Cybersecurity

Linde Nouwen

KdG Karel de Grote Hogeschool

CyberSecurity Scanning

Karel de Grote Hogeschool

Scanning

- Within the “methodology”:
  - Footprinting
    - Information on IP ranges (internal/external)
  - Scanning
    - Identify hosts within ranges
    - Enumeration (later): Determine ports → services/versions
  - Exploit services

Scanning

- Detection by IDS (IPS) possible
- Tread with care (proxy)

Scanning

- Scan types/steps:
  - Network Scan/Sweep
  - Port Scan
  - Fingerprinting

Extra:

- Vulnerability Scan (Exploitation)

CyberSecurity Scanning

Network Scanning/Sweep

Karel de Grote Hogeschool

Scanning

- Network Scan/Ping sweeper:
  - Identify active hosts within the discovered ranges
  - ICMP echo requests → wait for echo reply
  - Drawback:

a) "ping" blocked by default
   - Prevent network mapping
   - Stop DOS-attacks

b) sweep triggers IPS
   - Stop malicious scan = block IP

CyberSecurity Scanning

TCP & UDP Scan

Karel de Grote Hogeschool

Scanning

- Port Scanner/TCP-ping Tool:
  - No ICMP but TCP (or UDP)
  - Query if TCP/UDP port is open
  - Port = service

List of well-known services:
https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

Note: Socket = IP + port

Scanning

- Ports you should know:
  - TCP 20 and 21 (FTP)
  - TCP 22 (SSH)
  - TCP 23 (Telnet)
  - TCP 25 (Simple Mail Transfer Protocol, SMTP)
  - TCP and UDP 53 (Domain Name System, DNS)
  - UDP 69 (Trivial File Transfer Protocol, tftp)
  - TCP 80 (Hypertext Transfer Protocol, HTTP)
  - TCP 110 (Post Office Protocol v3, POP3)
  - UDP 161 and 162 (Simple Network Management Protocol, SNMP)
  - UDP 443 (Secure Sockets Layer over HTTP, https)

    Sometimes portnumbers differ from service!

Scanning

- Scanning + Vulnerability analysis combined:
  - Enumeration of vulnerabilities
  - Risk identification
  - Tools:
    - OpenVAS (Greenbone)
    - Nessus
    - Nexpose
    - Retina

Scanning

Port-states

- **Open** or **Accepted**: The host sent a reply indicating that a service is listening on the port.
- **Closed** or **Denied** or **Not Listening**: The host sent a reply indicating that connections will be denied to the port.
- **Filtered**, **Dropped** or **Blocked**: There was no reply from the host.

Scanning

Port-states (nmap)

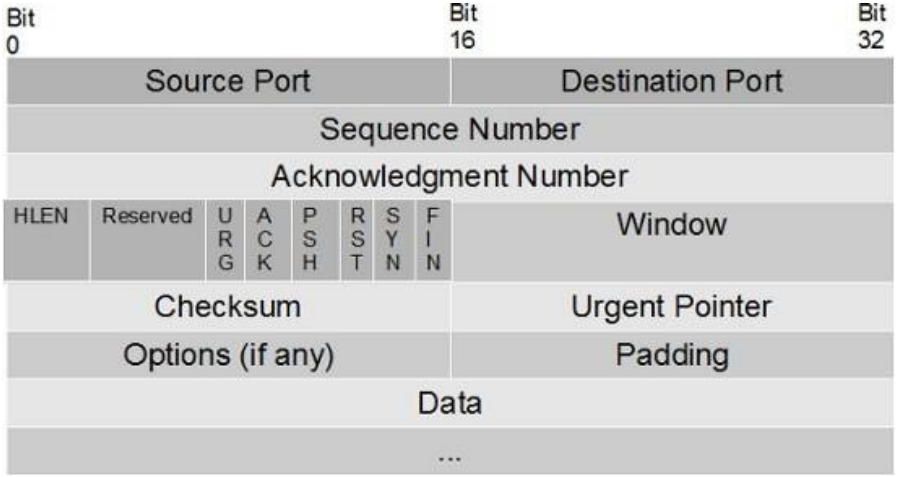
- **Open:** a port in this state is available and listening for connections to the associated service on that port. For example, a public webserver could have opened the TCP/port 80 (HTTP), TCP/443 (HTTPS), UDP/53 (DNS) and others.
- **Closed:** although, a closed port is accessible, it has no associated application or service that responds to connection requests.
- **Filtered:** a filtered port cannot be accessed because there is a packet filtering device which prevents the scanner to determine if that port is open or closed. The intermediate device may be a router using ACL's or a firewall.
- **Non-filtered**: a port in this state is accessible but we cannot determine with certainty whether it's open or closed. This state is a result from a specific scanning technique (ACK scan).
- **Open | Filtered:** This is an ambiguous state in which the scanner could not determine whether the port is open or filtered and is likely to be obtained when a scanning technique in which an open port cannot respond is used. (UDP scan or FIN, XMAS, Null)
- **Closed | Filtered:** occurs when the scanner cannot conclude whether the port is closed or filtered. (IP ID idle scan ONLY)

