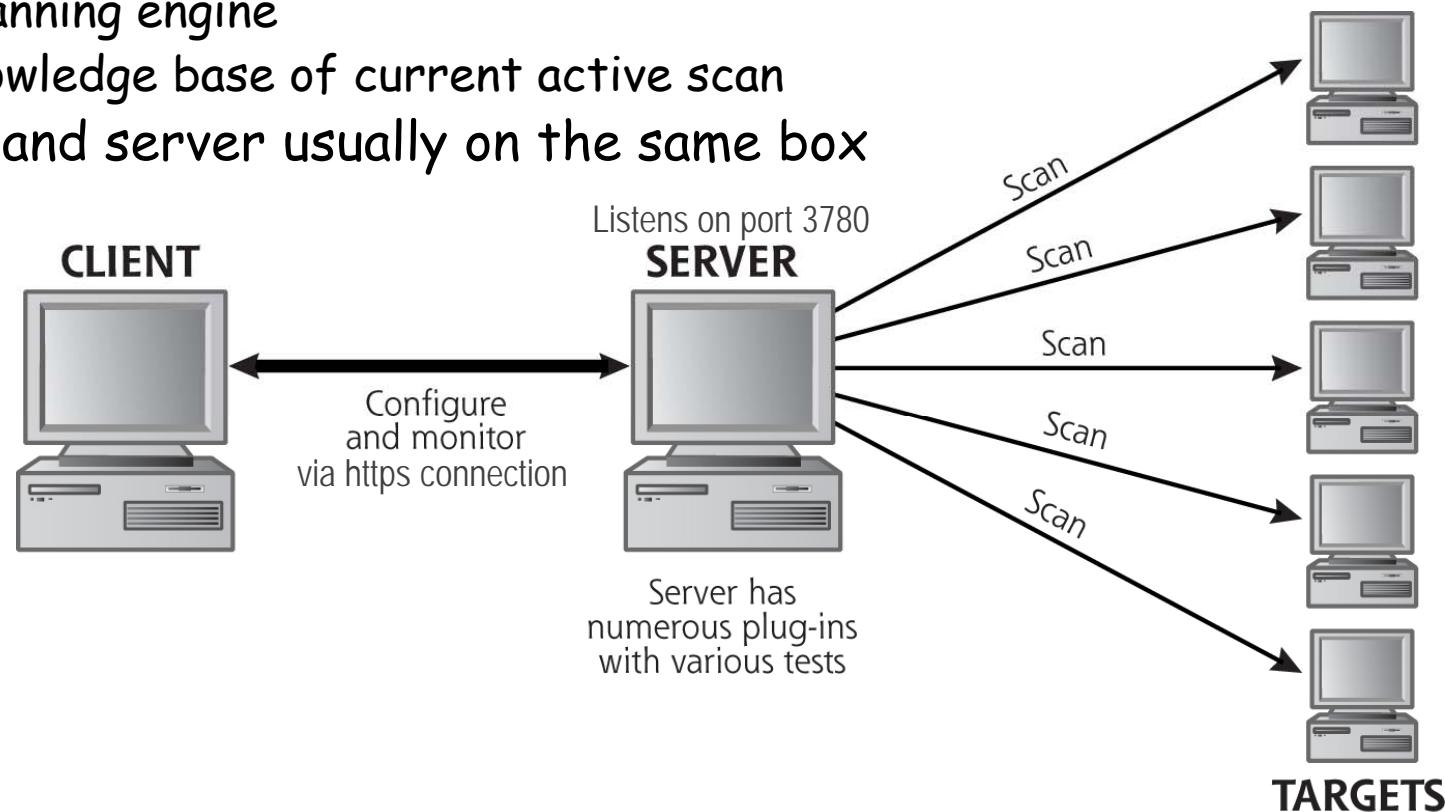
Vulnerability Scanning Tools

- Nexpose - "Free"
 - ❖ <https://www.rapid7.com/products/nexpose/>
- Nessus - "Free"
 - ❖ www.tenable.com/products/nessus
- Numerous commercial scanners available
- Many commercial services offer subscription-based services



Nexpose Architecture

- Client
 - ❖ User configuration tool
 - ❖ Results repository & report generation
- Server
 - ❖ Vulnerability database
 - ❖ Scanning engine
 - ❖ Knowledge base of current active scan
- Client and server usually on the same box



Nexpose Target Results

The screenshot shows the Nexpose Security Console interface. The top navigation bar includes a back button, forward button, address bar (localhost), search bar (Certificate error), and tabs (Nexpose Security Console). The main menu bar has options: File, Edit, View, Favorites, Tools, Help. The user is logged in as 'barry'. The left sidebar contains icons for Home, Site, Scan, Asset, and Dashboards.

The main content area displays the target details for 'Nexpose1' (IP: 10.1.5.55, Hardware: 00:50:56:A9:87:F6, Aliases: NESSUS1, Site: Nexpose1). The OS is identified as Microsoft Windows XP (highlighted with a red box). The CPE entry is cpe:/o:microsoft:windows-nt:xp:gold. The host type is Unknown, and the last scan was on Dec 30, 2016, at 1:07:53 PM (2 minutes ago).

Below the target details, there are sections for Risk Score (Original: 5,695, Context-Driven: 5,695) and User-Added Tags (None). There are also sections for Custom Tags (None), Locations (None), Owners (None), and Criticality (None). A 'SEE ASSET PAGE' link is present.

A yellow callout bubble with the text 'Scroll down' points to the 'VULNERABILITIES' section at the bottom of the page. This section lists two vulnerabilities:

Vulnerability	Severity	Instances
Microsoft Server Service / CanonicalizePathName() Remote Code Execution Vulnerability	Critical	1
MS08-067: Vulnerability in Server Service Could Allow Remote Code Execution (958644)	Critical	3

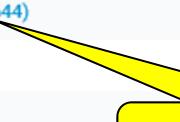
The bottom right corner of the page shows the number 55.

Vulnerabilities

RISK SCORE <small>?</small>	USER-ADDED TAGS <small>?</small>		
ORIGINAL 5,695	CUSTOM TAGS None	OWNERS None	 Add tags
CONTEXT-DRIVEN 5,695	LOCATIONS None	CRITICALITY None	

VULNERABILITIES

Vulnerability	Severity <small>▼</small>	Instances
Microsoft Server Service / CanonicalizePathName() Remote Code Execution Vulnerability	Critical	1
MS08-067: Vulnerability in Server Service Could Allow Remote Code Execution (958644)	Critical	3
MS09-001: Vulnerabilities in SMB Could Allow Remote Code Execution (958687)	Critical	2
CIFS NULL Session Permitted	Critical	1
MS06-035: Vulnerability in Server Service Could Allow Remote Code Execution (917159)	Critical	1
SMB signing disabled	Severe	2
SMB signing not required	Severe	2
ICMP timestamp response	Moderate	1
NetBIOS NBSTAT Traffic Amplification	Moderate	1

 Click to learn more

Vulnerability Information

VULNERABILITY INFORMATION

OVERVIEW

Title	Severity	Vulnerability ID	CVSS	Published	Modified
MS08-067: Vulnerability in Server Service Could Allow Remote Code Execution (958644)	Critical (10)	windows-hotfix-ms08-067	10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)	Oct 23, 2008	Feb 13, 2015

DESCRIPTION

This security update resolves a privately reported vulnerability in the Server service. The vulnerability could allow remote code execution if an affected system received a specially crafted RPC request. On Microsoft Windows 2000, Windows XP, and Windows Server 2003 systems, an attacker could exploit this vulnerability without authentication to run arbitrary code. It is possible that this vulnerability could be used in the crafting of a wormable exploit. Firewall best practices and standard default firewall configurations can help protect network resources from attacks that originate outside the enterprise perimeter.



