Intruder Detection

BEHAVIOR & INTRUSION

Learning outcome checklist

- *LO1: Know different intruder types*
- *LO2: Analyse intruder behaviors*
- *LO3: Understand how TCP 3-way handshake normally happens*
- *LO4: See the deviation from TCP 3-way handshake / connection*

Further reading

1. LO2: Computer_Security_Principles_and_Practice_(3rd_Edition), William Stallings, section Intruder Behavior page 270-272
2. Stephen Northcutt, Judy Novak. Network Intrusion Detection, Third Edition. Sams Publishing 2002,
    1. Tcp sequence: Chapter 2,
    2. LO3: tcpdump and tcp – tcpdump output (page 33-42)
    3. LO4: chapter 3 (page 59)

Intruders

(menti)

- significant security issue for networked systems is hostile/unwanted trespass (by users or software) - from benign to serious
- user trespass – unauthorized logon, privilege abuse
- software trespass – virus, worm, or trojan horse
- classes of intruders– masquerader, misfeasor, clandestine user

Intruders

- **Masquerader**: An individual who is not authorized to use the computer and who penetrates a system's access controls to exploit a legitimate user's account
- **Misfeasor**: A legitimate user who accesses data, programs, or resources for which such access is not authorized, or who is authorized for such access but misuses his or her privileges
- **Clandestine** user: An individual who seizes supervisory control of the system and uses this control to evade auditing and access controls or to suppress audit collection

Masquerader is likely to be an outsider; the misfeasor generally is an insider; and the clandestine user can be either an outsider or an insider. (menti)

Cyber Criminals

- Individuals or members of an organized crime group with a goal of financial reward
- Their activities may include:
    - Identity theft
    - Theft of financial credentials
    - Corporate espionage
    - Data theft
    - Data ransoming
- Typically they are young, often Eastern European, or Russian (but they can be from anywhere), who do business on the Web

Cyber Criminals

- They meet in underground forums to trade tips and data and coordinate attacks.
- International laws are tricky, and IP address can be misleading
- act quickly and precisely to make their activities harder to detect
- exploit perimeter via vulnerable ports
- use trojan horses (hidden software) to leave back doors for re-entry
- use sniffers to capture passwords
- do not stick around until noticed
- make few or no mistakes.

IDSs and IPSs can also be used for these types of attackers, but may be less effective because of the quick in-and-out nature of the attack.

Insider Attacks

- among most difficult to detect and prevent
- employees have access & systems knowledge
- may be motivated by revenge / entitlement
  - when employment terminated
  - taking customer data when move to competitor
- IDS / IPS may help but also need other and more direct approaches:
  - enforcing least privilege, monitor logs, protect sensitive resources with strong authentication, on termination delete employee's computer and network access and make a mirror image of employee's hard drive before reissuing it

Insider Attacks (less ethical)

- create network accounts for themselves and their friends
- access accounts and applications they wouldn't normally use for their daily jobs
- e-mail former and prospective employers
- conduct furtive instant-messaging chats
- visit web sites that cater to disgruntled employees, such as f'dcompany.com ratemyboss
- perform large downloads and file copying
- access the network during off hours.

Hacktivists/Activists

- Are either individuals, usually working as insiders, or members of a larger group of outsider attackers, who are motivated by social or political causes
- Also know as hacktivists
- Aim of their attacks is often to promote and publicize their cause typically through:
  - Website defacement
  - Denial of service attacks
  - Theft and distribution of data that results in negative publicity or compromise of their targets

Terrorist/State-Sponsored - Advanced Persistent Threats (APTs)

(menti)

- Groups of hackers sponsored by governments to conduct espionage (Spying) or sabotage activities
- Also known as Advanced Persistent Threats (APTs) due to the covert nature and persistence over extended periods involved with any attacks in this class
- Sometimes if a state player finds a vulnerability, they won't report it to the company and instead use it to spy.

https://attack.mitre.org/groups/

Hacker Behaviour Patterns

1. Select the target using IP lookup tools such as NSLookup, Dig, and others.
2. Map network for accessible services using tools such as NMAP.
3. Identify potentially vulnerable services (in this case, pcAnywhere).
4. Brute force (guess) pcAnywhere password.
5. Install remote administration tool called DameWare.
6. Wait for administrator to log on and capture his password.
7. Use that password to access remainder of network.

Benign intruders might be tolerable, although they do consume resources and may slow performance for legitimate users.

Classes of Intruders – Others

Hackers with motivations other than those previously listed

- Include classic hackers or crackers who are motivated by technical challenge or by peer-group esteem and reputation
- Many of those responsible for discovering new categories of buffer overflow vulnerabilities could be regarded as members of this class
- Given the wide availability of attack toolkits, there is a pool of “hobby hackers” using them to explore system and network security

Low-level intruder (script-kiddies)

- Hackers with minimal technical skill who primarily use existing attack toolkits
- They likely comprise the largest number of attackers, including many criminal and activist attackers
- Given their use of existing known tools, these attackers are the easiest to defend against
- Also known as “script-kiddies” due to their use of existing scripts (tools)

Mid-level Intruder

Hackers with sufficient technical skills to modify and extend attack toolkits to use newly discovered, or purchased, vulnerabilities

They may be able to locate new vulnerabilities to exploit that are similar to some already known

Hackers with such skills are likely found in all intruder classes

Adapt tools for use by others

High-Level Intruder

Hackers with high-level technical skills capable of discovering brand new categories of vulnerabilities

