Hacking Exposed 7
Network Security Secrets & Solutions

Chapter 2 Scanning

Scanning

- Determining if the system is alive
- Determining which services are running or listening
- Detecting the operating system
- Processing and storing scan data

Determining If the System is Alive

- Network ping sweeps
  - ARP host discovery: on the same subnet
    - Arp-scan: run as root by sudo to list IP-MAC
    - Nmap (Network Mapper): host and service discovery with various options (host only: -PR –sn)
    - Cain (Windows-only): beyond host and service discovery
  - ICMP host discovery: remote host/router
    - ICMP ECHO REQUEST, ICMP ECHO REPLY, ICMP TIMESTAMP, ICMP ADDRESS MASK, etc.
    - Ping: OS utilities for ECHO REQUEST/REPLY
    - Nmap: ICMP ping/address mask/timestamp, ARP ping, TCP ping
    - Hping3 and nping: any combinations of flags on any combinations of packet types, spoofing MAC/IP
    - Superscan: multiple ICMP in parallel
  - TCP/UDP host discovery: when internal and/or external ICMP is not permitted
    - Servers: TCP/UDP service ports
    - Desktops: local firewall to ban inbound connections, but accessible through remote desktop, file sharing, and disabled local firewall
    - Nmap/Superscan/Nping: all ports (slow and noisy) or specific ports

Address Resolution Protocol (ARP)

- root@kali:~# arp-scan --interface=wlan0 –localnet
- Interface: wlan0, datalink type: EN10MB (Ethernet)
- Starting arp-scan 1.9 with 256 hosts (http://www.nta-monitor.com/tools/arp-scan/)
- 10.0.1.3 0 b:1a:a0:c2:94:c0 Dell Inc
- 10.0.1.57 0b:0c:29:34:f9:6a VMware, Inc.
- 10.0.1.253 0b:19:55:9d:60:c1 CISCO SYSTEMS, INC.
- 29 packets received by filter, 0 packets dropped by kernel Ending arp-scan 1.9: 256 hosts scanned in 2.259 seconds (113.32 hosts/sec). 29 responded

Nmap –sn –PR –send-IP <IP-range>

- NMAP not only sends an ICMP ECHO REQUEST packet it also performs an ARP ping, some TCP pinging.
- **Understanding what tools do, is really important**. If the target network is being monitored by an IDS, you may inadvertently trigger an alert because of all of the extra traffic being generated

Ping Sweeps Countermeasures

- Detection
  - IDS: snort
  - Commercial firewall: network or desktop
    - Detect ICMP, TCP, UDP ping sweeps
      - A pattern of ICMP/TCP/UDP packets from a particular system or network
  - Host based tools: Scanlogd, courtney, ippl, protolog
  - **Not just tools, eyeballs count.**
- Prevention
  - ACL in firewall: limit ICMP traffic into your networks or systems
  - Allow only ECHO_REPLY, HOST UNREACHABLE, TIME EXCEEDED into specific hosts in DMZ; allow only ISP's specific IP addresses
    - Loki2: hackers use it to backdoor the OS and tunnel data in ICMP ECHO
  - Pingd: move ICMP from kernel to user space

