Intrusion & Anomaly Detection

Attacks

Lisa Frye, Instructor
frye@kutztown.edu
Kutztown University

Network Forensics

- "Unusual" Traffic
- "Normal" Traffic

- Gather network forensic evidence
  - Proactive
  - Reactive

- Why is discovery and reconnaissance important?

Types of Attacks

- Passwords
- Floods
- Ping sweeps / scans
- Port scans
- Denial of Service
- Spoofing / Poisoning
- Session hijacking
- Miscellaneous

Floods

- ICMP
- TCP
- Application
- SYN Flood

Scans

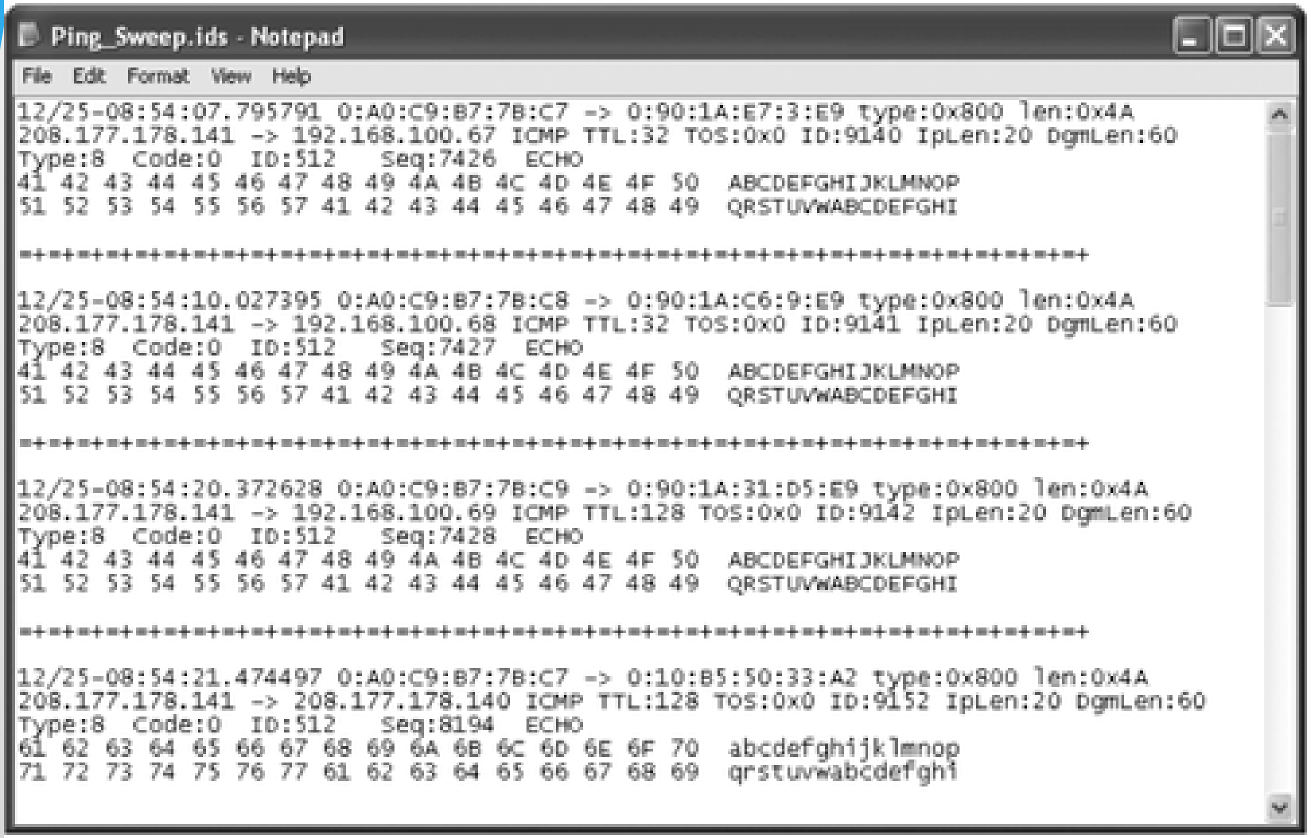
- Purpose?

ARP Scan

- Used to find local hosts
- Why only local hosts?
- Response to ARP request

ICMP Ping Scan

- Purpose?
- Protocol used?
- ICMP often blocked, why?
- How would you detect this type of attack?