Write new powerful attack toolkits

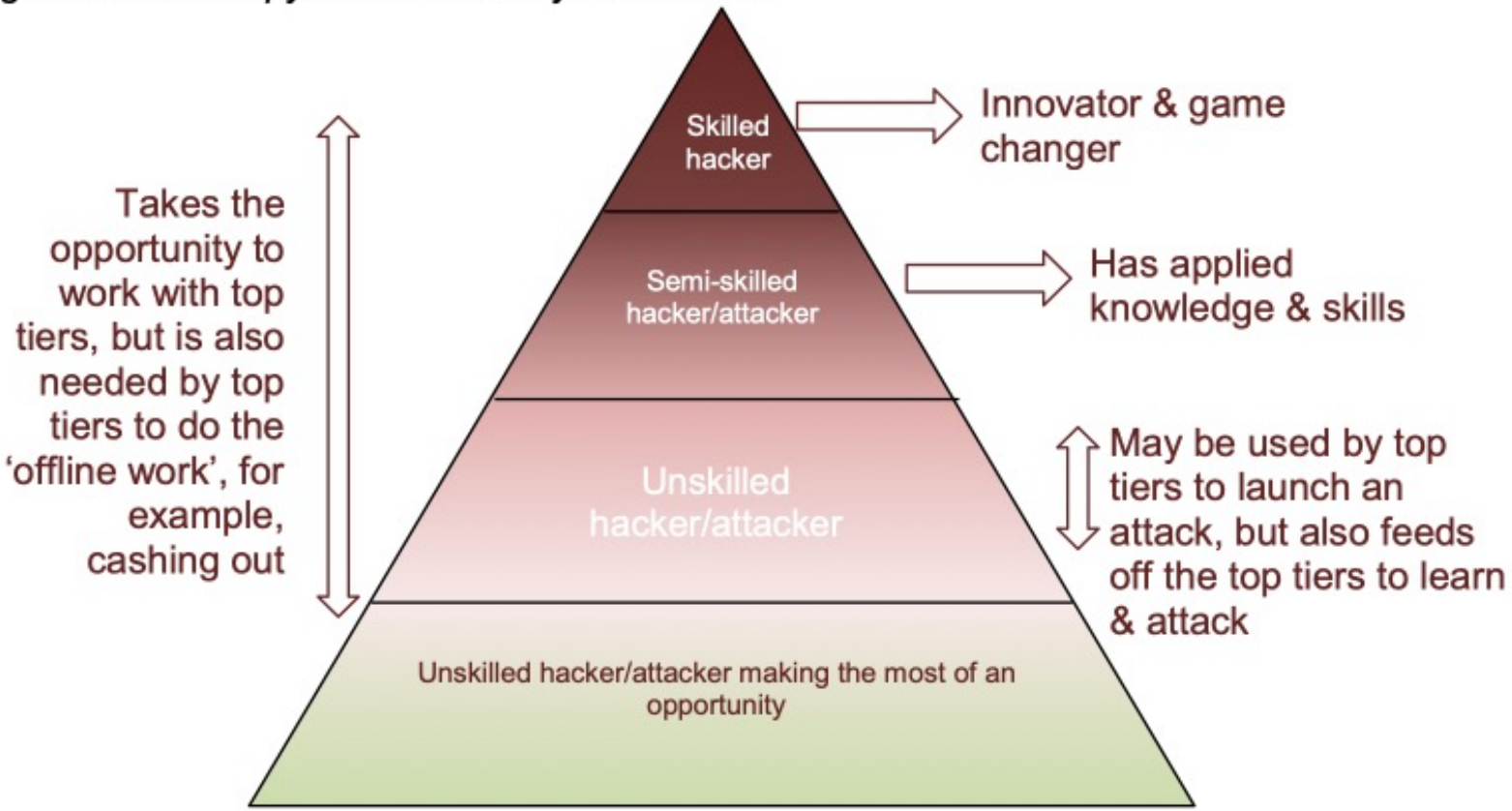
Some of the better known classical hackers are of this level

Some are employed by state-sponsored organizations

Defending against these attacks is of the highest difficulty

Categories by skill levels

Figure 1.7: Skills pyramid for the cyber attacker



Source: Holt (2013)

Figure: 2013-Cyber-crime-a-review-of-the-evidence-chapter-1-cyberdependent-crimes https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/246751/horr75-chap1.pdf

Examples of Intrusion

Remote root compromise

Web server defacement

Guessing/cracking passwords

Copying databases containing credit card numbers

Viewing sensitive data without authorization

Running a packet sniffer

Distributing pirated software

Using an unsecured modem to access internal network

Impersonating an executive to get information

Using an unattended workstation

Intruder Behavior

- The techniques and behavior patterns of intruders are constantly shifting, to exploit newly discovered weaknesses and to evade detection and countermeasures.
- However, intruders typically use following steps from a common attack methodology.



Ref: William, Stallings. *Computer security: Principles and practice*. Pearson Education India, 2008: section 8.1.

Intruder Behaviors

Information Gathering:

- Where the attacker identifies characteristics of the target systems using,
  - publicly available information, both technical and non-technical
  - Use network exploration tools to map target resources.

Initial Access:

- The initial access to a target system, typically
  - by exploiting a remote network vulnerability,
  - by guessing weak authentication credentials used in a remote service
  - via the installation of malware on the system using some form of social engineering
  - drive-by-download attack.

Intruder Behaviour: Public Info

Information gathering or a *reconnaissance attack* gain as much information about the network as possible before launching other more serious types of attacks. Quite often, the reconnaissance attack is implemented by using publicly available information.

- Employee names and e-mail addresses provide a good start
- Large companies usually have their phone numbers assigned in blocks from the local telephone company
- Internet Protocol (IP) address info is publicly available via the ARIN and many other Internet registering authorities. From www.arin.net, anyone can begin a search using a single known IP address.
- Attacker can perform electronic reconnaissance to find what systems and resources are on a network

Scanning the network

- Scanning the network is typically done using a *ping sweep* utility that pings a range of IP addresses
  - what hosts are currently live on the network?
  - The ping sweep identifies viable targets on the network
- Once the IP address of viable hosts is known, the attacker can then begin to probe those hosts to gather additional information, such as the OS or applications running on those hosts.
  - The more ports that are open, the more potential for someone to exploit the services running on the host computer.

IDS can look for both the ping sweeps and the probes for more data

Start small, then go big

MAT HONAN GEAR 08.06.12 08:01 PM

HOW APPLE AND AMAZON SECURITY FLAWS LED TO MY EPIC HACKING



https://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/

Intruder Behaviors

Privilege Escalation:

- Actions taken on the system, to increase privilege level of initial access. May be from normal user level to admin/root level privileges.

System Exploit:

- Actions by the attacker to access or modify information or resources on the system, or to navigate to another target system.

Maintaining Access:

- Actions such as
  - The installation of backdoors or other malicious software
  - through the addition of covert authentication credentials or other configuration changes to the system
- to enable continued access by the attacker after the initial attack.

Covering Tracks:

- Where the attacker disables or edits audit logs to remove evidence of attack activity, and uses rootkits and other measures to hide covertly installed files or code