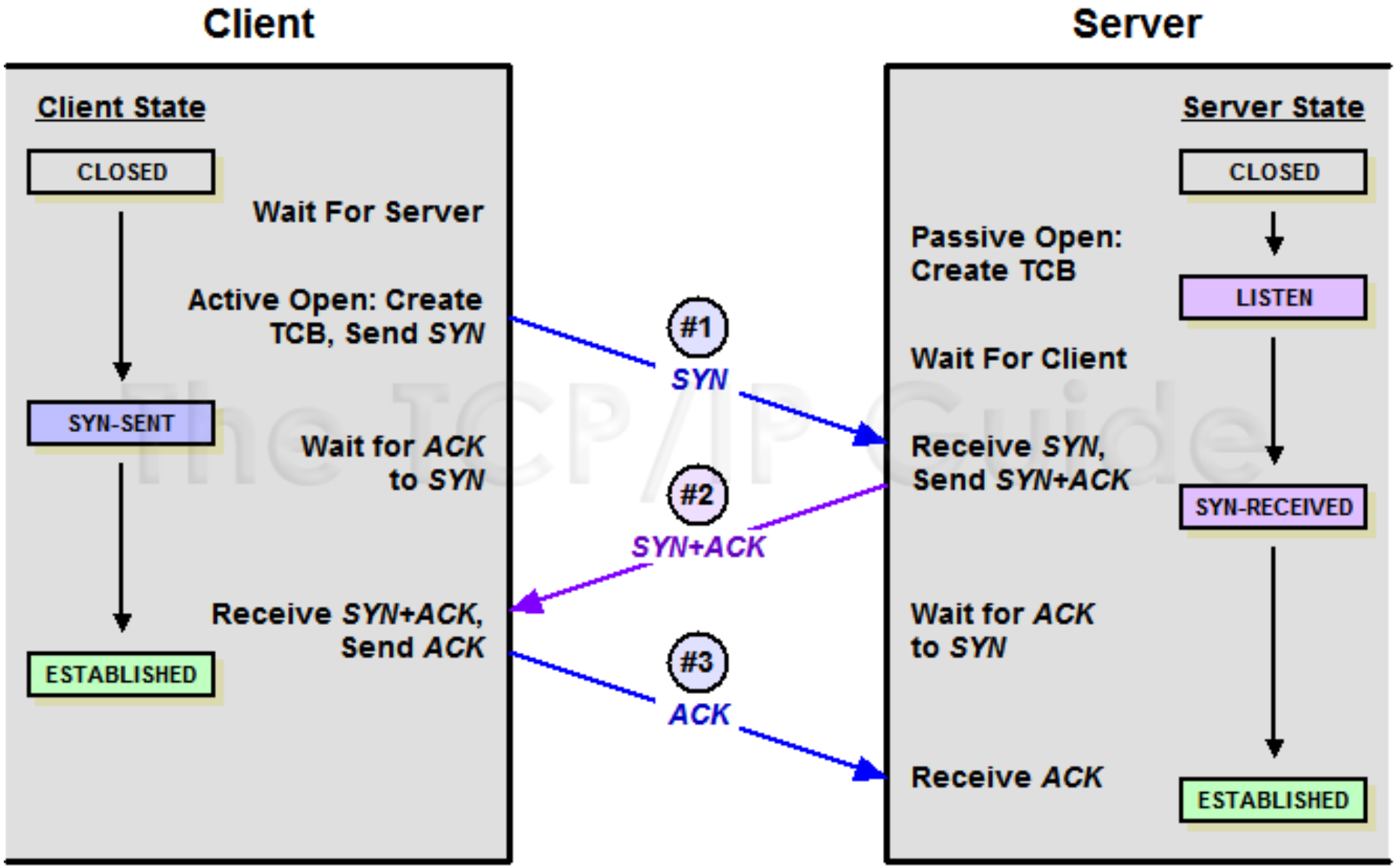
ICMP Attacks Illustrated

The simplicity of the ICMP protocol and the lack of awareness of security issues related to protocol has l
me to put in place this paper to attempt to illustrate some of the possible attacks using ICMP as a tool.