Ping_Sweep.ids - Notepad

File Edit Format View Help

```
12/25-08:54:07.795791 0:A0:C9:B7:7B:C7 -> 0:90:1A:E7:3:E9 type:0x800 len:0x4A
208.177.178.141 -> 192.168.100.67 ICMP TTL:32 TOS:0x0 ID:9140 IpLen:20 DgmLen:60
Type:8  Code:0  ID:512   Seq:7426  ECHO
41 42 43 44 45 46 47 48 49 4A 4B 4C 4D 4E 4F 50  ABCDEFGHIJKLMNOP
51 52 53 54 55 56 57 41 42 43 44 45 46 47 48 49  QRSTUVWABCDEFGHI

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

12/25-08:54:10.027395 0:A0:C9:B7:7B:C8 -> 0:90:1A:C6:9:E9 type:0x800 len:0x4A
208.177.178.141 -> 192.168.100.68 ICMP TTL:32 TOS:0x0 ID:9141 IpLen:20 DgmLen:60
Type:8  Code:0  ID:512   Seq:7427  ECHO
41 42 43 44 45 46 47 48 49 4A 4B 4C 4D 4E 4F 50  ABCDEFGHIJKLMNOP
51 52 53 54 55 56 57 41 42 43 44 45 46 47 48 49  QRSTUVWABCDEFGHI

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

12/25-08:54:20.372628 0:A0:C9:B7:7B:C9 -> 0:90:1A:31:D5:E9 type:0x800 len:0x4A
208.177.178.141 -> 192.168.100.69 ICMP TTL:128 TOS:0x0 ID:9142 IpLen:20 DgmLen:60
Type:8  Code:0  ID:512   Seq:7428  ECHO
41 42 43 44 45 46 47 48 49 4A 4B 4C 4D 4E 4F 50  ABCDEFGHIJKLMNOP
51 52 53 54 55 56 57 41 42 43 44 45 46 47 48 49  QRSTUVWABCDEFGHI

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

12/25-08:54:21.474497 0:A0:C9:B7:7B:C7 -> 0:10:B5:50:33:A2 type:0x800 len:0x4A
208.177.178.141 -> 208.177.178.140 ICMP TTL:128 TOS:0x0 ID:9152 IpLen:20 DgmLen:60
Type:8  Code:0  ID:512   Seq:8194  ECHO
61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70  abcdefghijklmnop
71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69  qrstuvwabcdefghi
```

Figure 9-15 A log file record displaying the signature of an automated ping sweep

TCP Port Scans

- SYN Scan or TCP Half-Open or "Stealth" Scan
- TCP Full Connect Scan
- FIN Scan
- NULL Scan
- Xmas Scan
- ACK Scan
- UDP Port Scan
- Random back door scans
- Specific Trojan scans