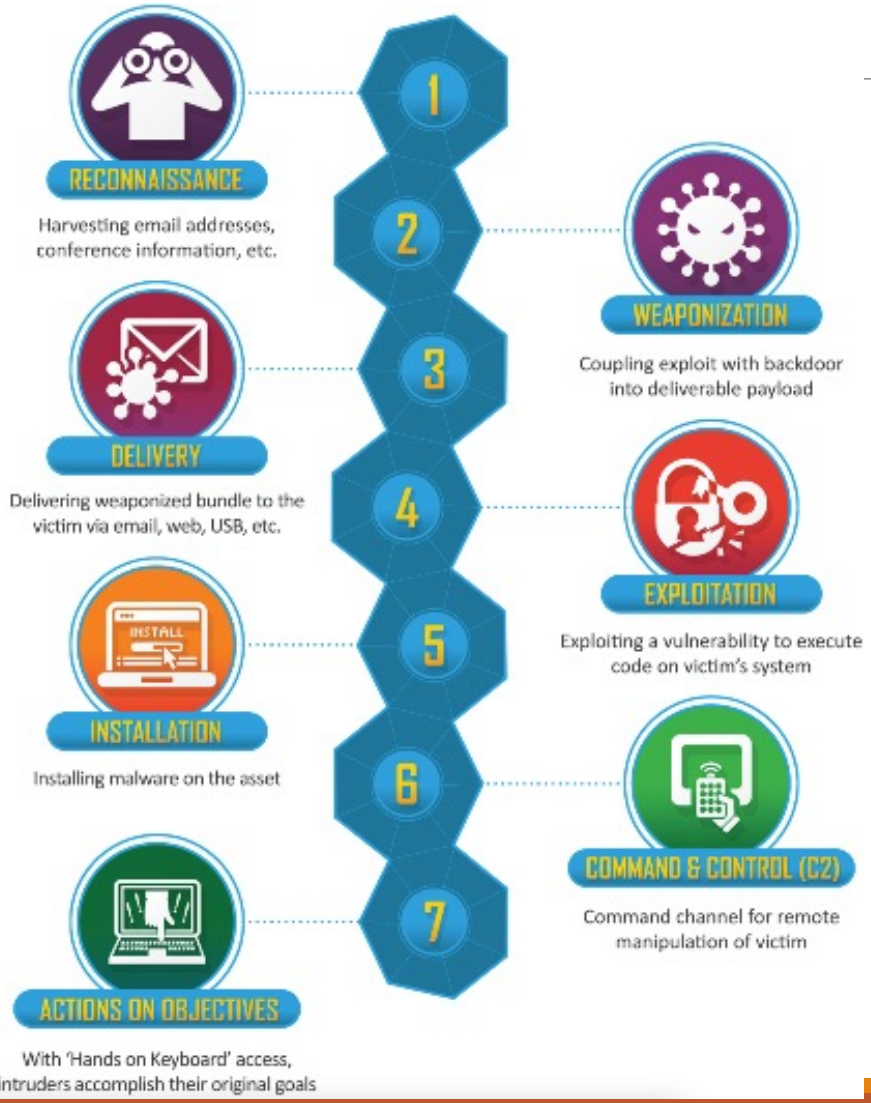
Analyse intruder behaviour

Menti

An intruder conducts the following attack. Re-arrange the steps of the intruder in a suitable order and name each step using the mentioned terminology (information gathering,…)

a. Transfer large number of documents to external repository
b. Identify vulnerable Web CMS
c. Install remote administration tool with backdoor for later access
d. Use rootkit to hide files installed on system
e. Install sniffer to capture administrator passwords
f. Exploit vulnerability in Web CMS plugin to gain system access

Cyber Kill Chain



Developed to aid security professionals in identifying the steps adversaries will follow

Based upon techniques/concepts of military kill chains

Source: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Apply cyber kill chain (1)

Menti

You are working in CERT team in company A. Your team receives two alerts:

a) an event produced from a Network Intrusion Detection System (NIDS)
b) an event from a Host Intrusion Prevention System (HIPS)

Which would you prioritize to deal first and why?

Apply cyber kill chain (2)

(Menti)The below graph showing each stage of the process on one axis and the countermeasure along the other can then identify the tool in place to perform the mitigation at that stage in the box where each intersects. An empty box indicates gaps where investments can be made to further enhance the organization's protections.

Which would you prioritize to invest between Audit log and Email queuing and why?



Detect	Deny	Disrupt	Degrade	Deceive
Web analytics	Firewall ACL			
NIDS	NIPS			
Vigilant User	Proxy filter	Inline AV	Email Queuing	
HIDS	Vendor Patch	EMET, DEP		
HIDS		AV		
NIDS	Firewall ACL	NIPS	Tarpit	DNS redirect
Audit log			Quality of Service throttle	Honeypot

Cyber Kill Chain Solution Cyber Threat Model © 2011 Lockheed Martin. All Rights Reserved.

(menti) Hadnagy was once hired as an SE auditor to attempt to access the servers of a printing company whose processes and vendors were proprietary and of interest to competi- tors. The CEO told Hadnagy that hacking him would be next to impossible because he “guarded his secrets with his life.”

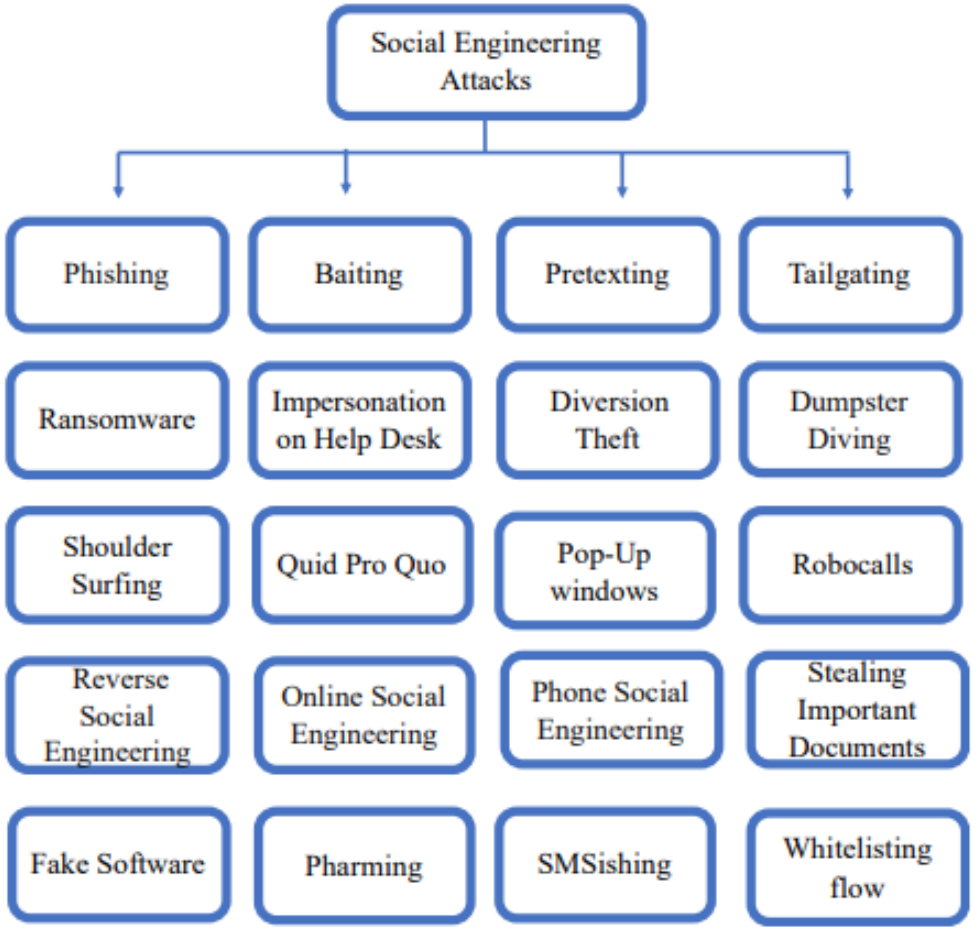
After some information gathering, Hadnagy found the locations of servers, IP addresses, email addresses, phone numbers, physical addresses, mail servers, employee names and titles and much more. Through Facebook, he was also able to get other personal details about the CEO, such as his favorite restaurant and sports team.But the real prize came when Hadnagy learned the CEO was involved in cancer fundraising, due to a family member’s succesfull battle with cancer.

