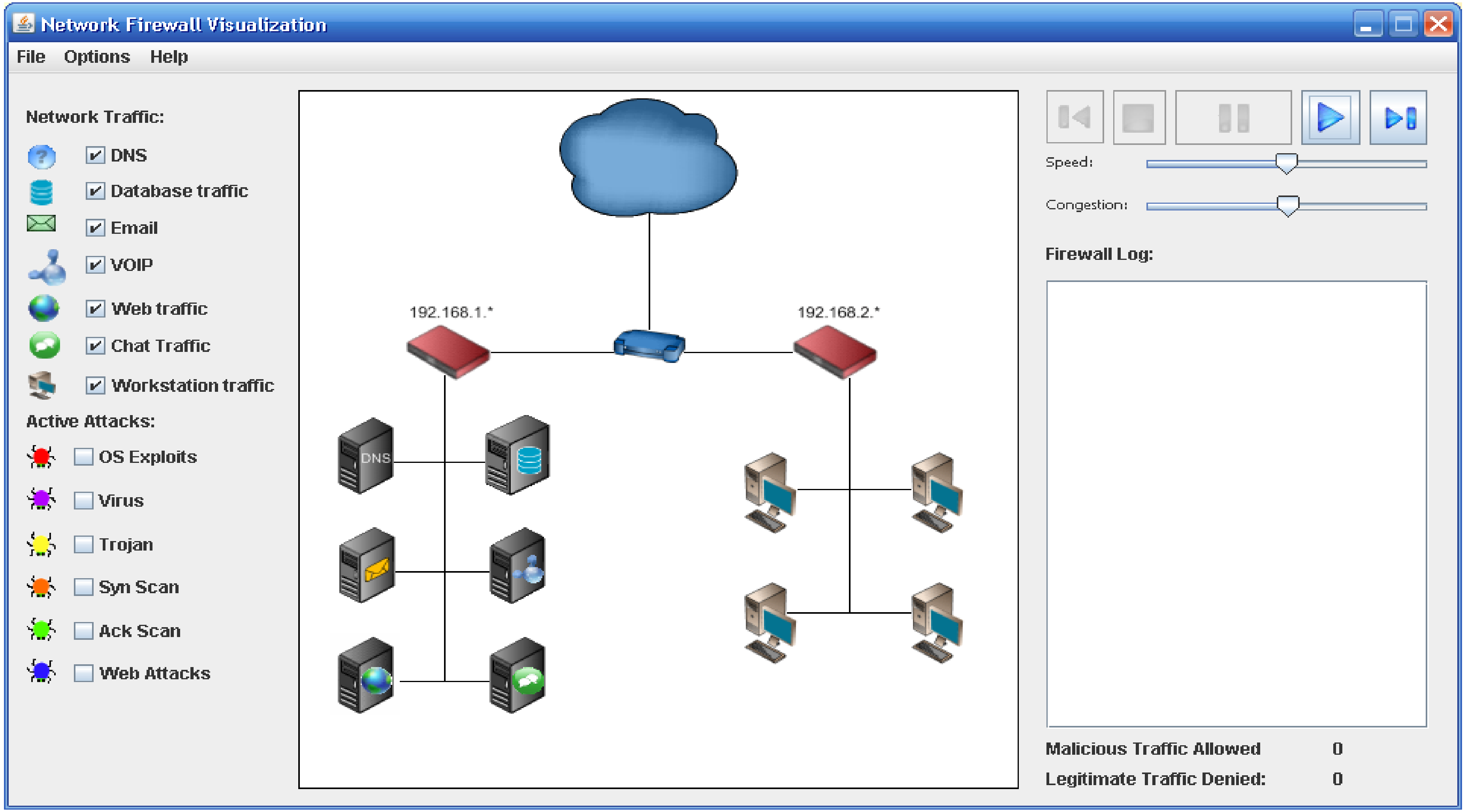
Network Security – Practical 3 Feedback

Dr. Sandra Scott-Hayward

CSC3064 Week 7 – Practical Feedback

School of Electronics, Electrical Engineering and Computer Science

CSC3064 – Practical 3 Review



Network Traffic:

- ☑ DNS
- ☑ Database traffic
- ☑ Email
- ☑ VOIP
- ☑ Web traffic
- ☑ Chat Traffic
- ☑ Workstation traffic

Active Attacks:

- □ OS Exploits
- □ Virus
- □ Trojan
- □ Syn Scan
- □ Ack Scan
- □ Web Attacks

Firewall Log:

Malicious Traffic Allowed 0

Legitimate Traffic Denied: 0

CSC3064 – Practical 3 Review

Lab3 Q1: Is traffic flowing from the internet into your system?