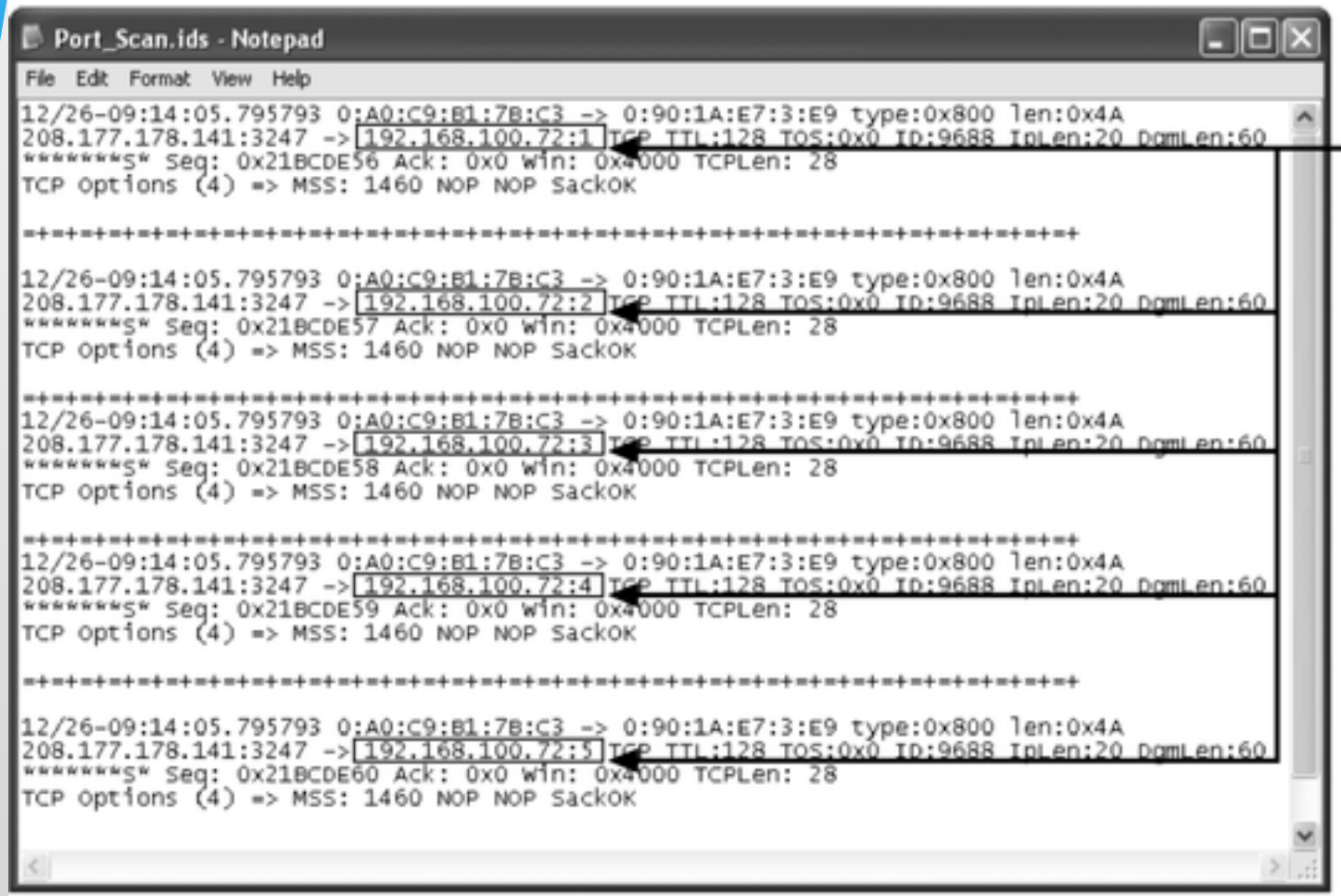


Figure 9-16 A log file record displaying the signatures of a port scan

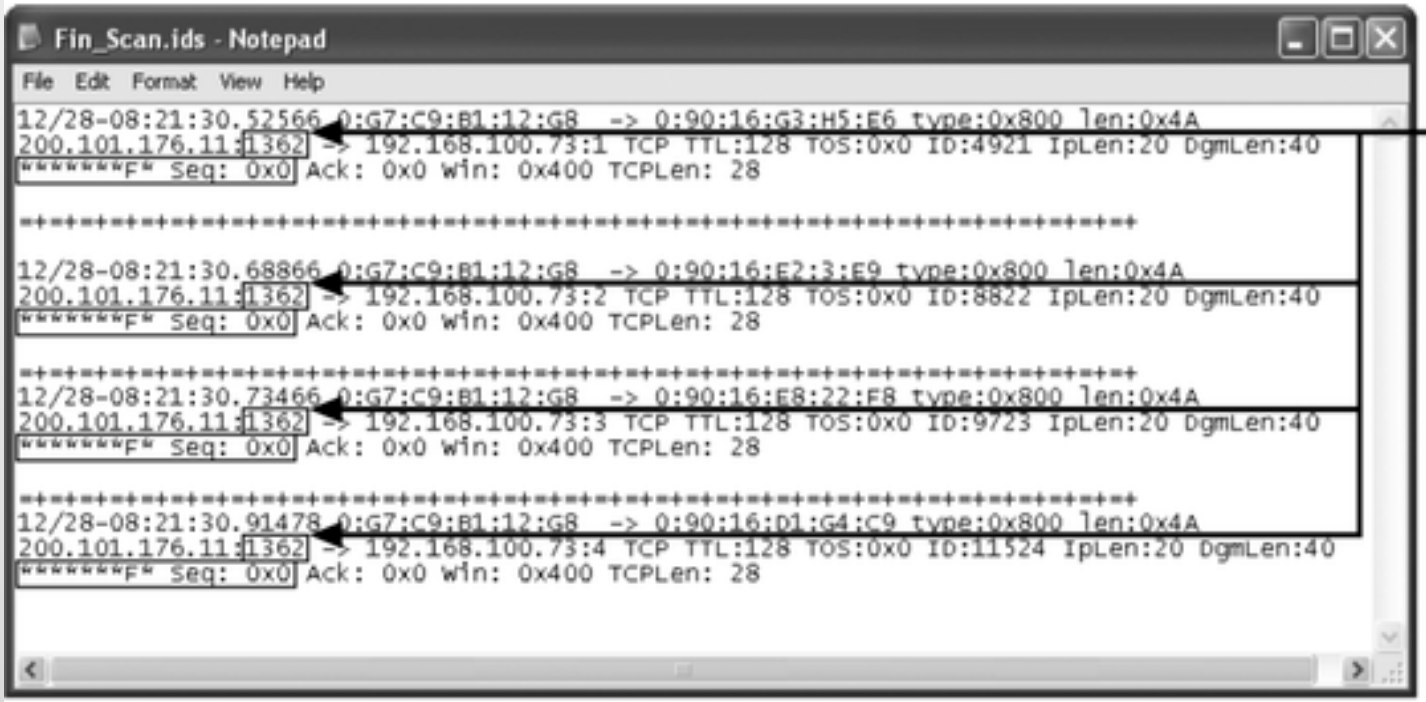


Figure 9-19 The signatures of a FIN scan conducted using Nmap

IP Scans

- IP Services

nmap Scans

- Circumvent three-way handshake
- Purpose?

Discover Routers

- Why common?
- ICMP

Denial of Service Attacks

- Purpose?

- Ping of Death
- Land exploit
- Smurf DOS attack
- RPC Locator DOS attack

Distribute DoS Attacks

- Handler machine
- Agents or Zombies
- Send command via IRC

- Prevention

Spoofing

- IP Address spoofing
- ARP poisoning
- Web spoofing
- DNS spoofing

IP Address Spoofing

- Explain
- Hacker enters fake IP in header as source IP, hacker may still not get return packet. Why?
- Hacker must determine sequence number. Why is this difficult?

IP address	MAC address
206.23.19.233	00-50-F2-7C-69-32
206.23.19.101	01-40-A1-36-21-03
206.23.19.32	02-59-B2-52-C5-01

IP address = 206.23.19.233
MAC address = 00-50-F2-7C-69-32

IP address = 206.23.19.101
MAC address = 01-40-A1-36-21-03

IP address = 206.23.19.32
MAC address = 02-59-B2-52-C5-01

IP address	MAC address
206.23.19.233	00-50-F2-7C-69-32
206.23.19.101	01-40-A1-36-21-03
206.23.19.32	~~02-59-B2-52-C5-01~~

06-32-A5-A9-34-89-01
MAC address changed