Armed with the information, he was ready to strike. He called the CEO and posed as a fundraiser from a cancer charity the CEO had dealt with in the past. He informed him they were offering a prize drawing in exchange for donations—and the prizes included tickets to a game played by his favorite sports team, as well as gift certificates to several restaurants, including his favorite spot.

The CEO bit, and agreed to let Hadnagy send him a PDF with more information on the fund drive. He even managed to get the CEO to tell him which version of Adobe reader he was running. Soon after he sent the PDF, the CEO opened it, installing a shell that allowed Hadnagy to access his machine.

Social Engineering

More than one company with elaborate authentication processes, firewalls, virtual private networks (VPNs), and network monitoring software has been left wide open to an attack by an employee unwittingly giving away key information in an e-mail or by answering questions over the phone with someone they don't know.



Source: Salahdine, Fatima, and Naima Kaabouch. "Social engineering attacks: A survey." *Future Internet* 11.4 (2019): 89.

Example

You find a loose thumb drive, in your own parking lot, with your own organization's logo on it, you pick it up and insert it *because you are trying to help.* For good reason. Suppose that the CEO dropped it and it has vital business information in there?

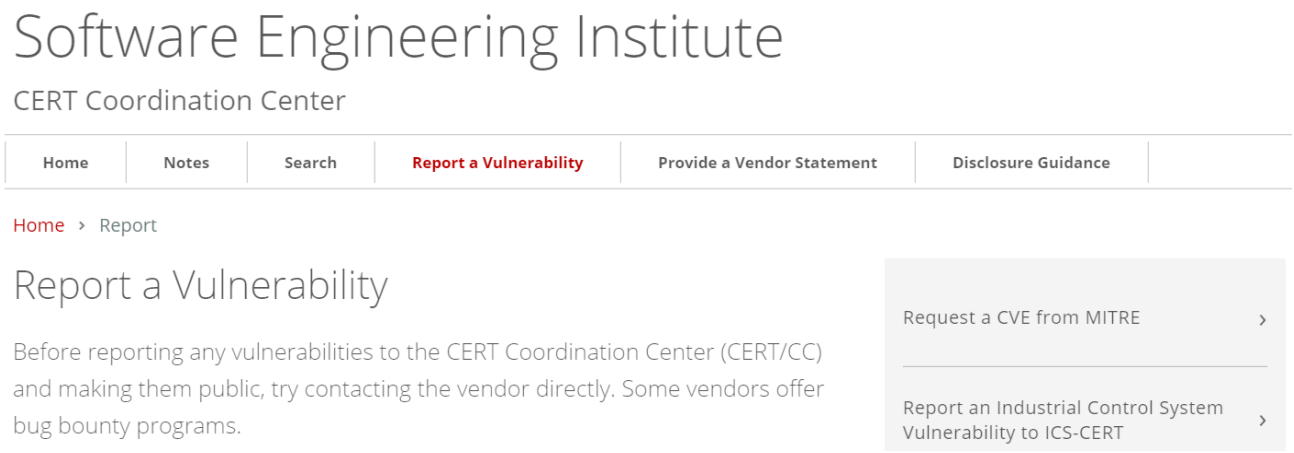
Exercise

(menti)

Between 2013 and 2015, Evaldas Rimasauskas impersonated a Taiwanese hardware supplier, Quanta Computer, whose services were used by two tech giants, Google and Facebook. He sent out fake invoices worth $122 million ($99 million and $23 million to Google and Facebook, respectively) to these companies for almost three years until he was arrested and prisoned for 30 years.

Intruder Response

- One of the results of the growing awareness of the intruder problem has been the establishment of a number of computer emergency response teams (CERTs).
- Cooperative ventures collect information about system vulnerabilities and disseminate it to systems managers. However, hackers also routinely read CERT reports.



Hackers Profiling Project

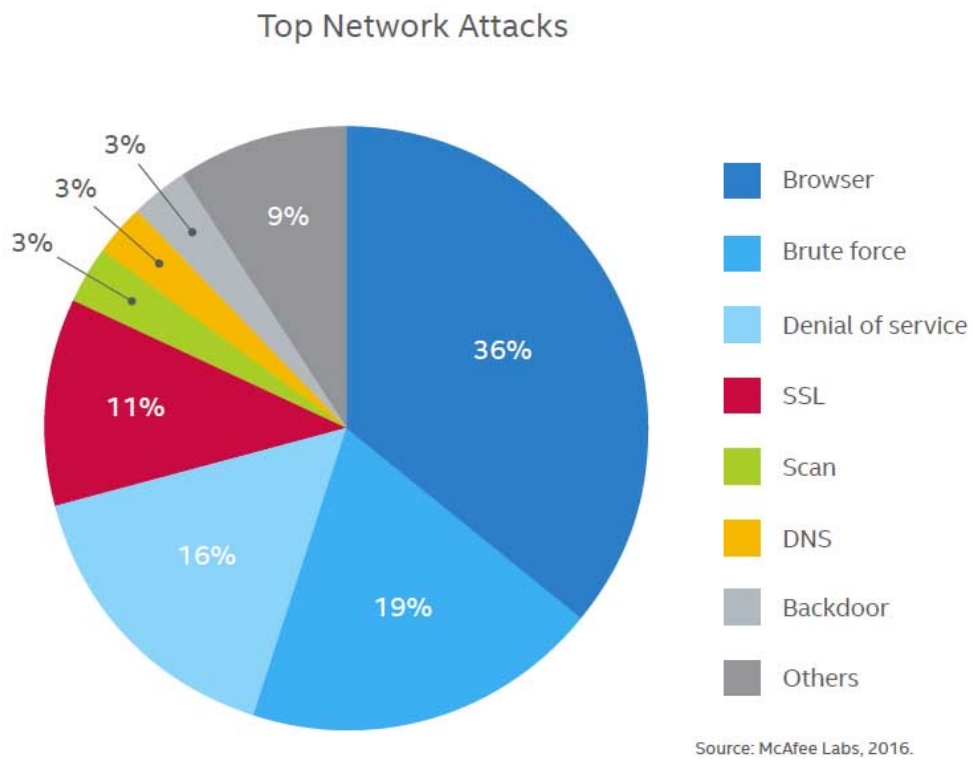


https://www.ted.com/talks/misha_glenny_hire_the_hackers?language=en#t-351721

TCP/IP Basics

LECTURE 2 – CNET349SL

Network Attack Types (2016)