Computer and Network Hacker Exploits

- Step 1: Reconnaissance
- **Step 2: Scanning**
 - ❖ Network Mapping
 - ❖ Determining Open Ports Using Port Scanners
 - ❖ Vulnerability-Scanning Tools
 - ❖ **Intrusion Detection System and Intrusion Prevention System Evasion**
 - ❖ Shares
- Step 3: Gaining Access
 - ❖ Application and Operating System Attacks
 - ❖ Network Attacks
 - ❖ Denial of Service Attacks
- Step 4: Maintaining Access
- Step 5: Covering Tracks and Hiding

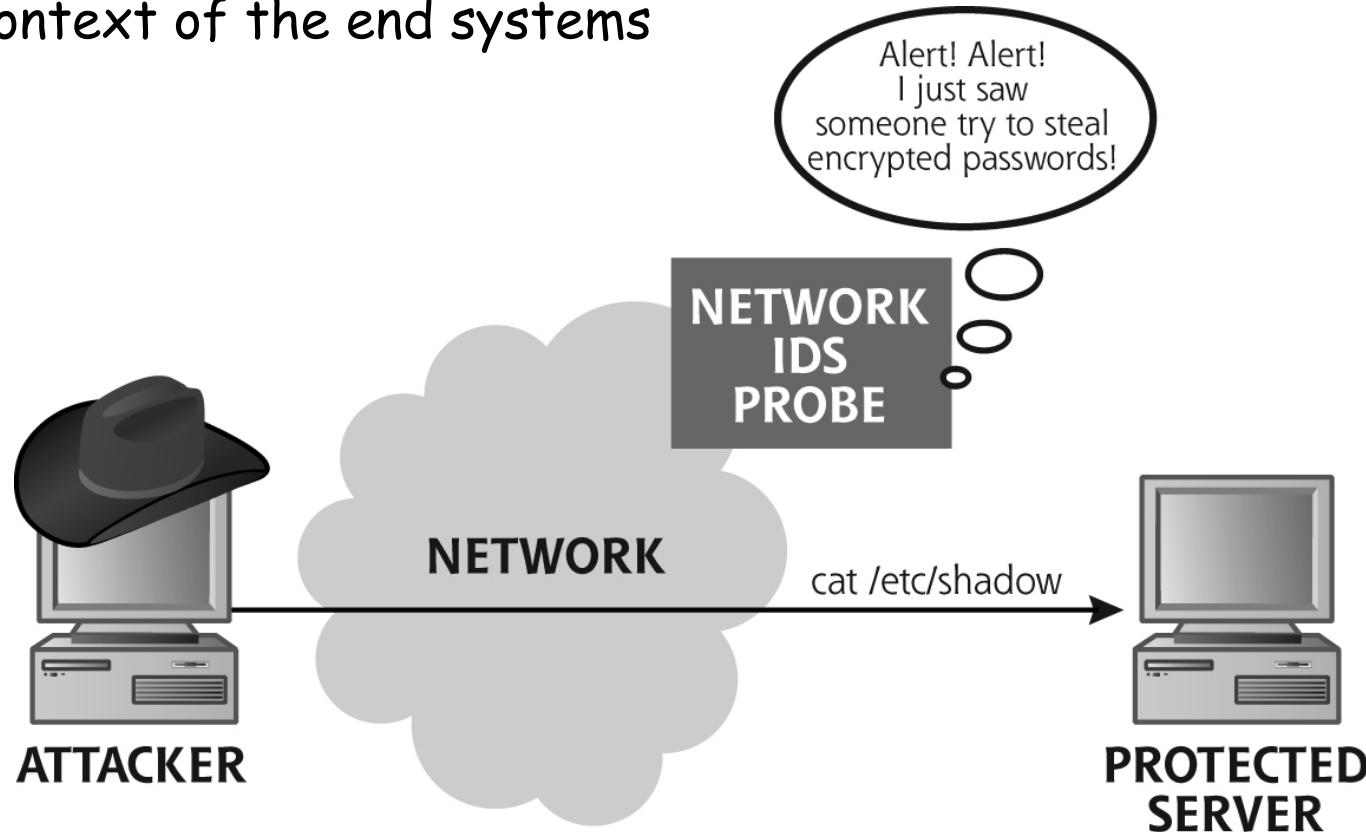
IDS and IPS Evasion

- ❑ Intrusion Detection System / Intrusion Prevention System
 - ❖ Attempt to thwart attacks by matching packet and traffic signatures against traffic it sees
 - ❖ Must sort through a mountain of traffic to fingerprint attack
- ❑ Scanning tools generate a tremendous amount of packets
 - ❖ A diligent sysadmin may notice
 - ❖ IDS / IPS will most likely raise an alert
- ❑ Your mission, if you choose to accept it, is to evade IDS and IPS



How Does Signature Matching Work?

- Monitor traffic looking for specific sequences of bytes
 - ❖ Alert raised if it sees "cat /etc/shadow" in traffic
- How can the attacker slip things past a network IDS?
 - ❖ Exploit the fact that the IDS does not maintain complete context of the end systems



Evade IDS / IPS Systems at the Network Level

- Change how your traffic appears to these systems
- Alter packet structure or syntax
- Manually fragment the message into smaller packets
 - ❖ Send each packet out of order with large delays between each
 - ❖ Long delay = IDS needs long-term (lots) memory
 - Snort Frag3 times out after 60 seconds
- "Attack at noon" becomes

"noon" ...

"at" ...

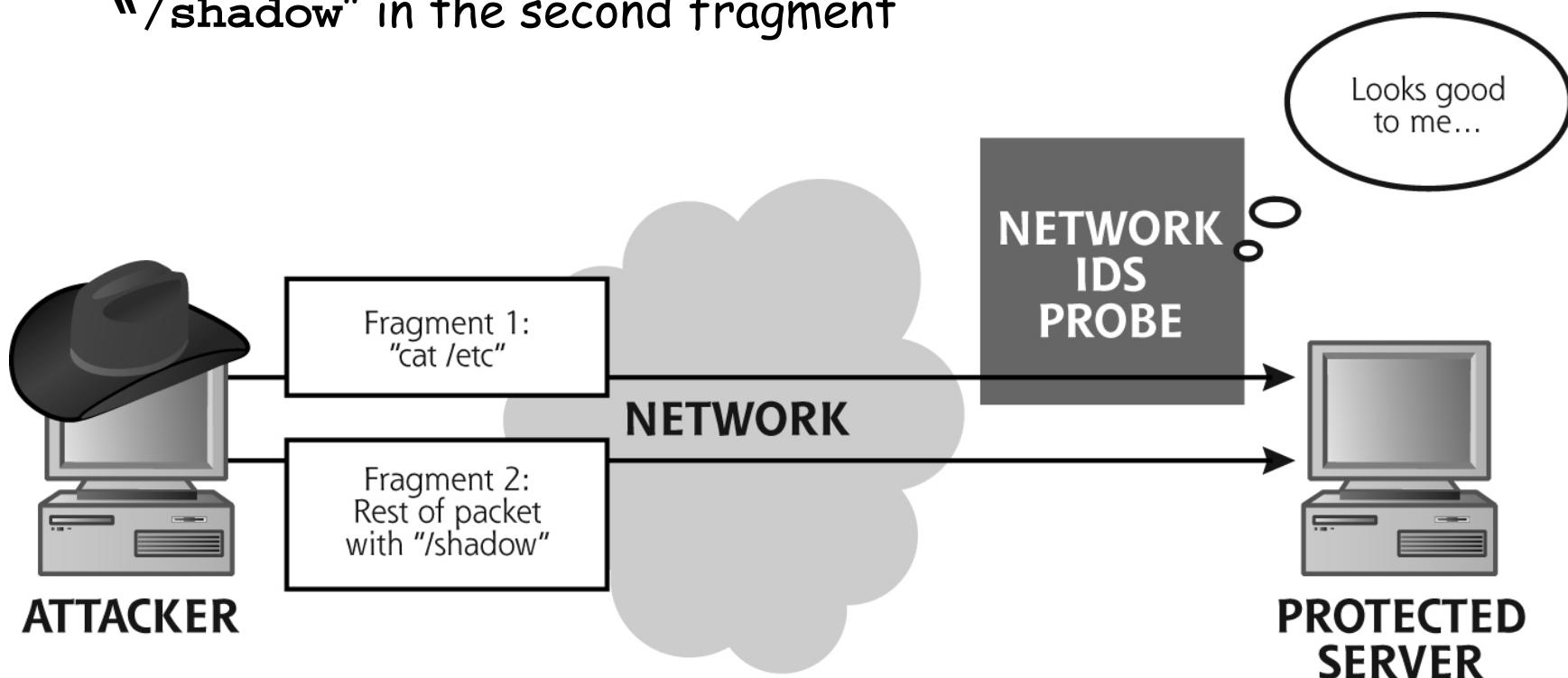
"Attack"