Scanning TCP

- General TCP knowledge
  - 3-way handshake
  - TCP flags
- Common scanning techniques:
  - Full/Open scan (Connect scan)
  - Stealth/half-open scan (SYN scan)
  - Xmas Tree Scan
  - FIN Scan
  - Null Scan
  - Idle Scanning
  - Ack Scanning

Scanning TCP

- General TCP knowledge
  - 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.

Scanning TCP

- General TCP knowledge
  - difference between FIN/RST

	FIN	RST
Connection Termination	Graceful	Abort
Termination Process	Two-way handshake (2x)	Unconditionally closes the connection
Typical Usage	Normal TCP connections	When errors or anomalies occur in the connections

Scanning TCP

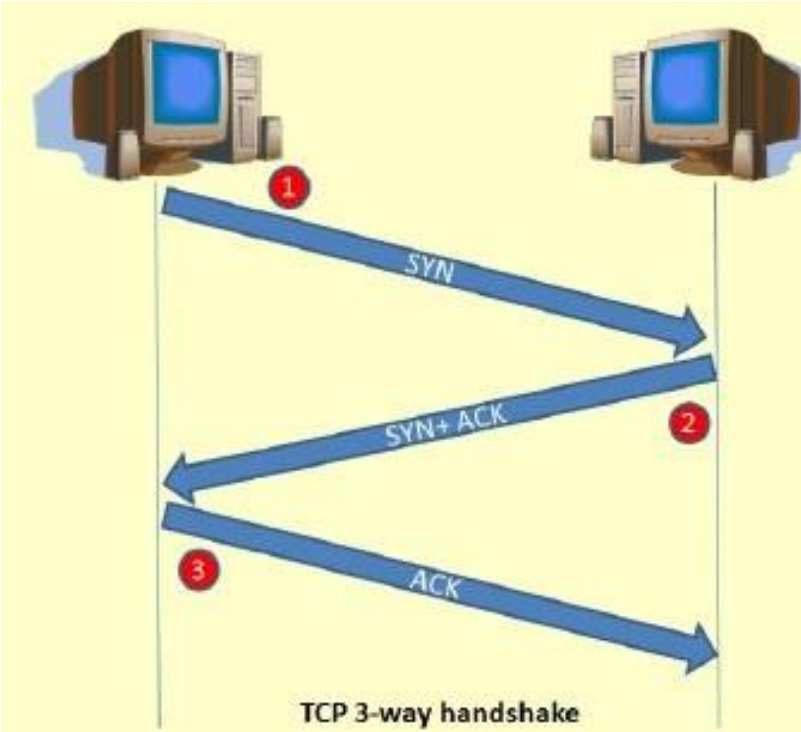
- General TCP knowledge
  - difference between PSH/URG

- PSH:
  - On layer4, client & server use buffers to store data.
  - This is OK, but not for “real-time” protocols. E.g. telnet= server would wait until buffer is full & typing commands could take forever.
  - When sender indicates PSH = 1, the segment is not buffered but forwarded immediatly to the application layer.

- URG:
  - Also needs “Urgent Pointer” (16 bit field) = points to the data in the segment that is urgent.
  - Data is immediatly delivered to application layer.
  - Data is delivered out of sequence.
  - Not often used by modern protocols.
  - Example: quick reset of connection without the need on the receiver’s side to handle all data.