Overview

- TCP (Transmission Control Protocol) Stream Reassembly
- IP Fragmentation
- ICMP Review
- UDP
- Protocol “benders”
- DNS Review

Internet Protocols

ADDRESSES – TCP BASICS

Addresses

Domain Name System

- Domain names, such as http://nsbm.lk/
- TCP/UDP
- Use port numbers

Internet Protocol

- Uses IP Addresses for communication, hop to hop delivery
- IP Address translation via DNS or host tables
- Unreliable protocol

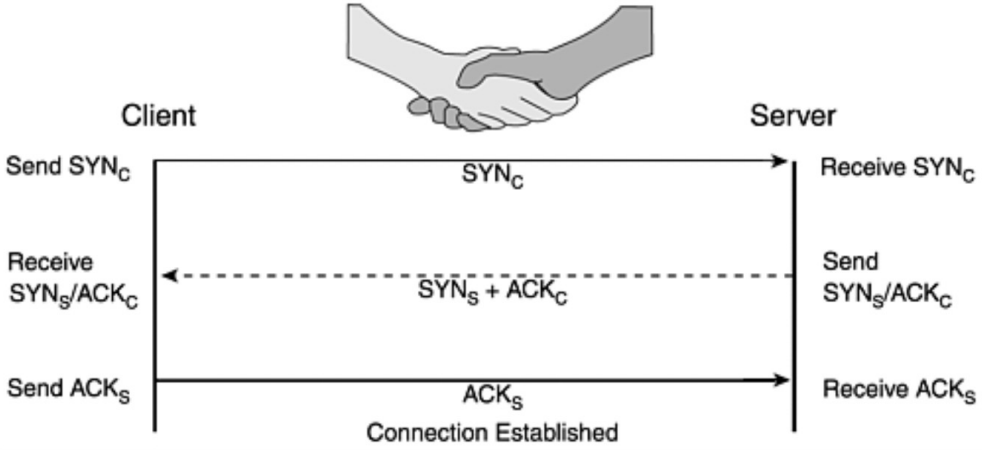
Address Resolution Protocol (ARP)

- In IPv4, ARP identifies the MAC address of a host, given its IP Address.
- Internet Protocol version 6 (IPv6) is the most recent version
- ARP is not a routable protocol

Establishing a TCP connection – 3-way handshake protocol

3-way handshake

- Tel_client requests a TCP connection with a SYN
- Myhost server responds with a SYN/ACK
- Tel-client responds with an ACK



Source: Northcutt, S., & Novak, J. (2002). *Network intrusion detection*. Sams Publishing, page 37

TCP Sequence and Acknowledgement Numbers

TCP Sequence Numbers

- 32-bit numbers used to order multiple segments
- Each segment identified by a beginning sequence number

TCP Acknowledgment Numbers

- 32 bit numbers used to acknowledge receipt of sent data
- Represents the next TCP sequence number expected from sender

Example 1

tel_client.com.38060 >myhost.com.telnet: **S** 3774957990:3774957990(0) win 8760 <mss 1460> (DF)

myhost.com.telnet >tel_client.com.38060: **S** 2009600000:2009600000(0) **ack** 3774957991 win 1024 <mss 1460>

tel_client.com.38060 >myhost.com.telnet: 3774957991:3774957991(0) **ack** 2009600001 win 8760 <mss 1460> (DF)

S: SYN flag; Ack: ACK flag; DF: do not fragment flag

Win means window size, window size of 8760 says that the client has an 8760-byte buffer for aggregated incoming data to this connection.

Mss means maximum segment size that it advertises to the server, mss informs the destination host that the physical network on which tel_client.com resides should not receive more than 1460 bytes of TCP payload (20- byte IP header + 20-byte TCP header + 1460-byte payload = 1500 bytes, which is the maximum transmission unit, or MTU, for Ethernet) at a time.

menti

Example 2

What are the values of A, B, C? menti

tel_client.com.38060 > myhost.com.telnet: **S** 3774957992:3774957992(0) win 8760 <mss 1460> (DF)

myhost.com.telnet > tel_client.com.38060: **S** 2009600010:2009600010(0) **ack** A win 1024 <mss 1460>

tel_client.com.38060 > myhost.com.telnet: B:B(0) **ack** C win 8760 <mss 1460> (DF)

Terminating a TCP Session

Client terminates with a FIN, server does an ACK

07:15:54.796413 sendit.net.39905 > mailserver.com.
25: F 14:14(0) ack 186 win 8760 (DF)

07:15:54.797241 mailserver.com.25 > sendit.net.
39905: . Ack 15 win 8760 (DF)

Server terminates with a FIN, client does an ACK

07:15:54.798865 mailserver.com.25 > sendit.net.

399905: F 186:186(0) ack 15 win 8760 (DF)

07:15:54.798896 sendit.net.39905 > mailserver.com.
25: . Ack 187 win 8760 (DF)

Exercise

07:15:54.796413 sendit.net.39905 > mailserver.com.25: F 20:20(0) ack 186 win 8760 (DF)

07:15:54.797241 mailserver.com.25 > sendit.net.39905: . A B win 8760 (DF)

07:15:54.798865 mailserver.com.25 > sendit.net.399905: F 190:190(0) ack C win 8760 (DF)

07:15:54.798896 sendit.net.39905 > mailserver.com.25: . D E win 8760 (DF)

What are the values of A, B, C, D, E?

TCP Delivery failures

How does the receiver inform the sender that data has not been received?

- Lost or delayed TCP segment from the middle of a stream
  - Duplicate acknowledgment numbers
  - No acknowlegment by receiver
    - Retransmission timeout by sender

Example – Delivery failure

10.10.10.100.ftp >10.10.10.101.1054: P 1:81(80) ack 1 win 32120

10.10.10.101.1054 >10.10.10.100.ftp: . ack 81 win 8680 (DF)

10.10.10.100.ftp > 10.10.10.101.1054: P 81:116(35) ack 1 win 32120 (DF) [tos 0x10]

10.10.10.100.ftp >10.10.10.101.1054: P 116:144(28) ack 1 win 32120 (DF) [tos 0x10]

10.10.10.101.1054 > 10.10.10.100.ftp: . ack 81 win 8680 (DF)

10.10.10.100.ftp >10.10.10.101.1054: P 144:173(29) ack 47 win 32120 (DF) [tos 0x10]

10.10.10.101.1054 > 10.10.10.100.ftp: . ack 81 win 8680 (DF)

10.10.10.100.ftp > 10.10.10.101.1054: P 81:116(35) ack 1 win 32120 (DF) [tos 0x10]