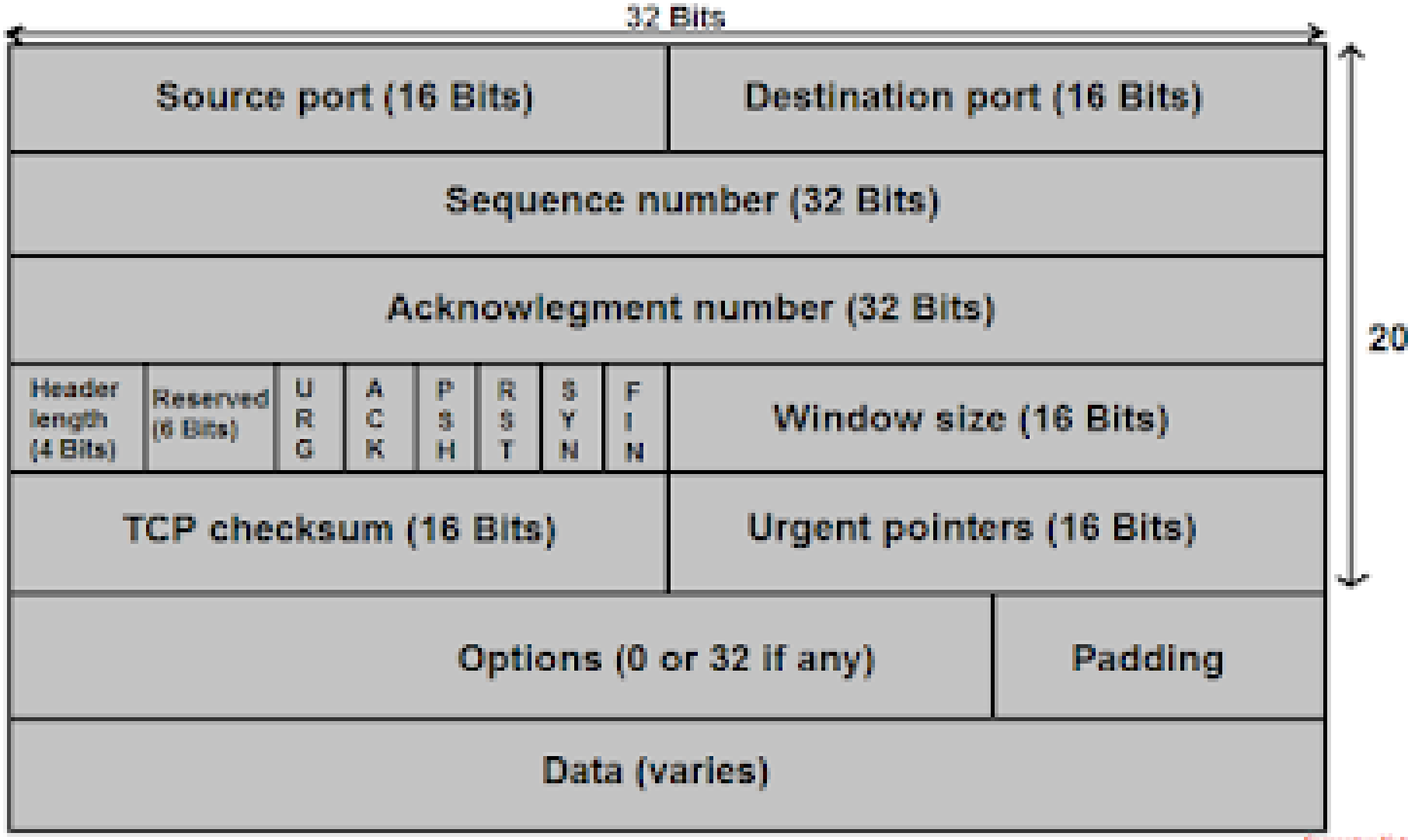
Determining Which Services Are Running or Listening

- Port scanning
  - Identifying TCP/UDP services running on the target
  - Identifying type of OS of the target
  - Identifying applications or versions of a service
  - Scan types (anomalous TCP packets)
    - TCP connect scan (3-way handshake), TCP SYN scan (half-open scan, SYN then SYN/ACK or RST/ACK), TCP FIN scan (RST if closed port), TCP Xmas Tree scan (FIN/URG/PUSH), TCP null scan, TCP ACK scan, TCP Windows scan, TCP RPC scan, UDP scan (ICMP port unreachable msg, if closed port)
  - Nmap
    - Port scanning after host discovery
    - Options: -oN (out to a human-readable file), -f (fragment packets to pass firewall/IDS), -D (intermix decoy scans and real scans)
  - SuperScan (Windows-based with GUI), ScanLine (Windows-based with command-line), netcat (Windows/Linux, minimize your footprint on a compromised system, Swiss Army knife of security; netcat for Nmap = ncat)

3-way handshake



TCP Header


32 Bits
Source port (16 Bits)
Destination port (16 Bits)
Sequence number (32 Bits)
Acknowlegment number (32 Bits)
Header length (4 Bits)
Reserved (6 Bits)
URG
ACK
PSH
RST
SYN
FIN
Window size (16 Bits)
TCP checksum (16 Bits)
Urgent pointers (16 Bits)
Options (0 or 32 if any)
Padding
Data (varies)
20

TCP FLAG

- URG (1 bit): indicates that the Urgent pointer field is significant
- ACK (1 bit): indicates that the Acknowledgment field is significant. All packets after the initial SYN packet sent by the client should have this flag set.
- PSH (1 bit): Push function. Asks to push the buffered data to the receiving application.
- RST (1 bit): Reset the connection
- SYN (1 bit): Synchronize sequence numbers. Only the first packet sent from each end should have this flag set. Some other flags and fields change meaning based on this flag, and some are only valid for when it is set, and others when it is clear.
- FIN (1 bit): Last packet from sender.