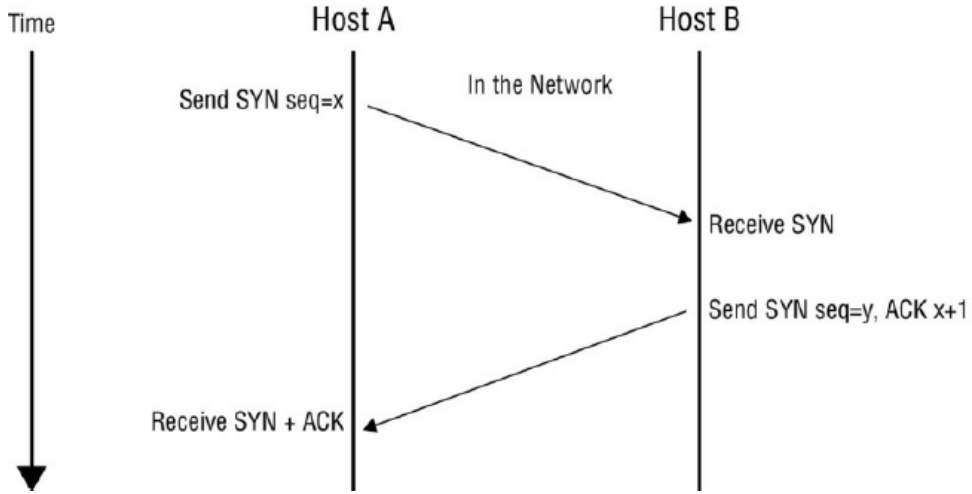
Scanning TCP

- Common scanning techniques:
  - Full/Open scan (Connect scan)
    - 3 way-handshake is completed
    - IDS detection + logging
    - Takes longer
    - Result:
      - Handshake completed = open port
      - RST received = closed port



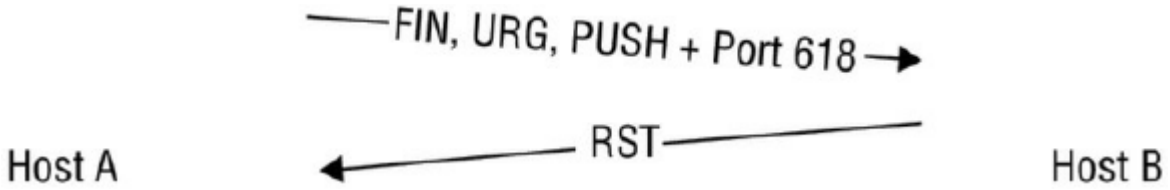
Scanning TCP

- Common scanning techniques:
  - Stealth/half-open scan (SYN scan)
    - TCP 3-way handshake
    - Only perform 1 & 2
    - Connection stays open
    - Connection gets removed after time = not logged
    - Ideal for "initial" scanning
    - Possible results = returned 2nd packet
      - SYN+ACK = open port
      - RST = closed port
      - None = filtered port



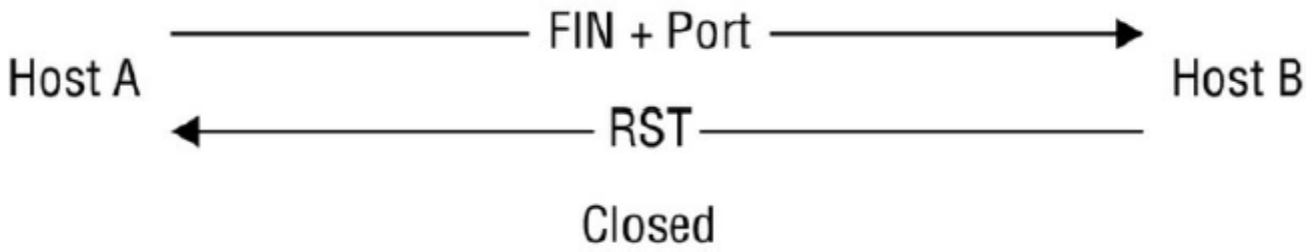
Scanning TCP

- Common scanning techniques:
  - Xmas Tree Scan
    - FIN, URG and PSH flag on
    - Impossible/illegal combination
    - Normally dropped, maybe response
    - Response can reveal OS information
    - Possible results:
      - RST = closed
      - No response = open (| filtered)