Example - Retransmission Timer

17:14:18:726864 1.1.1.1.62555 > 192.168.44.63.3128: S 20583734:20583734(0) win 8192 <mss 1380> (DF)

17:14:21.781140 1.1.1.1.62555 > 192.168.44.63.3128: S 20583734:20583734(0) win 8192 <mss 1380> (DF)

17:14:27:776662 1.1.1.1.62555 > 192.168.44.63.3128: S 20583734:20583734(0) win 8192 <mss 1380> (DF)

17:14:39:775929 1.1.1.1.62555 > 192.168.44.63.3128: S 20583734:20583734(0) win 8192 <mss 1380> (DF)

Damage assessment

Repeated SYN attempts to a system without a reply – jimmying a door without successful entry

Completion of three-way handshake – entry

Server port number – the intruder's interest

The number of bytes exchanged – determining what kind of haul the intruder made off with

TCP Reassembly issues

- The IDS/IPS must properly examine and interpret TCP Sessions
  - Must look for the 3-way handshake that starts session
  - Must terminate sessions when end hosts do
  - Must reassemble TCP segments exactly as end hosts do
- It must reassemble TCP segments exactly as end hosts do
  - Overlapping segments
  - TCP Sequence Number wrapping
  - Data on SYN
  - Multiple TCP SYNs in the same session
  - Unexpected TCP flags
  - Session timeout

Normal TCP stimulus response

What happens when we attempt a telnet connection to the following:

- A destination host listening on the telnet port
- A destination host not listening on the telnet port
- A destination host that doesn't exist
- A destination host whose telnet connection is blocked by a router that responds with an ICMP error message
- A destination host whose telnet connection is blocked by a router that doesn't respond

Stephen Northcutt, Network Intrusion Detection, chapter 5, TCP stimulus-response, page 86

Normal TCP stimulus response

Listening telnet server

Client requests a TCP connection with a SYN

Server responds with a SYN/ACK

Stimulus

tel_client.com.38060 > myhost.com.telnet: **S** 3774957990:3774957990(0) win 8760 <mss 1460> (DF)

Response

myhost.com.telnet > tel_client.com.38060: **S** 2009600000:2009600000(0) **ack** 3774957991 win 1024 <mss 1460>

Normal TCP stimulus response

Non-listening telnet server

- Client requests a TCP connection with a SYN
- Server responds with a RESET/ACK

Stimulus

tel_client.com.38060 > myhost.com.telnet: **S** 3774957990:3774957990(0) win 8760 <mss 1460> (DF)

Response

myhost.com.telnet > tel_client.com.38060: R 0:0(0) ack 3774957991 win 0

Normal TCP stimulus response

Destination host doesn't exist

Client requests a TCP connection with a SYN

Router from the subnet where the destination host was formerly found responds with "ICMP Host Unreachable" error

Stimulus

tel_client.com.38060 > myhost.com.telnet: **S** 3774957990:3774957990(0) win 8760 <mss 1460> (DF)

Response

router.com > tel_client.com: icmp: host myhost.com unreachable

Normal TCP stimulus response

Telnet blocked by router

Client requests a TCP connection with a SYN

Router from the subnet where the destination host was formerly found responds with ICMP unreachable error –admin prohibited filter (meaning that the access was blocked)

Stimulus

tel_client.com.38060 > myhost.com.telnet: **S** 3774957990:3774957990(0) win 8760 <mss 1460> (DF)

Response

router.com > tel_client.com: icmp:myhost.com unreachable - admin prohibited filter

Normal TCP stimulus response

Telnet blocked, router silenced

Client requests a TCP connection with a SYN

Router does not respond to blocked telnet request, so client keeps retrying x times

Stimulus

tel_client.com.38060 > myhost.com.telnet: **S** 3774957990:3774957990(0) win 8760 <mss 1460> (DF)

Continuous Stimuli - No Response

tel_client.com.38060 > myhost.com.telnet: S 3774957990:3774957990(0) win 8760 <mss 1460> (DF)
tel_client.com.38060 > myhost.com.telnet: S 3774957990:3774957990(0) win 8760 <mss 1460> (DF)
tel_client.com.38060 > myhost.com.telnet: S 3774957990:3774957990(0) win 8760 <mss 1460> (DF)

Break

PART 3 – IP FRAGMENTATION

Fragmentation

- Occurs when maximum transmission unit (MTU) is smaller than the datagram
- Reassembled by destination host
- Should be scrutinised carefully, as it can be used to bypass detection
- Reassembly by the receiving host
- All fragments
  - Share the same **IP identification number**
  - Must specify what **offset** in original datagram
  - Must specify **length** of data payload
  - Must specify if **more fragments** follow

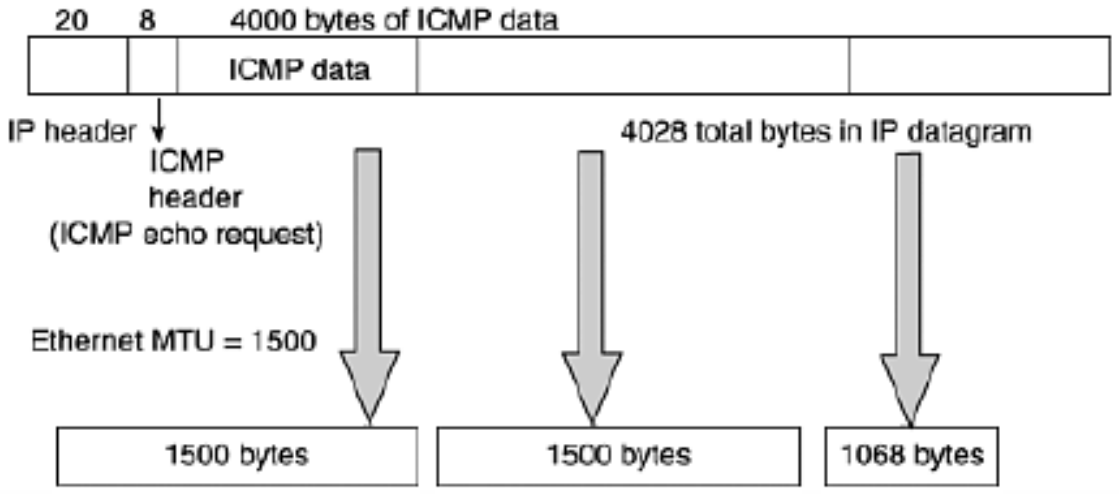
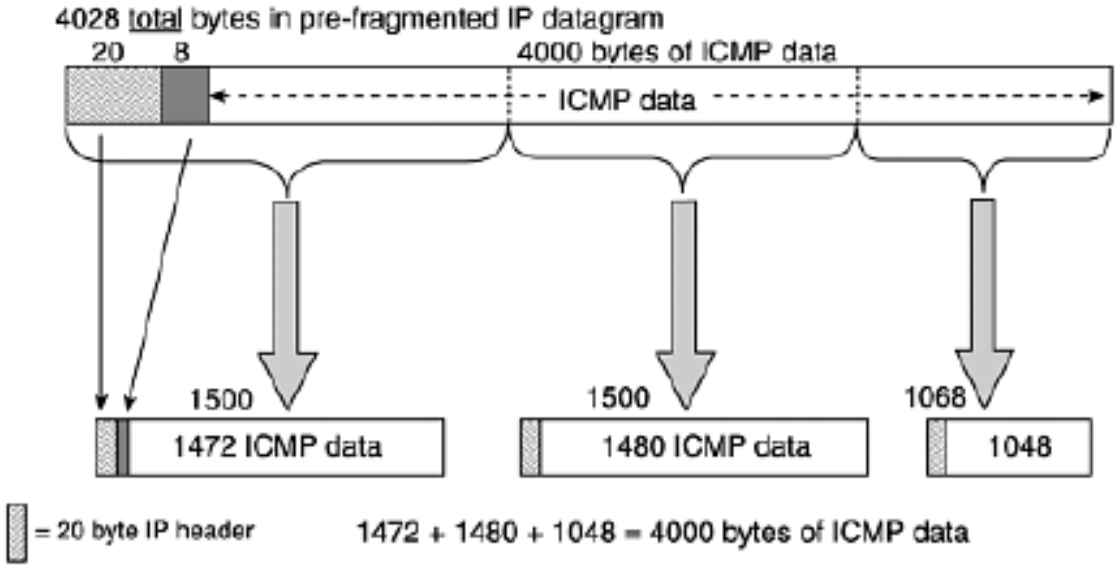