Port Scanning Countermeasures

- Detection
  - Snort: packet fragmentation handled after 1.x
  - Scanlogd: detect and log
  - Firewalls:
    - e.g., detect SYN scans but ignore FIN scans
    - threshold logging – group alerts to one email
  - Attacker: listen for particular ports and alert in Win
- Prevention
  - Disabling all unnecessary services/ports
  - /etc/inetd.conf in UNIX

Detecting The Operating System

Active Operating System Detection

- Useful info for vulnerability mapping
  - Banner grabbing: some applications tell it all
  - Scanning available ports: some services are OS specific!
  - Stack fingerprinting: TCP/IP stack implementation
- Making guess from available ports
  - Windows: ports 135, 139, 445 (139 only for Windows 95/98); 3389 for RDP (Remote Desktop Protocol)
  - UNIX: TCP 22 (SSH), TCP 111 (RPC portmapper=port 135), TCP 512-514 (Berkeley Remote services, rlogin), TCP 2049 (NFS, Network File System), 3277x (RPC, Remote Procedure Call in Solaris)
- Active stack fingerprinting (Phrack Magazine)
  - Vendors interpret RFCs differently when writing TCP/IP stack
  - Nmap –O: signature listing at Nmap-os-fingerprints
    - FIN probe (Windows 7/200x/Vista respond with FIN/ACK), Bogus flag probe, Initial Sequence Number sampling, “Don’t fragment bit” monitoring, TCP initial window size, ACK value (+0 or +1), ICMP message quenching, ICMP message quoting, ICMP message echoing integrity, TOS, fragmentation handling, TCP options
- Countermeasures
  - Detection: same detection tools: Snort, Scanlogd, ecc.
  - Prevention: secure proxy or firewall, Active Defence

Port 135, 139, 445

- Port 135 Microsoft EPMAP, end-point mapper. Microsoft relies upon DCE RPC to remotely manage services. Some services that use port 135 of end-point mapping are: DHCP server, DNS server, WINS server
- Port 139 NetBIOS
- Port 445 MS Server Message Block (SMB), SAMBA-compatible

.:: Project Loki: ICMP Tunneling ::.

Current issue : #49 | Release date : 1996-11-08 | Editor : daemon9 — Get tar.gz

TCP/IP Stack Fingerprint

The TCP/IP fields that may vary include the following:

- Initial packet size (16 bits)
- Initial TTL (8 bits)
- Window size (16 bits)
- Max segment size (16 bits)
- Window scaling value (8 bits)
- "don't fragment" flag (1 bit)
- "sackOK" flag (1 bit)
- "nop" flag (1 bit)

These values may be combined to form a 67-bit signature, or fingerprint, for the target machine. Just automatically checking the Initial TTL and window size fields is often enough in order to successfully identify an operating system.

Detecting The Operating System

Passive Operating System Detection

- To be stealthy to IDS: passive
- Passive stack fingerprinting
  - At a central location or a port with packet capture (by port mirroring)
  - Siphon: a passive port-mapping, OS identification, and network topology tool
    - Passive signatures in osprints.conf
      - TCP/IP session: TTL, window size, DF (Don't Fragment), etc.
  - Tend to fail if: (1) applications build their own packets, (2) not able to capture packets, (3) a remote host changes the connection attributes (active detection also fails on this)
- Countermeasures
  - Same as OS detection countermeasures

Processing and Storing Scan Data

- Efficiency in managing scan data → speed to compromise a large number of systems
- Metasploit
  - A vast platform of tools, payload, and exploits
  - PostgreSQL for database
  - db_connect: tells metasploit how to connect to database and which database to use
  - db_nmap (root required): run Nmap scans
    - Metasploit could scan but slower than Nmap
  - db_import: import Nmap results into database, commands:
    - hosts: show hosts and their OS
    - services: show all available ports and services
    - Filtering (-s) to see, e.g., all hosts with SSH or running Windows 2008