CPR E 431

BASICS OF INFORMATION SYSTEM SECURITY

Firewall and Intrusion Prevention System

Packet Filtering Firewall

Video Summary

- Issues with Packet Filtering Firewalls
- Allow/Deny Default Policies
- TCP/Webserver Communications
- Example Network

Issues with Packet Filtering Firewalls

Advantages

- Simplicity
- Transparent to users
- Very fast

Disadvantages

- Cannot prevent attacks that employ application specific vulnerabilities or functions (If the attack is based on the content will not be detected)
- Limited logging functionality
- Do not support advanced user authentication (manually configuring IPs)
- Vulnerable to attacks on TCP/IP protocol bugs
- Improper configuration can lead to breaches

Allow/Deny Default Policies

Explain the differences between Allow/Deny default policies!

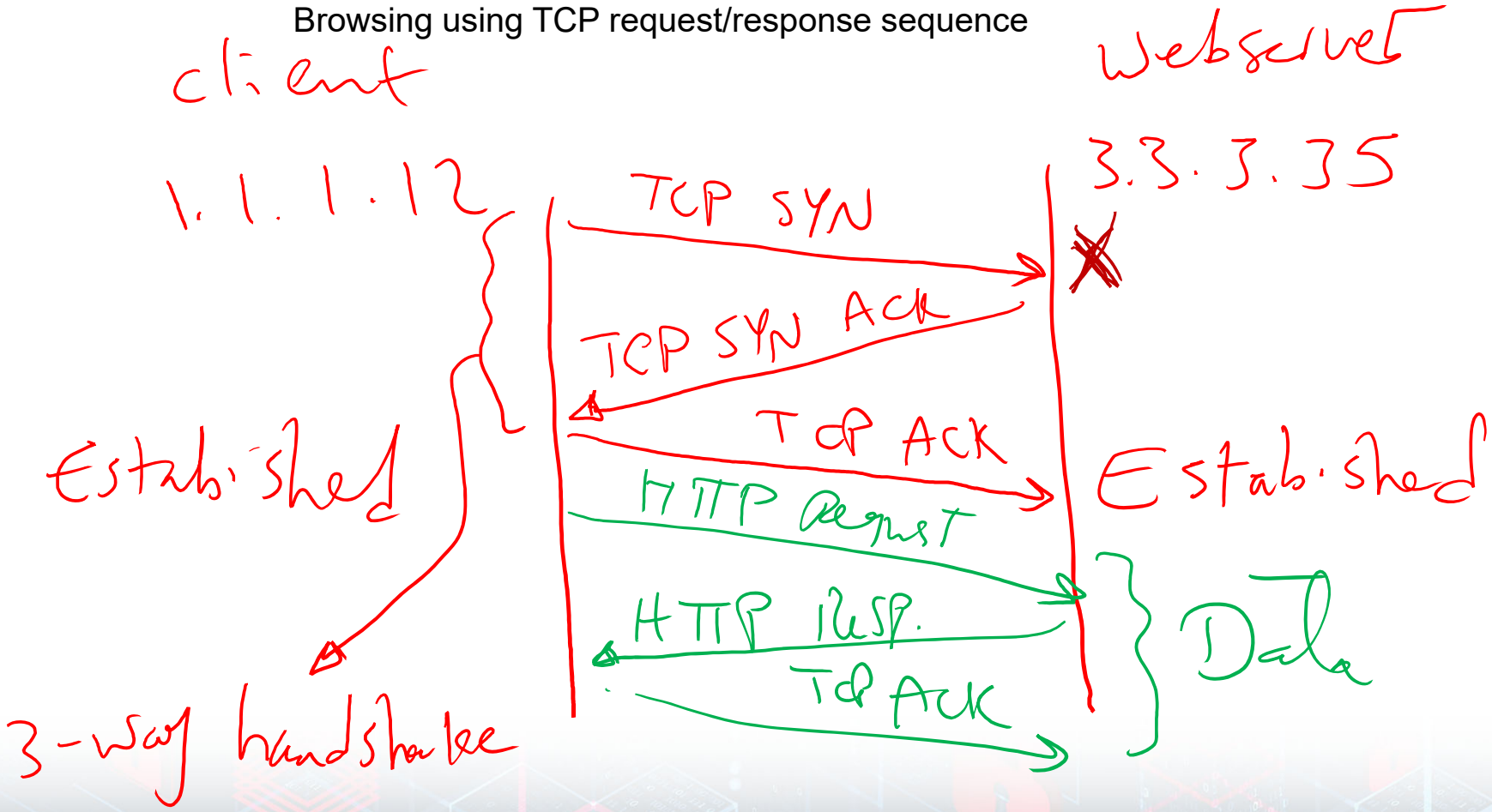
Security point of view => Default Deny

User point of view => Default Allow

Allow malicious users

TCP/Webserver

Browsing using TCP request/response sequence



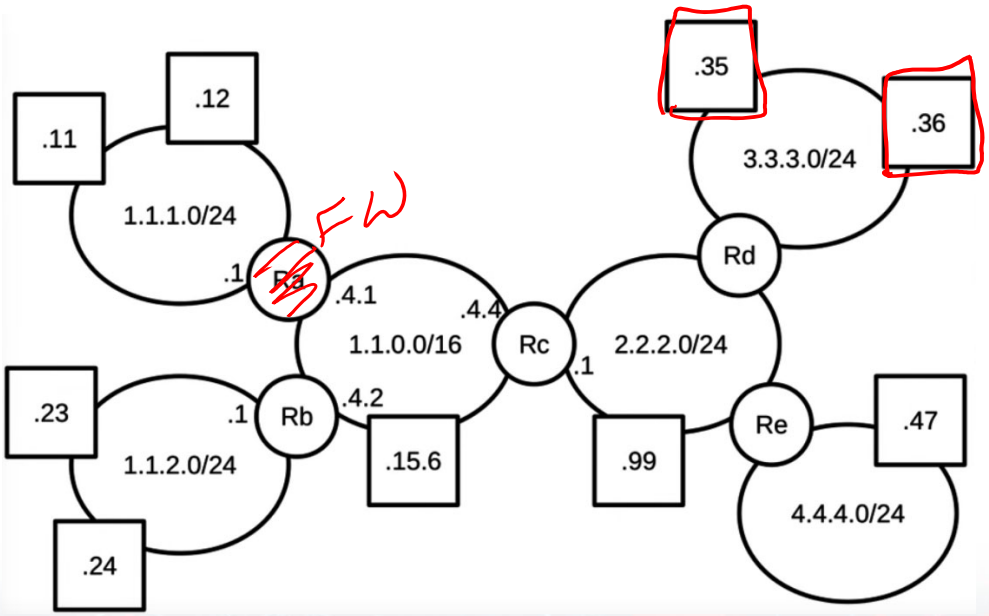
Example Network

What if we have the firewall on Ra

Aim: Stop 1.1.1.12 from browsing to servers on 3.3.3.0/24

TCP

SrcIP	DstIP	SrcPort	DstPort	Protocol	Action
1.1.1.12	3.3.3.0/24	*	80	6	Deny



FW

Default Action

Allow

Example Network

What if we have the firewall on Ra
Aim: Stop 1.1.1.12 from browsing to servers on 3.3.3.0/24

How the firewall will stop 1.1.1.12?

Drop TCP SYN

How we can bypass the previous rule?

HTTP 80

HTTPS 443

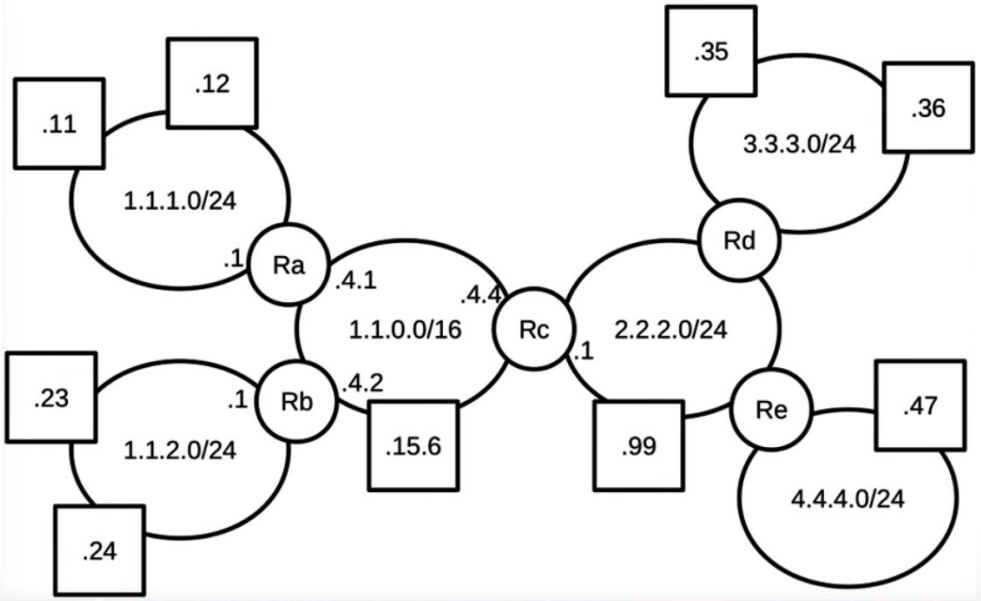
How we can correct the previous rule?