A1: No (Deny by default Firewall)

Lab3 Q2: Do you feel your system is secure?

A2: Secure from external attack but legitimate traffic is also denied.

(Not secured against internal attacks)

Lab3 Q3: What traffic flows through the firewall after adding your DNS Rule?

A3: DNS traffic is allowed out to the cloud i.e. from the DNS server

Note: you need the workstation traffic to generate the DNS requests.

CSC3064 – Practical 3 Review

Lab3 Q4: Which active attacks now work against machines behind the firewall?

A4: No active attacks

Lab3 Q5: How many rules did you have to write to secure your network?

A5: Note: You cannot completely secure the network because it can’t protect against web attacks while enabling legitimate web traffic.

CSC3064 – Practical 3 Review

A5: Selecting individual network traffic options produces the following flows:

DNS Traffic between cloud and DNS server, and workstations and DNS server

Database Traffic between cloud and database server, and workstation and database server

Email from cloud to email server followed by email server to workstation, and reverse

VoIP from cloud to VoIP server followed by VoIP server to workstation, and reverse

Web from cloud to web server (and to DB server) and then to web/workstation, and from workstation to web

Chat traffic between cloud and IRC server and workstation, and reverse

CSC3064 – Practical 3 Review

A5: All traffic blocked by default

DNS Out Rule – Source IP: 192.168.1.5 Port 53 – Dest Any/Any – Type Any

DNS In Rule – Source IP: Any/Any – Dest IP: 192.168.1.5 Port 53 – Type Any

DNS traffic allowed

Note: All attacks active – all blocked at Firewall except syn/ack scan targeting port 53

DB Out Rule – Source IP: 192.168.1.233 Port 3306 – Dest Any/Any – Type Any

DB In Rule – Source IP: Any/Any – Dest IP: 192.168.1.233 Port 3306 - Type Any

CSC3064 – Practical 3 Review

A5: *Mail Out Rule – Source IP: 192.168.1.136 Port 25 – Dest Any/Any – Type Any*

Mail In Rule – Source IP: Any/Any – Dest IP: 192.168.1.136 Port 25 - Type Any

VoIP Out Rule – Source IP: 192.168.1.74 Port 38287 – Dest Any/Any – Type Any

VoIP In Rule – Source IP: Any/Any – Dest IP: 192.168.1.74 Port 38287 - Type Any

Chat Out Rule – Source IP: 192.168.1.68 Port 5222 – Dest Any/Any – Type Any

Chat In Rule – Source IP: Any/Any – Dest IP: 192.168.1.68 Port 5222 - Type Any

Web Out Rule – Source IP: 192.168.1.114 Port 80 – Dest Any/Any – Type Any

Web In Rule – Source IP: Any/Any – Dest IP: 192.168.1.114 Port 80 - Type Any

All Workstation Out Rule – Source IP: 192.168.2. / Any– Dest Any/ Port 80 – Type TCP*

or individually Workstation 1-4 Out

CSC3064 – Practical 3 Review

Lab3 Q5: How many rules did you have to write to secure your network?

A5: 13-16 rules

Lab3 Q6: What firewall rule(s) did you create to allow chat traffic on the network?

A6: Source IP: 192.168.1.68 Port 5222 – Dest Any/Any – Type Any

Source IP: Any/Any – Dest IP: 192.168.1.68 Port 5222 - Type Any

Lab3 Q7: Which active attacks now work against machines behind the firewall?

A7: SYN scan, ACK scan, Web Attacks

CSC3064 – Practical 3 Review

Lab3 Q8: What does the stateful packet inspection flag on this firewall do?

A8: It stops the ACK scan.

Lab3 Q9: Is this the behaviour you expect from stateful packet inspection? Briefly explain.

A9: Yes, only capable of blocking ACK scan by checking for an existing connection request i.e. checking for a previous SYN packet (see the precise description for this tool in the Help: Defining Traffic section)