Evade IDS / IPS Systems at the Network Level

- Older IDS/IPS systems could not handle fragmentation
- Seems easy for the IDS/IPS to reconstruct the message since fragment offsets are included in the packets, however...
- What if we
 - ❖ fragment packets in unexpected ways
 - Not all OSs reconstruct specially-crafted fragments the same
 - ❖ also flood the IDS/IPS with bogus fragments filling up frag memory

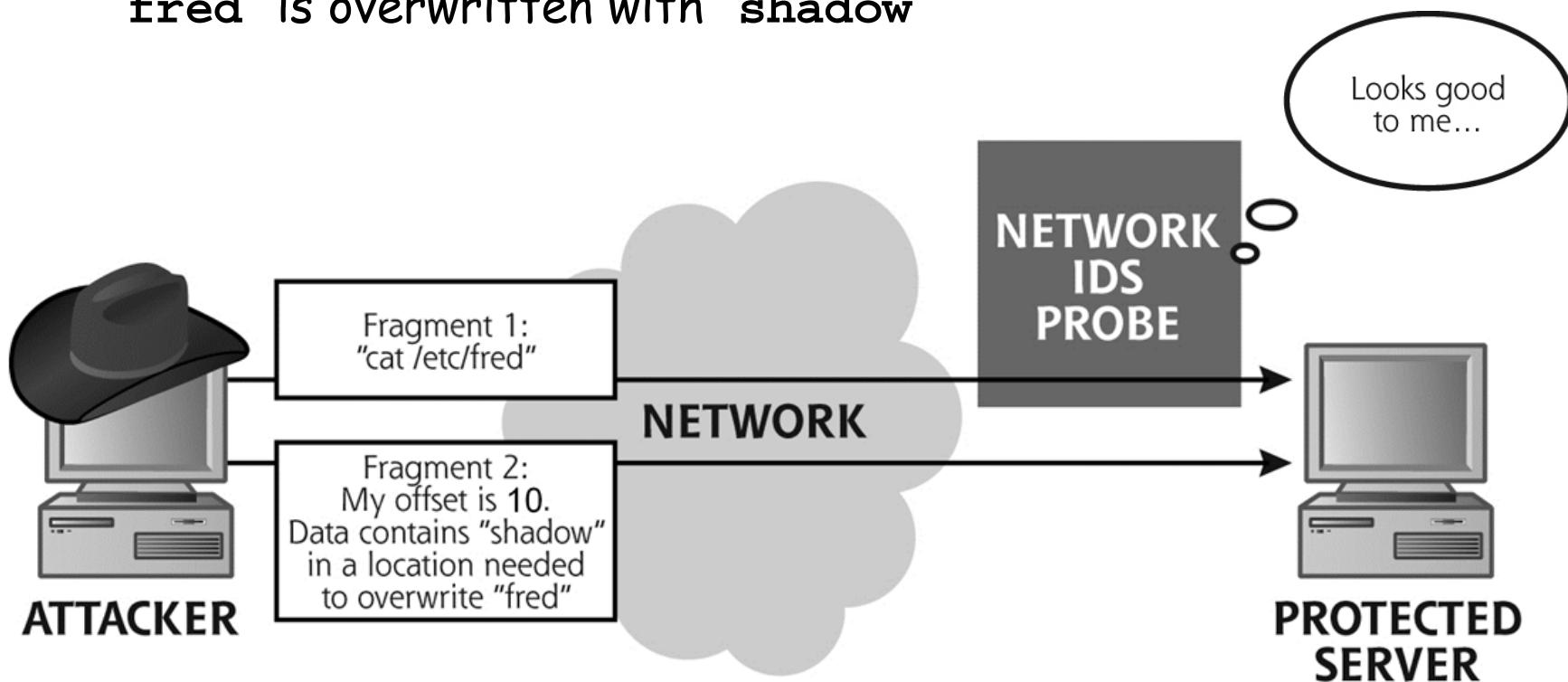
Tiny Fragment Attack

- Create multiple, small fragments such that no one fragment triggers the IDS
 - ❖ Send "cat /etc" in the first fragment and the remainder "/shadow" in the second fragment



Fragment Overlap Attack

- First fragment "cat /etc/fred" is fine
- Second fragment provides an incorrect (too small) frag offset
 - ❖ When the packet is reconstructed at the protected server, "fred" is overwritten with "shadow"



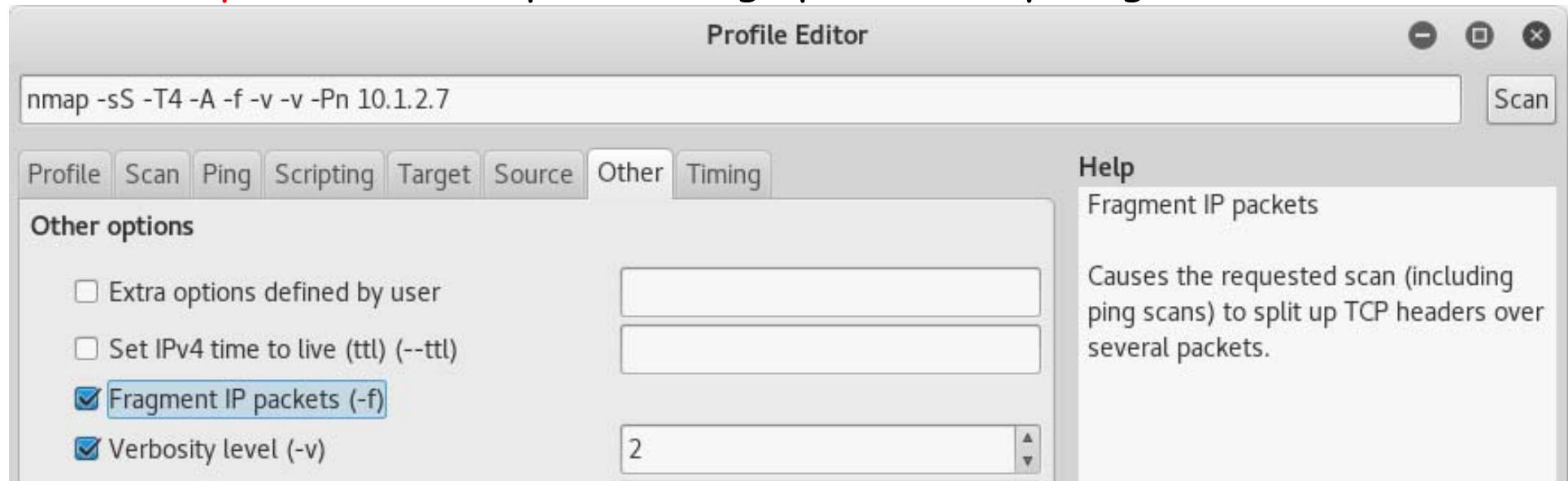
How are Fragments Reassembled?

- Various operating systems reassemble packets differently
 - ❖ Earliest fragment not allowed to be overlapped
 - ❖ Fragment with lowest offset will overwrite others, regardless of when it arrives
 - ❖ Complete overlap or partial overlap are handled differently

- IDS might not know which method end systems (hosts) use
 - ❖ Could ask IDS to reassemble using all methods
 - ❖ Cisco Secure IDS has one setting to choose whether it reassembles for Windows, Solaris, Cisco IOS, or Linux/BSD
 - ❖ Snort with Frag2 preprocessor always reassembles for Linux machines
 - ❖ Snort with Frag3 preprocessor includes multiple frag reassembly buffers running in parallel

IP Fragment Attack Tools

- ❑ Nmap has a limited packet frag option → tiny fragment attack



- ❑ FragRoute intercepts, modifies, and rewrites egress traffic
 - ❖ FragRoute does not route
 - It must reside on the same machine as the attack tool
 - Built into Kali (tools.kali.org/information-gathering/fragroute)