Figure 3.3. Byte allocations per fragment.



Source: Figure 3.4, Network intrusion detection, Stephen Northcutt, page 51, chapter 3

Fragmentation

- All fragments
  - Share the same IP identification number
  - Must specify what offset in original datagram
  - Must specify length of data payload
  - Must specify if more fragments follow

```
ping.com > myhost.com: icmp: echo request
(frag 21223:1480@0+)
ping.com > myhost.com: (frag
21223:1480@1480+)
ping.com > myhost.com: (frag A:1480@B)

menti
```

Fragment ID

The fragment ID is taken from the IP identification (IP ID) field

IP ID increases by 1 each new datagram is sent

Some newer TCP/IP stacks randomise this value

Important Notes

Only first fragment carries protocol header

If packet filter is not stateful, it can block first fragment only and subsequent fragments may be allowed in

When DF flag is set, packet will not be fragmented. This could be used to discover network MTU

Teardrop attack

```
evilfrag.com.139 > target.net.139: udp 28
(frag 242:36@0+)
evilfrag.com > target.net: (frag 242:4@24)
```

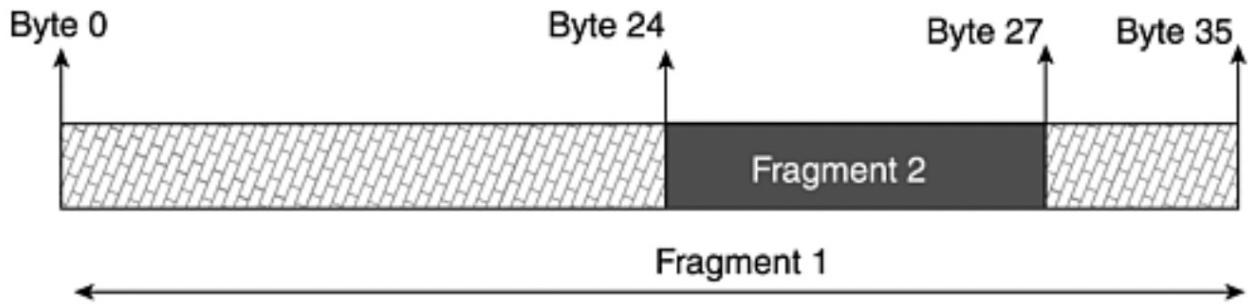
Explanation: Evilfrag.com.139 > target.net.139: udp 28 (fragment id 242, offset 0, flags[+], length:36) Evilfrag.com > target.net: (fragment id 242, offset 24, flags[none], length 4)

What is wrong with these fragments?

Teardrop attack

Evilfrag.com.139 > target.net.139: udp 28 (id 242, offset 0, flags[+], length:36)
Evilfrag.com > target.net: (id 242, offset 24, flags[none], length 4)

Figure 3.10. Teardrop fragment mutation.



Fragments with overlapping offset fields
Some systems will crash, hang, or reboot.

IDS/IPS and Fragmentation

IDS/IPS must reassemble fragments like destination host does

What about overlapping fragments?

Fragment time-out differences?

TCP Lab

READING TCP

Example: Normal TCP session

192.168.1.104.13223 > 192.168.1.102.1025: S 1000:1000(0) win 5480 <mss 1460>

192.168.1.102.1025 > 192.168.1.104.13223: S 1906728845:1906728845(0) ack 1001 win 64240 <mss 1460>