Scanning TCP

- Common scanning techniques:
  - FIN Scan
    - FIN flag on
    - Packet to close connection = often can pass through firewalls
    - Result:
      - Same as Xmas scan
      - RST = closed
      - None = open (| filtered)



Scanning TCP

- Common scanning techniques:
  - Null Scan
    - No Flags set
    - Result
      - RST = closed port
      - None = open port (| filtered)

Scanning TCP

- Common scanning techniques:
  - Idle Scanning
    - High stealthiness
    - Hides scanning/attacking party's identity
    - Bounces off zombie system

Scanning TCP

- Common scanning techniques:
  - Idle Scanning
- Principle:
  - One way to determine whether a TCP port is open is to send an SYN (session establishment) packet to the port. The target machine will respond with an SYN/ACK (session request acknowledgment) packet if the port is open, and an RST (reset) if the port is closed.
  - A machine that receives an unsolicited SYN/ACK packet will respond with an RST. An unsolicited RST will be ignored.
  - Every IP packet on the Internet has a fragment identification number (IP ID). Since many operating systems simply increment this number for each packet they send, probing for the IP ID can tell an attacker how many packets have been sent since the last probe.

Scanning TCP

IPv4 header format

Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Version				IHL				DSCP						ECN		Total Length															
4	32	Identification																Flags			Fragment Offset											
8	64	Time To Live								Protocol								Header Checksum															
12	96	Source IP Address																															
16	128	Destination IP Address																															
20	160	Options (if IHL > 5)																															
⋮	⋮																																
60	480																																

Scanning TCP

- Common scanning techniques:
  - Idle Scanning
    - Principle exploited, for each port to scan:
      - 1. Probe the zombie's IP ID and record it.
      - 2. Forge a SYN packet from the zombie and send it to the desired port on the target. Depending on the port state, the target's reaction may or may not cause the zombie's IP ID to be incremented.
      - 3. Probe the zombie's IP ID again. The target port state is then determined by comparing this new IP ID with the one recorded in step 1.

So the IP ID of the zombie defines the result:

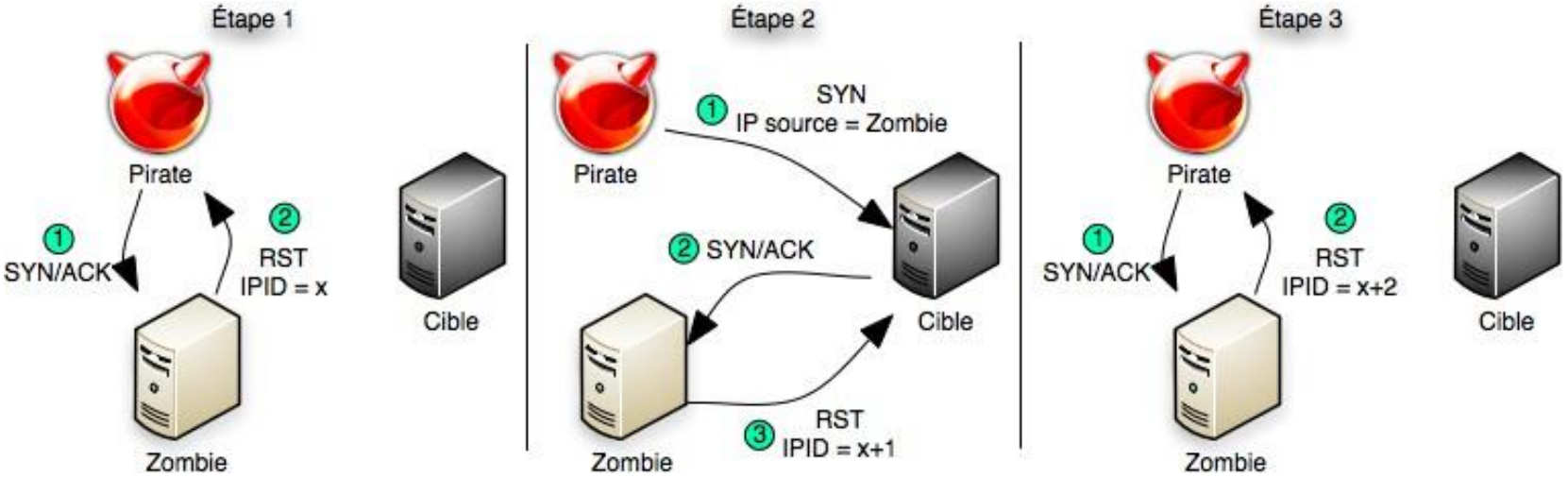
ID+1 = only reply was sent = closed port (or filtered)