Evade at the Application Level

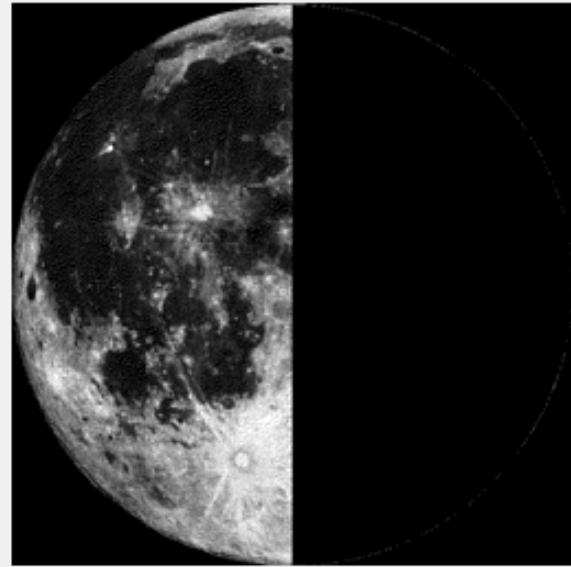
Recall how a web server uses CGI scripts:

```
POST http://www.briancasey.org/artifacts/astro/moon.cgi HTTP/1.1  
Content-Length: 25  
Host: www.briancasey.org  
<<snip>>  
<crlf>  
year=2007&month=11&day=30
```

25 characters

The Moon's Phase

...and tada



The Moon for Nov 30, 2007 (At Midnight, US Central time, as viewed from the Northern Hemisphere)

Illuminated Fraction: 0.516
0.2 days before last quarter

Year: 2007 Month: November Day: 30

Get Moon

Many CGI Scripts Have Vulnerabilities

- ❑ Since scripts run on servers, attacker could take control of server
 - ❑ CGI programs usually have same level of privileges as web server
 - ❑ Attacker can escape out of the web server process and send data directly to command line for execution
 - ❑ Cool! How do I find a vulnerable website?

Define: Web Server Scanners

- Automated program that searches for known script vulnerabilities in web servers and web apps
 - ❖ Search for "default" example scripts left on system during install
 - ❖ Search for specific scripts that are known to be vulnerable
- Typically called Web Application Security Scanners
- There are many Web scanners out there
 - ❖ **w3af** → Web Application Attack and Audit Framework
 - ❖ **Nikto**

w3af Configure



- Find and **exploit** web application vulnerabilities
- w3af.org Works best in Linux - **Removed from Kali-rolling**

w3af – Web Application Attack and Audit Framework

Profiles Edit View Tools Configuration Help

Scan config Log Results Exploit

Profiles Target: scanme.nmap.org

empty_profile

OWASP_TOP10

audit_high_risk

bruteforce

fast_scan

full_audit

full_audit_manual_disc

sitemap

web_infrastructure

Plugin Active

- ▷ audit
- ▷ auth
- ▷ bruteforce
- ▷ discovery
- ▷ evasion
- ▷ grep
- ▷ mangle

Plugin Active

- ▷ output

The Open Web Application Security Project (OWASP) is a worldwide free and open community focused on improving the security of application software. OWASP searched for and published the ten most common security flaws. This profile search for this top 10 security flaws. For more information about the security flaws: http://www.owasp.org/index.php/OWASP_Top_Ten_Project.

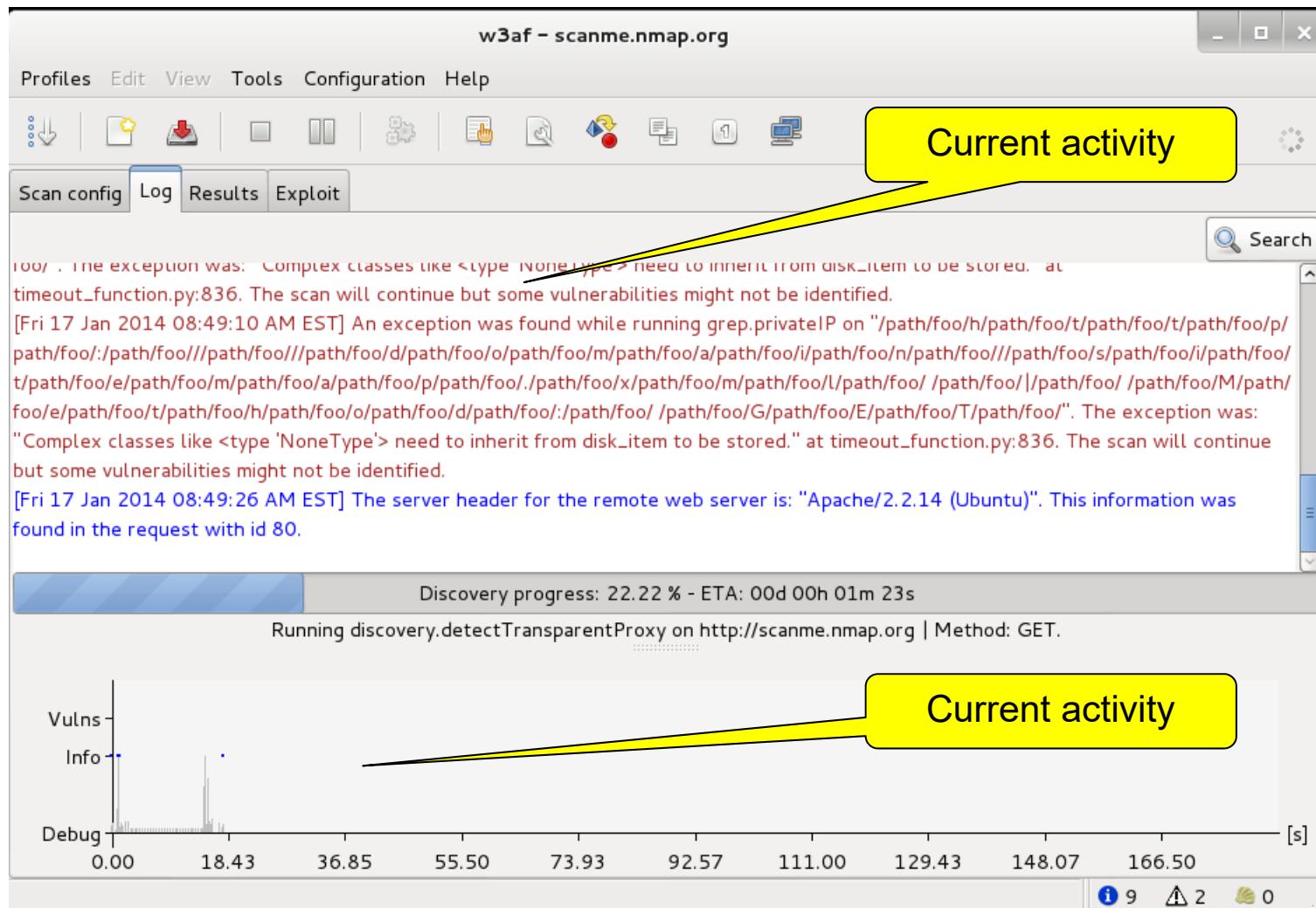
OWASP - Open Web Application Security Project