Data redirected to attacker's computer

IP address = 206.23.19.49
MAC address = 06-32-A5-A9-34-89-01
Attacker's computer

IP address = 206.23.19.233
MAC address = 00-50-F2-7C-69-32

IP address = 206.23.19.101
MAC address = 01-40-A1-36-21-03

IP address = 206.23.19.32
MAC address = 02-59-B2-52-C5-01

ARP Spoofing

- IP address associated with more than 1 MAC address
- Frequent changes to ARP mappings on hosts and devices
- Abnormal amount of ARP requests
- Numerous invalid entries in ARP table

Web and DNS Spoofing

- Web Spoofing – explain
- Defense?

- DNS Spoofing – explain

TCP Session Hijacking

- Explain
- Source routing
- ACK Storms
- Wireless networks

Man-In-The-Middle (MITM) Attack

- Explain
- Numerous methods for each step

- Two types
  - Passive
  - Active

Create MITM Attack

- List steps for conducting a MITM attack

Replay Attacks

- Explain
- Anti-replay features
- Example – purchase a TV

Other Attacks

- Unusual protocols and applications
- Invalid or "dark" destination addresses
- Malformed packets
- IP fragmentation overriding
- TCP splicing
- "Phone home" traffic
- SNMP exploit
- imapd attack (UNIX)

Attack Trees

- Identify possible attack goals
- Identify all attacks against each goal and add them to tree
- Research all node values