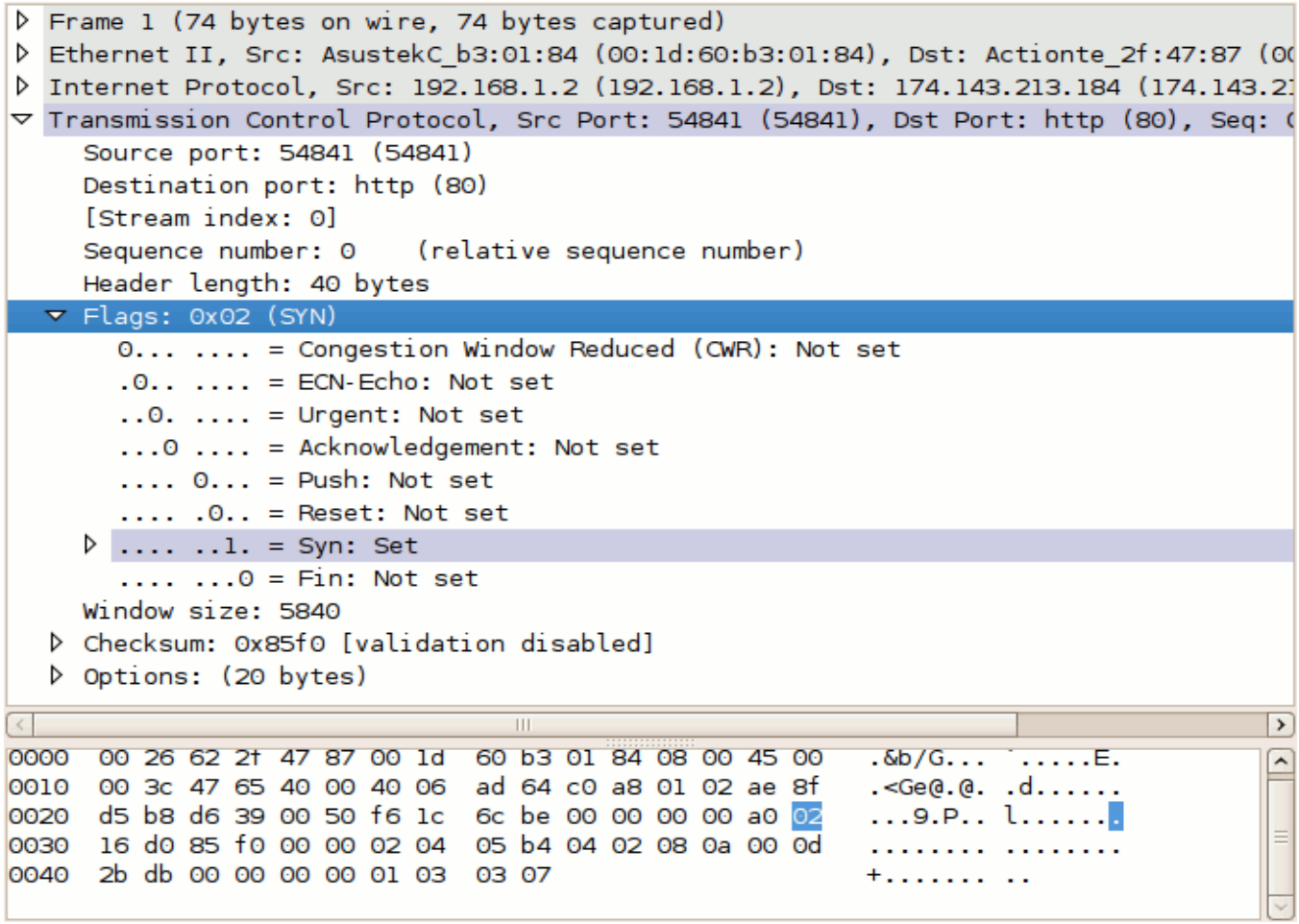
192.168.1.104.13223 > 192.168.1.102.1025: . ack 1906728846 win 5480

192.168.1.104.13223 > 192.168.1.102.1025: P 1001:1012(11) ack 1906728846 win 5480

192.168.1.102.1025 > 192.168.1.104.13223: . ack 1012 win 64229

192.168.1.104.13223 > 192.168.1.102.1025: R 1012:1012(0) win 5480

Look at wireshark



Exercise 1

- What is **unexpected** about the order that the client sends the TCP segments?
- Did the destination host accept the payloads that the client host sent?
- How do you know?

Exercise 1

192.168.1.104.343 > 192.168.1.102.1025: S 1000:1000(0) win 5480 <mss 1460>

192.168.1.102.1025 > 192.168.1.104.343: S 730837648: 730837648 (0) ack 1001 win 64240 <mss 1460>

192.168.1.104.343 > 192.168.1.102.1025: . ack 730837649 win 5480

192.168.1.104.343 > 192.168.1.102.1025: P 1012:1017(5) ack 730837649 win 5480

192.168.1.102.1025 > 192.168.1.104.343: . ack 1001 win 64240

192.168.1.104.343 > 192.168.1.102.1025: P 1001:1012(11) ack 730837649 win 5480

192.168.1.102.1025 > 192.168.1.104.343: . ack 1017 win 64224

Exercise 2

- What is **unexpected** about the data that the client sends to the server? Does the server accept the data?

  How do you know?

Exercise 2

192.168.1.104.36953 >192.168.1.102.1025: S 1000:1004(4) win 5480 <mss 1460>

192.168.1.102.1025 >192.168.1.104.36953: S 3153601991: 3153601991 (0) ack 1001 win 64240 <mss 1460>

192.168.1.104.36953 >192.168.1.102.1025: . ack 3153601992 win 5480

192.168.1.104.36953 >192.168.1.102.1025: P 1004:1015(11) ack 3153601992 win 5480

192.168.1.102.1025 >192.168.1.104.36953: . ack 1001 win 64240

192.168.1.104.36953 >192.168.1.102.1025: R 1015:1015(0) win 5480

192.168.1.102.1025 >192.168.1.104.36953: . ack 1001 win 64240

Exercise 3

- What is **wrong** with a particular TCP segment that the client sends to the server?
- How did the server react?
- Does the server accept the data that the client sent?

Exercise 3

192.168.1.104.29623 >192.168.1.102.1025: S 1000:1000(0) win 5480 <mss 1460>

192.168.1.102.1025 >192.168.1.104.29623: S 3772001185: 3772001185 (0) ack 1001 win 64240 <mss 1460>

192.168.1.104.29623 >192.168.1.102.1025: . ack 3772001186 win 5480

192.168.1.104.9999 >192.168.1.102.1025: P 1001:1012(11) ack 3772001186 win 5480

192.168.1.102.1025 >192.168.1.104.9999: R 3772001186:3772001186(0) win 0

192.168.1.104.29623 >192.168.1.102.1025: R 1012:1012(0) win 5480

Exercise 4

- What is wrong with a particular TCP segment that the client sends to the server?
- Did the server accept that payload that the client sent?
- How do you know?

Exercise 4

192.168.1.104.26509 >192.168.1.102.1025: S 1000:1000(0) win 5480 <mss 1460>

192.168.1.102.1025 >192.168.1.104.26509: S 2308158009: 2308158009(0) ack 1001 win 64240 <mss 1460>

192.168.1.104.26509 >192.168.1.102.1025: . ack 2308158010 win 5480

192.168.1.104.26509 >192.168.1.102.1025: P 1001:1012(11) ack 55555win 5480

192.168.1.102.1025 >192.168.1.104.26509: . ack 1001 win 64240

192.168.1.104.26509 >192.168.1.102.1025: R 1012:1012(0) win 5480

Exercise 5

- What is wrong with a particular TCP segment that the client sends to the server?
- Did the server accept that payload that the client sent?
- How do you know?

Exercise 5

192.168.1.104.10424 >192.168.1.102.1025: S 1000:1000(0) win 5480 <mss 1460>

192.168.1.102.1025 >192.168.1.104.10424: S 826905806: 826905806 (0) ack 1001 win 64240 <mss 1460>

192.168.1.104.10424 > 192.168.1.102.1025: . ack 826905807 win 5480

192.168.1.104.10424 > 192.168.1.102.1025: P 1001:1012(11) win 5480

192.168.1.104.10424 >192.168.1.102.1025: R 1012:1012(0) win 5480

192.168.1.102.1025 >192.168.1.104.10424: . ack 1001 win 64240