i 0 ▲ 0 0 0

w3af Running



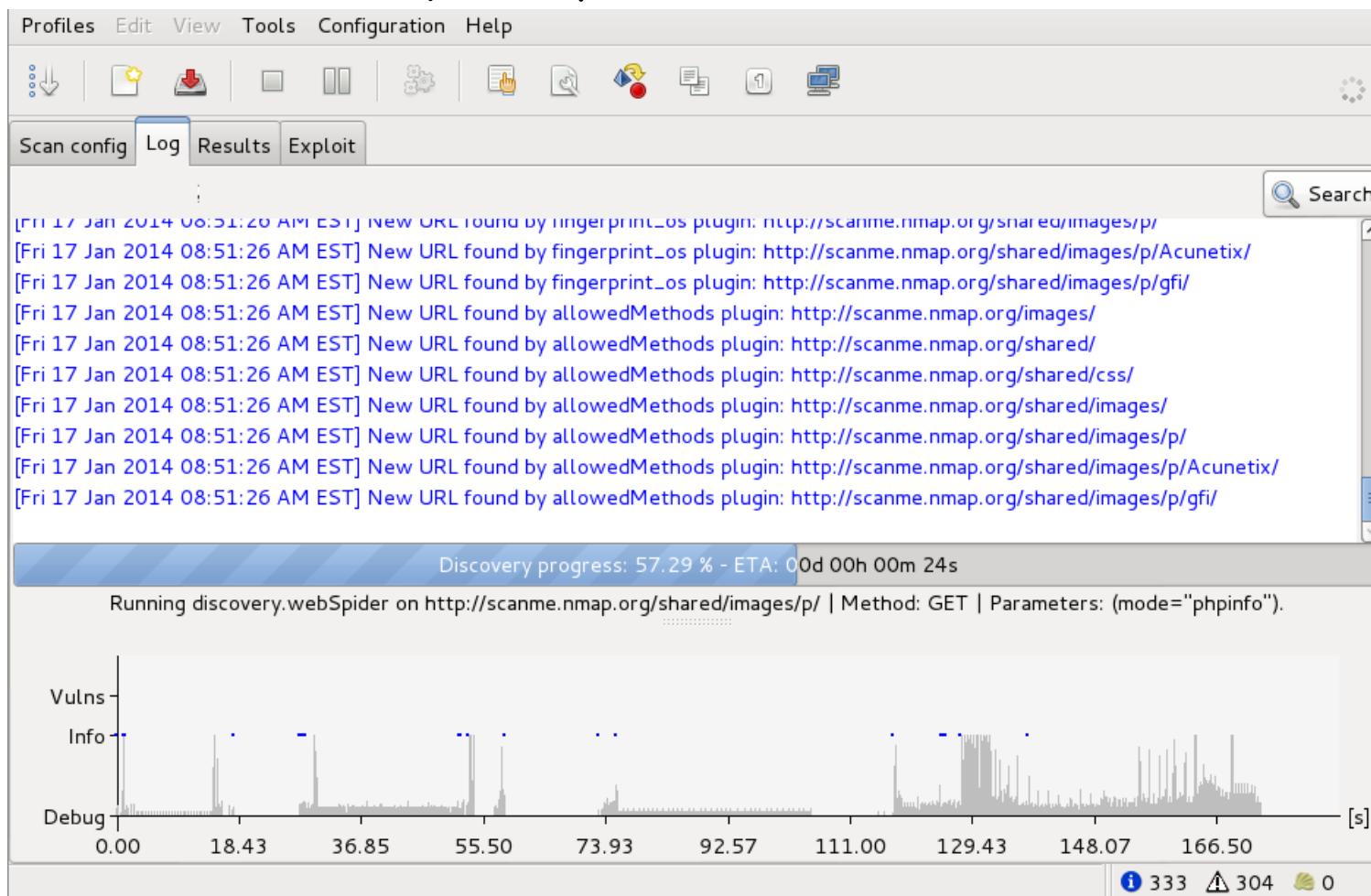
- Watch current activity in Log tab and timeline (bottom)



w3af Timeline Symbols



- Grey bar → quantity of debug messages
- Blue dot → information messages
- Vertical red bar → quantity of vulnerabilities found there



w3af Example Scan



URLs requested from target

w3af - scanme.nmap.org

Profiles Edit View Tools Configuration Help

Scan config Log Results Exploit

[Fri 17 Jan 2014 08:50:01 AM EST] - http://scanme.nmap.org?DksjfK9=type&zdc&A&Cwir&Crepair&Csam...
[Fri 17 Jan 2014 08:50:01 AM EST] - http://scanme.nmap.org?DksjfK9=ps+-aux%3B
[Fri 17 Jan 2014 08:50:01 AM EST] - http://scanme.nmap.org?DksjfK9=%2F..%2F..%2Fbin%2Fchgrp+nobody+%2Fetc%2Fshadow%7C
[Fri 17 Jan 2014 08:50:01 AM EST] - http://scanme.nmap.org?DksjfK9=SELECT+TOP+1+name+FROM+sysusers
[Fri 17 Jan 2014 08:50:01 AM EST] - http://scanme.nmap.org?DksjfK9=exec+master..xp_cmdshell+dir
[Fri 17 Jan 2014 08:50:01 AM EST] - http://scanme.nmap.org?DksjfK9=exec+xp_cmdshell+dir
[Fri 17 Jan 2014 08:50:07 AM EST] halberd plugin is starting. Original halberd author: Juan M. Bello Rivas ; http://halberd.superadditive.com/
[Fri 17 Jan 2014 08:50:21 AM EST] The site: http://scanme.nmap.org doesn't seem to have a HTTP load balancer configuration.

Discovery progress: 77.77 % - ETA: 00d 00h 00m 20s

Running discovery.sharedHosting on http://scanme.nmap.org | Method: GET.

Vulns

Info

Debug

0.00 18.43 36.85 55.50 73.93 92.57 111.00 129.43 148.07 166.50 [s]

241 224 0

w3af Results



w3af - scanme.nmap.org

Profiles Edit View Tools Configuration Help

Scan config Log Results Exploit

KB Browser URLs Request/Response navigator

Vuln Info Misc

Knowledge Base

- ▷ findComments (2)
- ▷ errorPages (1)
- ▷ creditCards (1)
- ▷ serverHeader (1)
- ▷ strangeHTTPCode (1)
- ▷ findvhost (1)
- ▷ afd (1)
- ▷ allowedMethods (1)
- ▷ fingerprint_os (1)
- ▷ directoryIndexing (1)

The URL: "http://scanme.nmap.org" discloses the credit card number:
"-0078565546631069"". This vulnerability was found in the request with id 1.

Request Response

Raw Headers

```
GET http://scanme.nmap.org HTTP/1.1
Host: scanme.nmap.org
Accept-Encoding: gzip
Accept: /*
User-Agent: w3af.sourceforge.net
```

i 336 ▲ 305 0

Nikto - Web Server Scanner

- Designed to find various default and insecure files, configurations and programs on many web servers
- Scans for over 6,700 potentially dangerous files / CGIs
- Checks for
 - ❖ outdated versions of servers
 - ❖ Server configuration items such as
 - the presence of multiple index files
 - HTTP server options
 - ❖ Attempts to identify installed web servers and software
- Automatically searches for CGI directories
- Uses robots.txt to focus searches
- www.cirt.net/Nikto2



Nikto IDS Evasion Techniques

- `nikto -host http://scanme.nmap.org -evasion 1`
- Techniques based on paper by Rain Forest Puppy
 - ❖ www.ussrback.com/docs/papers/IDS/whiskerids.html
- Nikto changes the request format in subtle, yet still fully functional, ways
- Let's look at the request to the vulnerable script called `broken.cgi`
 - ❖ `GET /cgi-bin/broken.cgi HTTP/1.0`

Evasion
techniques
on next slides

Nikto IDS Evasion Techniques

GET /cgi-bin/broken.cgi HTTP/1.0

1. URL Encoding - use hex equivalents of characters
 - ❖ GET /%63%67%69%2d%62%69%6e/broken.cgi HTTP/1.0
 - ❖ Try it: www.%61%6d%61%7a%6f%6e.com
2. Directory self-reference - ./
 - ❖ ./ → change to the current directory → no real action
 - ❖ GET ./cgi-bin/././broken.cgi HTTP/1.0
3. Premature URL ending - place URI in header
 - ❖ GET / HTTP/1.0\r\nHEADER: ../../cgi-bin/broken.cgi HTTP/1.0\r\n
 - ❖ Which equates to:
 - GET /HTTP/1.0\r\n
 - HEADER: ../../cgi-bin/broken.cgi HTTP/1.0\r\n
 - ❖ IDS may stop scanning after "HTTP/1.0"

Nikto IDS Evasion Techniques

GET /cgi-bin/broken.cgi HTTP/1.0

4. Prepend long random string

- ❖ GET /bunchofjunktomaketheURLlonger/..../cgi-bin/broken.cgi HTTP/1.0
- ❖ Everything before ../../ is ignored
- ❖ Scanner may only look at first 1,000 characters

5. Fake Parameter

- ❖ GET /index.htm?param=../../cgi-bin/broken.cgi HTTP/1.0
- ❖ Scanner may stop looking after "?"