ID+2 = zombie sent out a packet between probes = open port

ID+3 = zombie not usefull (non-predictable IP IDs or other communication going on…)

Scanning TCP

- Common scanning techniques:
  - Idle Scanning



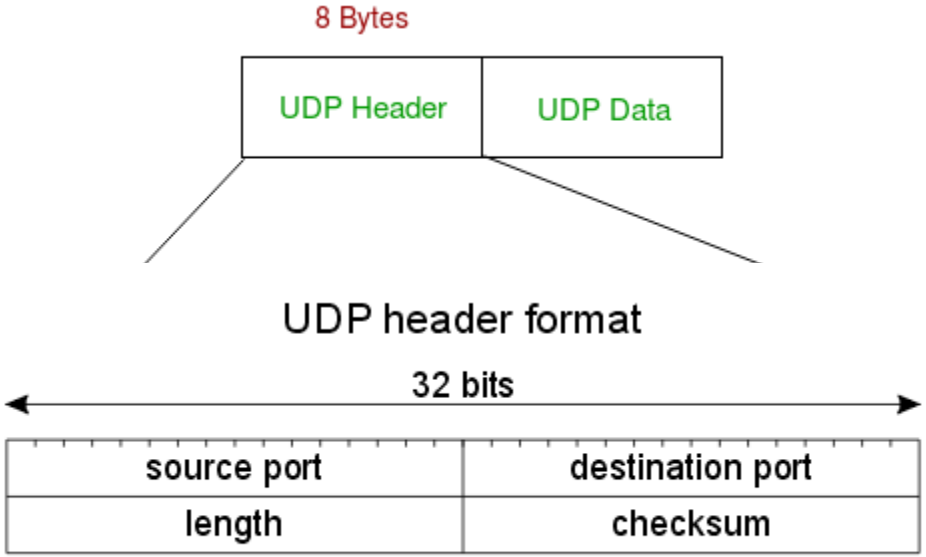
Zombie ... multifunctional printer

Scanning

- Common scanning techniques:
  - ACK Scanning
    - Used when port not definitely open/closed
    - Check for FW existence (Statefull = SPI)
    - How
      - Normally ACK can only follow SYN
      - Victim gets sent a segment with only ACK flag turned on (to destination port)
      - Answer = RST → unfiltered port (open or closed)
      - Otherwise (no response or ICMP error) → filtered port

Scanning UDP

- UDP Scanning
- Not connection-oriented
  - Client sends and doesn't expect answer
- No flags
- UDP header = 8 bytes (TCP = 20 bytes)



Scanning UDP

- UDP Scanning
  - Send UDP packet
  - Receive:
    - ICMP port-unreachable = port closed
    - ICMP error (type 3, codes 1,2,9,10 or 13) = port filtered
    - No response = port open (| filtered)

CyberSecurity Scanning

Fingerprinting

Karel de Grote Hogeschool

Scanning

- Fingerprinting
  - Identify the underlying OS from subtle packet differences
  - Active
  - Passive

	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.

Scanning

- Fingerprinting
  - Active

nmap -O <ip address>

- 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

Scanning

- Fingerprinting
  - Passive

- the inspection of the initial time to live (TTL) value in the header of a packet.
- Window size used in TCP packets during the SYN and SYN+ACK steps of the three-way handshake.

Operating System	Time To Live	TCP Window Size
Linux (Kernel 2.4 and 2.6)	64	5840
Google Linux	64	5720
FreeBSD	64	65535
Windows XP	128	65535
Windows Vista and 7 (Server 2008)	128	8192
iOS 12.4 (Cisco Routers)	255	4128

Scanning

- Extra's:
- Proxies
  - Tor
  - https://www.torproject.org/about/overview.html.en
- NMAP
  - See exercises

CyberSecurity Scanning Defense

Karel de Grote Hogeschool

Scanning

- **Defense:**
  - Disconnect
  - Install only “hardened” applications/OS- es
  - Update (automatic)
  - Security zones (DMZ)
  - Install IPS
  - Do own vulnerability check + correct where needed