SrcIP	DstIP	SrcPort	DstPort	Protocol	Action
1.1.1.12	3.3.3.0/24	*	80	6	Deny
1.1.1.1	1.1.1.1	1.1	443	6	Deny

Example Network

What if we moved the firewall from computer 1.1.1.12 to Ra
Aim: Stop everyone except 1.1.1.12 from browsing to servers on 3.3.3.0/24

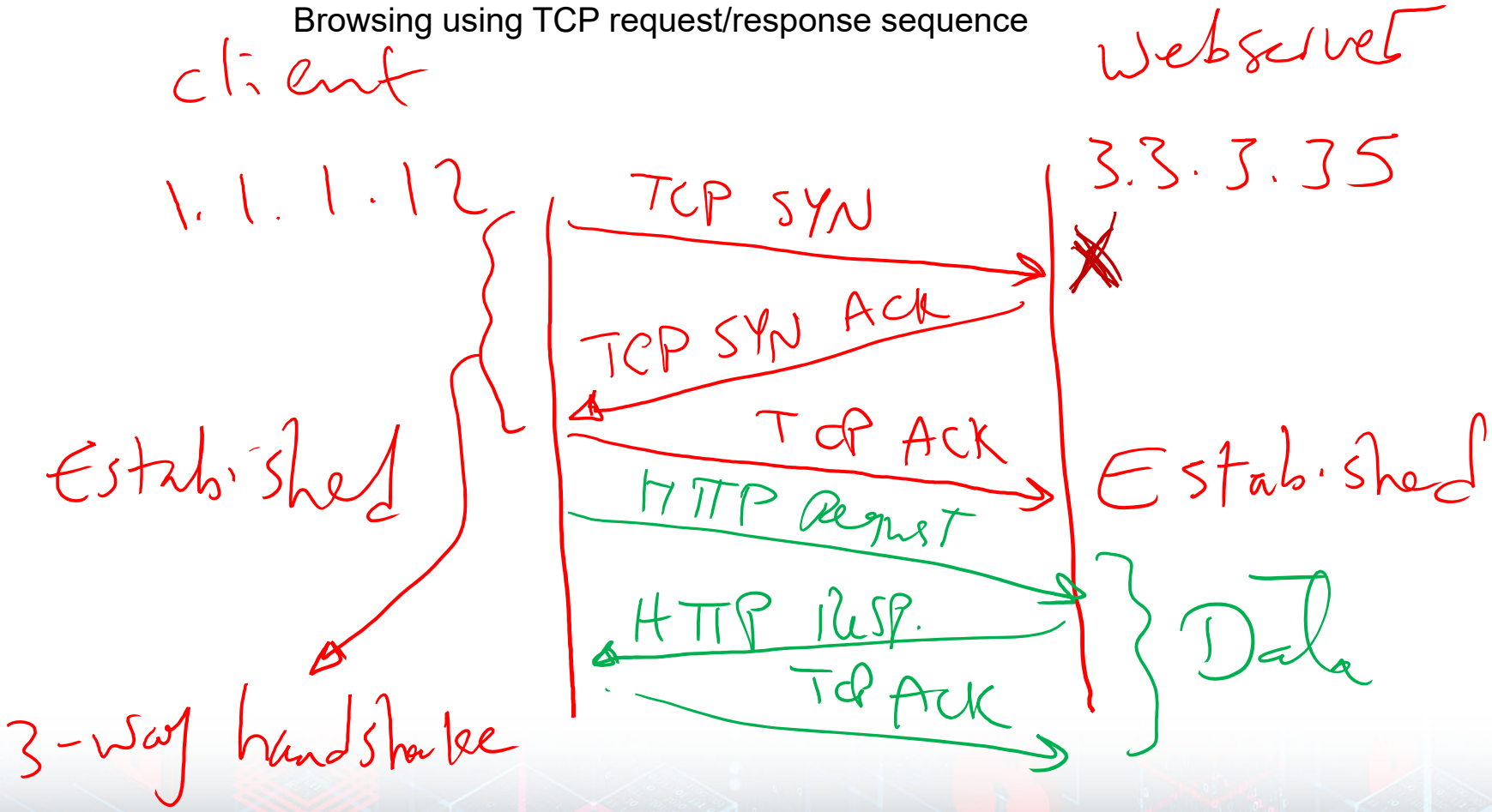
SrcIP	DstIP	SrcPort	DstPort	Protocol	Action
.12	3.3.3.0/24	*	80	6	Allow



Default Drop.

TCP/Webserver

Browsing using TCP request/response sequence



Example Network

What if we moved the firewall from computer 1.1.1.12 to Ra
Aim: Stop everyone except 1.1.1.12 from browsing to servers on 3.3.3.0/24

Is 1.1.1.12 able to communicate with the server successfully?

How we can resolve this issue?

SrcIP	DstIP	SrcPort	DstPort	Protocol	Action

Example Network

What if we moved the firewall from computer 1.1.1.12 to Ra
Aim: Stop everyone except 1.1.1.12 from browsing to servers on 3.3.3.0/24

Is 1.1.1.12 able to communicate with the server successfully?

No

How we can resolve this issue?

SrcIP	DstIP	SrcPort	DstPort	Protocol	Action
.12	3.3.3.0/24	*	80	6	Allow
3.3.3.0/24	.12	80	*	6	Allow

Example Network

What other problem we have here? Can an attacker reach 1.1.1.12? What about using 3.3.3.36 to send attack 1.1.1.12?

Yes

How to stop that?

???

Video Summary

- Issues with Packet Filtering Firewalls
- Allow/Deny Default Policies
- TCP/Webserver Communications
- Example Network