Use alternate space (instead of space (0x20))

6. TAB → GET<tab>/cgi-bin/broken.cgi<tab>HTTP/1.0

A. Carriage return (0x0d)

B. Vertical tab (0x0b)

Nikto IDS Evasion Techniques

GET /cgi-bin/broken.cgi HTTP/1.0

7. Change the case of the URL

- ❖ GET /CGI-BIN/broken.cgi HTTP/1.0
- ❖ Windows systems are case insensitive
- ❖ Will be allowed through a Linux IDS and execute on a Windows web app

8. Use Windows directory separator (backslash → \)

- ❖ GET /cgi-bin\broken.cgi HTTP/1.0
- ❖ Will be allowed through a Linux IDS and execute on a Windows web app

NULL method

- ❖ GET%00 /cgi-bin/broken.cgi HTTP/1.0
- ❖ If IDS uses C-library strings, everything after the null (%00) is ignored since the null char is used to indicate end of string

Yet More Nikto IDS Evasion Modes

GET /cgi-bin/broken.cgi HTTP/1.0

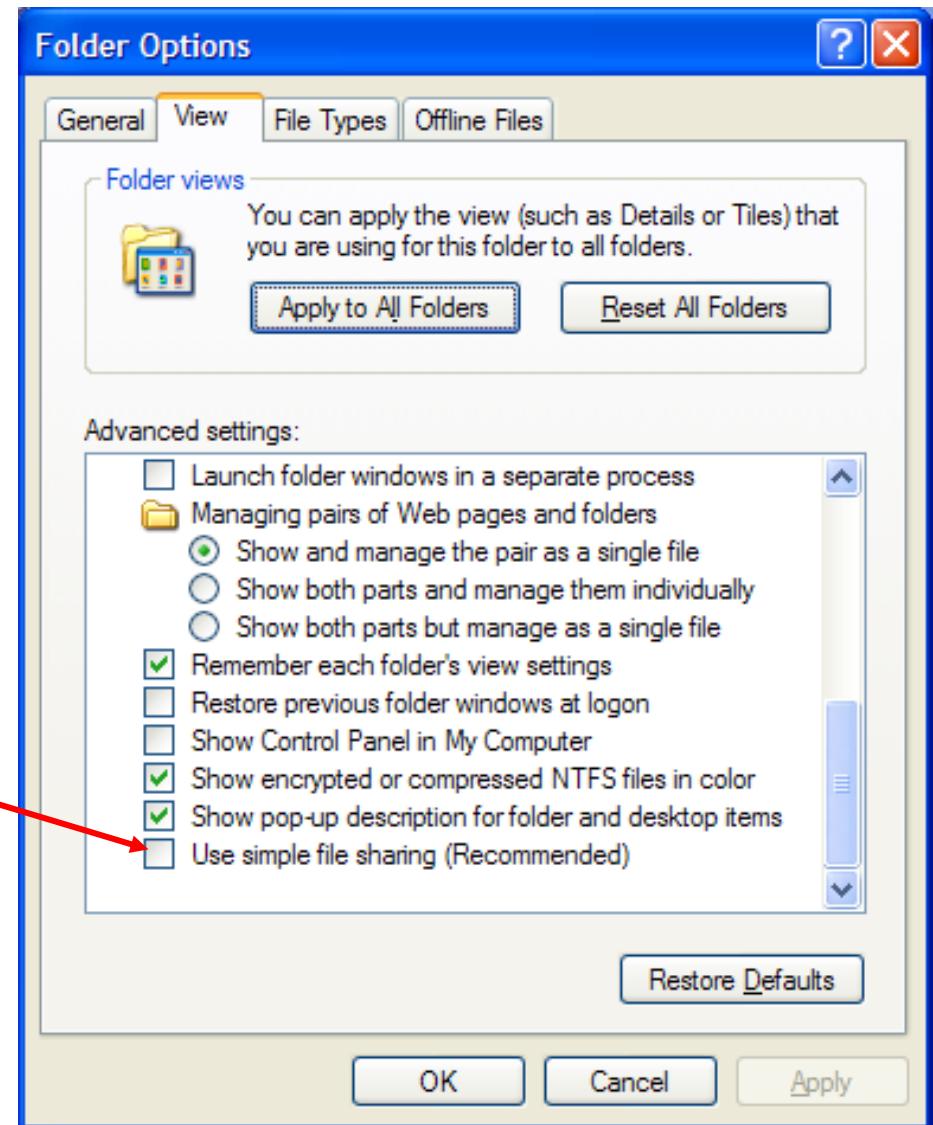
- Session splicing - send separate TCP segments in same connection
 - ❖ "G"
 - ❖ "ET"
 - ❖ "/cgi-"
 - ❖ "bin"
 - ❖ "/broken.cgi HTTP/1.0"
 - ❖ This is essentially **transport**-level IDS evasion
- Attacker can also craft hundreds of different combinations of these techniques
 - ❖ nikto -host http://scanme.nmap.org -evasion 126
 - ❖ Run evasions 1, 2, and 6
 - ❖ This exacerbates the IDS's job

Computer and Network Hacker Exploits

- Step 1: Reconnaissance
- **Step 2: Scanning**
 - ❖ Network Mapping
 - ❖ Determining Open Ports Using Port Scanners
 - ❖ Vulnerability-Scanning Tools
 - ❖ Intrusion Detection System and Intrusion Prevention System Evasion
 - ❖ **Shares**
- Step 3: Gaining Access
 - ❖ Application and Operating System Attacks
 - ❖ Network Attacks
 - ❖ Denial of Service Attacks
- Step 4: Maintaining Access
- Step 5: Covering Tracks and Hiding

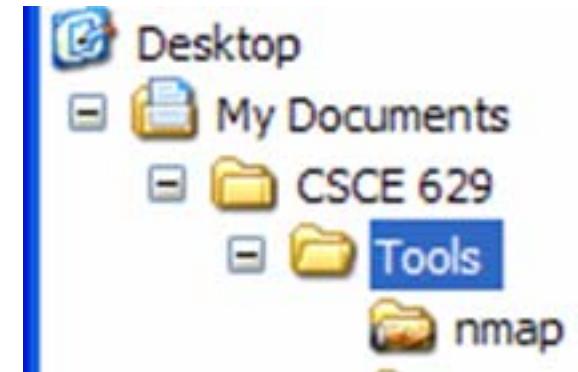
Windows LAN Scans

- ❑ Requires LAN (insider) access
- ❑ Windows machines have unique "features" built in by Microsoft to "enhance the user's experience"
- ❑ Microsoft has always supported file and printer sharing



Windows Network Shares

- Windows allows users to create shares
 - Shares can be files, directories, and drives
 - ❖ Win XP: "Hand" denotes the item is shared
 - ❖ Vista, Win7, ...: Icon is gone
 - To enable sharing, Microsoft developed NetBIOS
 - ❖ Network Basic Input/Output System
 - ❖ Allows computer communication over a LAN
 - ❖ Since NetBIOS is not routable over the Internet and everyone on the LAN is presumed trustworthy, Microsoft did not concern itself a great deal with security...
 - ... then LANs got increasingly complex
- So, Microsoft created NetBIOS over TCP/IP (NetBT)



Server Message Block (SMB)

- Client-server application-layer network protocol that provides sharing
- SMB can run on TCP port 139 (NetBIOS over TCP)
- Windows: SMB can run directly on top of TCP via TCP port 445
 - ❖ Preferred method

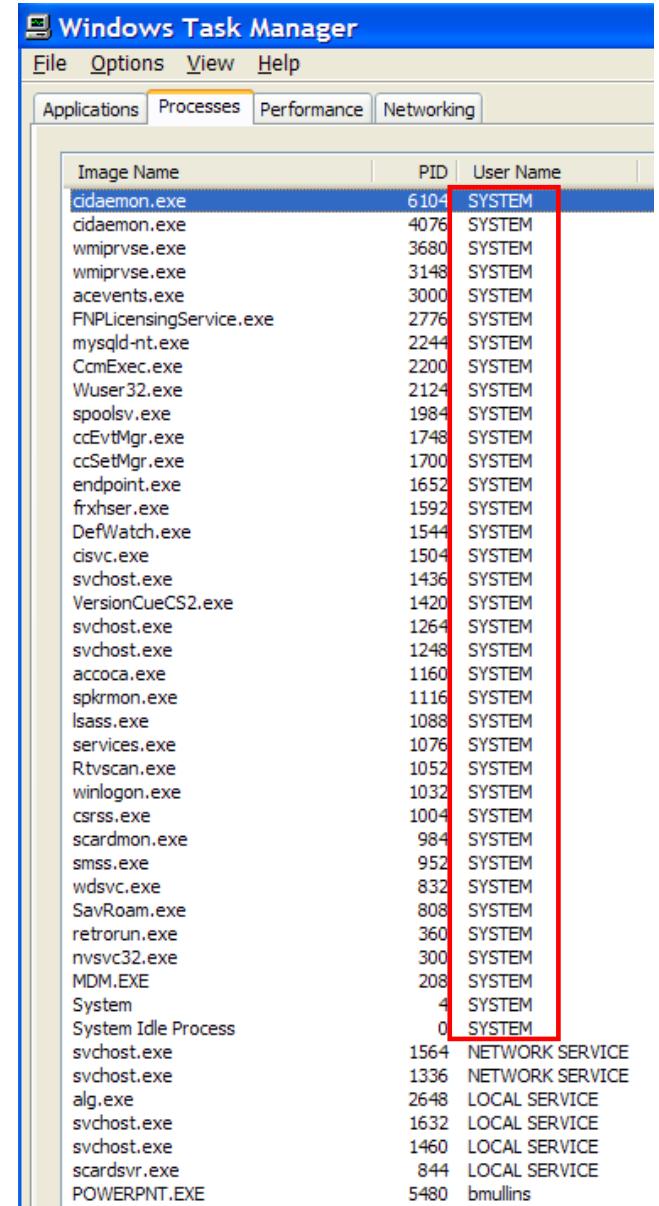
OSI	TCP/IP	Port 139	Port 445
Application			
Presentation	Application (e.g., HTTP)	SMB	SMB
Session (error recovery)		NetBIOS	
Transport	TCP/UDP	TCP/UDP	TCP/UDP
Network	IP	IP	IP
Link	Ethernet	Ethernet	Ethernet

Server Message Block (SMB)

- ❑ SMB protocol is implemented on Unix systems using Samba
- ❑ CIFS (Common Internet File System) was SMB as it existed in Windows 2000

Windows Network Shares

- Many local services run as **SYSTEM**
 - ❖ **SYSTEM has virtually unlimited privileges**
- **SYSTEM sometimes needs to access information on other machines**
 - ❖ Available shares, usernames, etc.
 - ❖ It can't log on to the other systems using UserID/password
 - It has no password
- **SYSTEM uses Null sessions via NetBT**
 - ❖ Unauthenticated connection
 - Undefined (null) username and domain / Empty password string



The screenshot shows the Windows Task Manager with the 'Processes' tab selected. A red box highlights the first column, 'Image Name', which lists various Windows services and system processes. All of these processes are running under the 'SYSTEM' account, as indicated by the 'User Name' column. The table includes columns for 'Image Name', 'PID', and 'User Name'.

Image Name	PID	User Name
cidaemon.exe	6104	SYSTEM
cidaemon.exe	4076	SYSTEM
wmiprvse.exe	3680	SYSTEM
wmiprvse.exe	3148	SYSTEM
acevents.exe	3000	SYSTEM
FNPoSicensingService.exe	2776	SYSTEM
mysqld-nt.exe	2244	SYSTEM
CmExec.exe	2200	SYSTEM
Wuser32.exe	2124	SYSTEM
spoolsv.exe	1984	SYSTEM
ccEvtMgr.exe	1748	SYSTEM
ccSetMgr.exe	1700	SYSTEM
endpoint.exe	1652	SYSTEM
frxhser.exe	1592	SYSTEM
DefWatch.exe	1544	SYSTEM
cisvc.exe	1504	SYSTEM
svchost.exe	1436	SYSTEM
VersionCueCS2.exe	1420	SYSTEM
svchost.exe	1264	SYSTEM
svchost.exe	1248	SYSTEM
accoca.exe	1160	SYSTEM
spkrmon.exe	1116	SYSTEM
lsass.exe	1088	SYSTEM
services.exe	1076	SYSTEM
Rtvscan.exe	1052	SYSTEM
winlogon.exe	1032	SYSTEM
cssrss.exe	1004	SYSTEM
scardmon.exe	984	SYSTEM
smss.exe	952	SYSTEM
wdsvc.exe	832	SYSTEM
SavRoam.exe	808	SYSTEM
retrorun.exe	360	SYSTEM
nvsvc32.exe	300	SYSTEM
MDM.EXE	208	SYSTEM
System	4	SYSTEM
System Idle Process	0	SYSTEM
svchost.exe	1564	NETWORK SERVICE
svchost.exe	1336	NETWORK SERVICE
alg.exe	2648	LOCAL SERVICE
svchost.exe	1632	LOCAL SERVICE
svchost.exe	1460	LOCAL SERVICE
scardsvr.exe	844	LOCAL SERVICE
POWERPNT.EXE	5480	bmuillins

Net Commands

- Used to update, fix, or **view** network settings

C:\Users\bmullins.CDN>net

The syntax of this command is:

NET

```
[ ACCOUNTS | COMPUTER | CONFIG | CONTINUE | FILE | GROUP | HELP |
HELPMSG | LOCALGROUP | PAUSE | SESSION | SHARE | START |
STATISTICS | STOP | TIME | USE | USER | VIEW ]
```

C:\Users\bmullins.CDN>

- On the next slide, I view my computer's network settings

Hidden shares are indicated by a \$ (e.g. C\$)

C:\Users\bmullins.CDN>net share

	Share name	Resource	Remark
<hr/>			
Hidden	C\$	C:\	Default share
	G\$	G:\	Default share
	IPC\$		Remote IPC
	S\$	S:\	Default share
	ADMIN\$	C:\WINDOWS	Remote Admin
Visible	My Music	G:\My Documents\My Music	
	The command completed successfully.		

To see the contents of a hidden share, you must use an administrator's account on the target

C:\Users\bmullins.CDN>net user

User accounts for \\DESKTOP-9GUNCEU

VMware_Conv_SA	barry-local	DefaultAccount
fatcat	ghost	
The command completed successfully.		

C:\Users\bmullins.CDN>net accounts

Force user logoff how long after time expires?:	0
Minimum password age (days):	0
Maximum password age (days):	60
Minimum password length:	14
Length of password history maintained:	None
Lockout threshold:	Never
Lockout duration (minutes):	Never
Lockout observation window (minutes):	60
Computer role:	WORKSTATION
The command completed successfully.	

Net View

Client/server network

Peer-to-peer
Windows computer
network

- Scan the LAN for other computers in domains or workgroups

```
net view [\ComputerName] [/domain[:DomainName]]
```

Domain or workgroup

```
C:\Users\Administrator>net view /domain:lissard2
Server Name          Remark
```

\\AS-LISSARD2-02	AS-LISSARD2-02
\\BS-LISSARD2-01	Disk Station
\\DC-LISSARD2-01	DC-LISSARD2-01
\\DC-LISSARD2-02	
\\DESKTOP-2GC8FPE	
\\DESKTOP-9GUNCEU	
\\DS-LISSARD2-01	
\\FS-LISSARD2-01	
\\JONNYLACEYPC	
\\JPWINDOWS8	JPWindows8
\\LISW10797U	
\\LISW744PA	
\\LISW744PC	
\\LISW744XY	

Displaying SMB Shares

- Display available (not hidden) shares on another computer
 - ❖ `net view [\ComputerName]`

```
C:\Users\user.WIN-AJACIDD48FR>net view \\10.1.2.7
Shared resources at \\10.1.2.7
```

Share name	Type	Used as	Comment

Ace_Faculty	Disk		
Admin	Disk		Admin Use Only
ghost	Disk		ghost folder
ISO	Disk		ISO files
Mullins	Disk		
music	Disk		System default shared folder
NetBackup	Disk		System default shared folder
PCE	Disk		PCE
PCE Share	Disk		PCE Share Folder

Displaying SMB Shares

- Displays SMB shares on remote computer
 - ❖ `smbmap -d domain -H x.x.x.x`
- May have to provide a set of credentials if share is restricted
 - ❖ `smbmap -u user -p password -d domain -H x.x.x.x`

```
root@kali:~/Desktop# smbmap -d cdn-01 -H 10.1.2.7
[+] Finding open SMB ports....
[+] Guest SMB session established on 10.1.2.7...
[+] IP: 10.1.2.7:445      Name: 10.1.2.7
      Disk                                         Permissions
      ----
      Ace_Faculty                               NO ACCESS
      Admin                                     NO ACCESS
      ghost                                    NO ACCESS
```

- `smbclient` works too
 - ❖ `smbclient -L 10.1.2.7 -U user -W domain`

Displaying Domain Users

□ **net user /domain**

```
C:\Users\bmullins.CDN>net user /domain
```

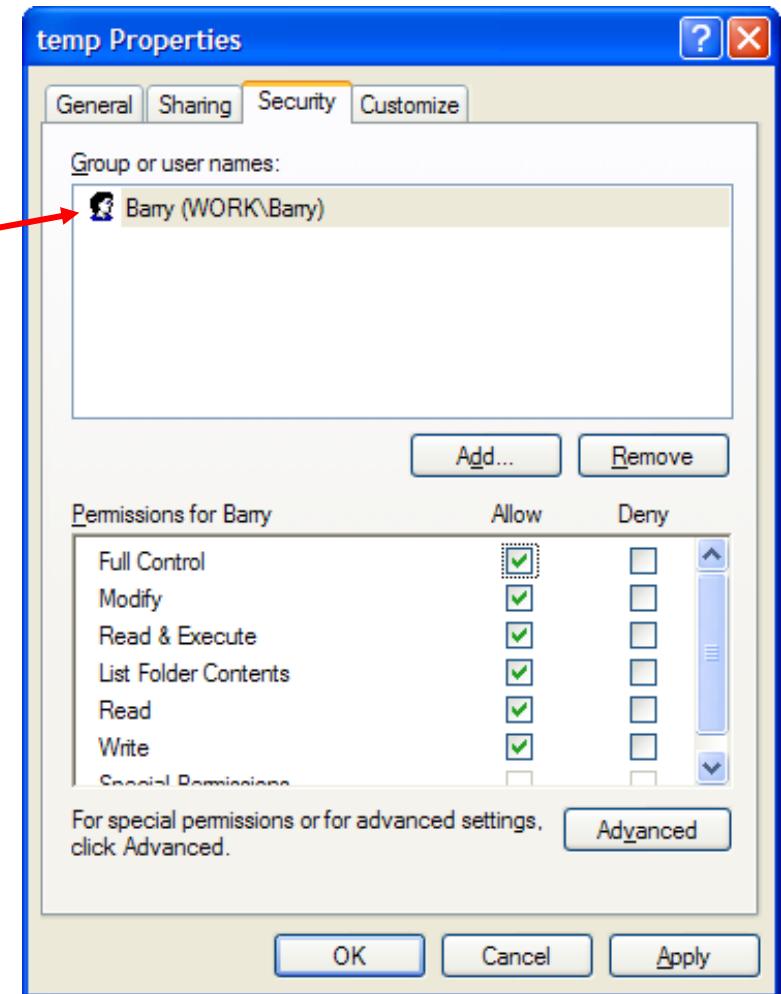
```
The request will be processed at a domain controller for domain CDN.LOCAL.
```

```
User accounts for \\DC-CDN-01.CDN.LOCAL
```

aaragon	aduchane	alin
aroberts	atroya	bburfeind
bfrogberg	bheitmeyer	bjeffries
blambert	blaw	bmullins
bnolan	bvoetberg	cbramlette
ccady	ccunningham	cpeters
crodriguez	crondeau	csolberg

Restricted-Access Share

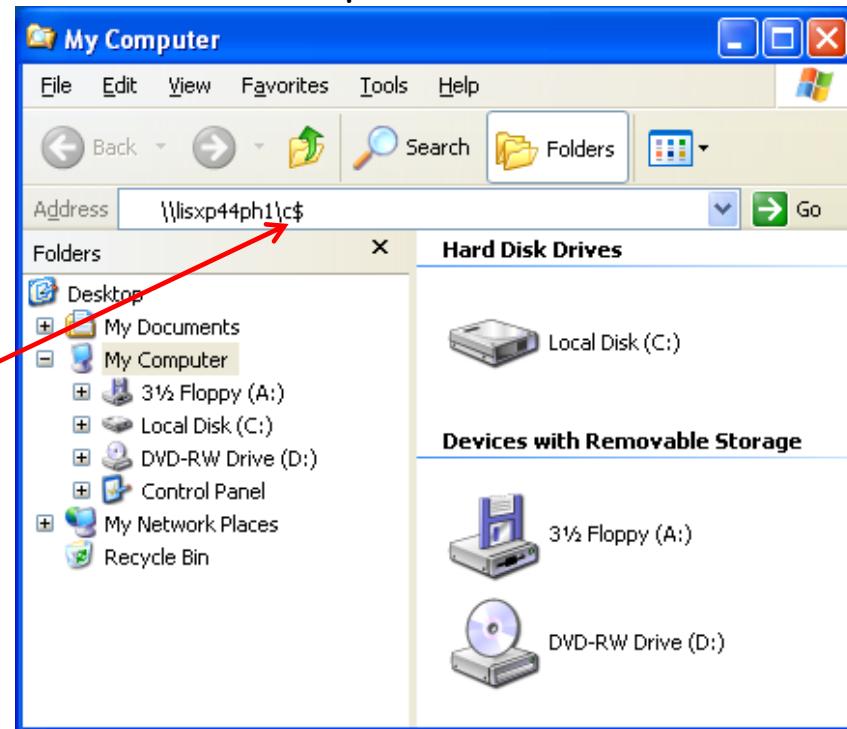
- ❑ A user can restrict access to files/folders to self
 - ❖ Not even an administrator or SYSTEM can access
 - ❖ You can see it but not access the contents
- ❑ Do not change file permissions to access the files/folders!
- ❑ If this happens, you must connect as each user on the target until you find the owner



Mapping Drives (1)

- Once you know some users and their passwords, you can map their share to a local drive and search it:
 - ❖ > `net use g: \\10.1.2.122\c$` a hidden share
 - ❖ > `net use g: \\10.1.2.122\my music` a visible share
 - After "The password or user name is invalid for \\..."
 - You will be asked for a username and a password
 - Unless you already gave the username and password

- ❖ Could also use Windows explorer and enter credentials when asked
 - Need admin creds here since it is a hidden share



Mapping Drives (2)

Map to remote share

- ❖ `net use g: \\10.1.2.122\My Music /u:<target>\jsmith`
 - Asks for jsmith password if not provided
 - Must use `/u:<target>\jsmith` since user account is on local (target) machine (e.g., `/u:lisxp41b1\jsmith` or `/u:10.1.1.6\jsmith`)

Share is now effectively a hard drive on your machine

Move to share → g:

Search for flags (on g:)

- ❖ `dir /s/a g:\flag*.txt` or just `dir /s/a flag*.txt`
- ❖ `/a` = all; useful for finding hidden files
- ❖ `/s` = Displays files in specified directory and all subdirectories
- ❖ Will only search files in My Music folder and below
 - `G:\My Documents\My Music`

Not searched

C:\Users\bmullins.CDN>net share		
Share name	Resource	Remark
C\$	C:\	Default share
G\$	G:\	Default share
IPC\$		Remote IPC
S\$	S:\	Default share
ADMIN\$	C:\WINDOWS	Remote Admin
My Music	G:\My Documents\My Music	

The command completed successfully.

Could insert password here

Mapping Drives (3)

- Did you find a flag file?
- If not, disconnect the drive
 - ❖ `net use g: /d`

>Password included this time

- ... and repeat

```
net use g: \\10.1.2.122\My Music socialengr /u:<target>kmitnick  
g:  
dir /s/a flag*.txt
```

- Log in as each user you know (`/u:<username>`) and have the password
- Remember to disconnect when done
 - ❖ `net use g: /d`

Example of Mapping Drives and Search

```
C:\ Command Prompt  
C:\Documents and Settings\Barry>net use i: \\lisxp462vlt\tools /u:user  
The password or user name is invalid for \\lisxp462vlt\tools.  
Enter the password for 'user' to connect to 'lisxp462vlt':   
The command completed successfully.  
  
C:\Documents and Settings\Barry>i:  
I:>dir /s/a flag?.txt  
Volume in drive I is System Drive  
Volume Serial Number is 0452-057C  
  
Directory of I:\  
  
01/23/2008  06:44 PM           52 flag.txt  
                   1 File(s)      52 bytes  
  
Total Files Listed:  
                   1 File(s)      52 bytes  
                   0 Dir(s)  72,299,556,864 bytes free  
  
I:>type flag.txt  
This is a test of the emergency broadcast system.  
  
I:>c:  
  
C:\Documents and Settings\Barry>net use * /d  
You have these remote connections:  
  
I:          \\lisxp462vlt\tools  
Continuing will cancel the connections.  
  
Do you want to continue this operation? (Y/N) [N]:   
The command completed successfully.  
  
C:\Documents and Settings\Barry>i:  
The system cannot find the drive specified.  
C:\Documents and Settings\Barry>
```

↑
Enter password