Computer Security (CS361)

Assignment-2

Date: 15/04/2023

Minshu Shaw (210123)

Hritik Pankaj (2101086)

1. Installation:

- Install Snort, an open-source network intrusion detection system (NIDS), on your system using the appropriate method for your operating system.

Example (Ubuntu):

sudo apt-get update

sudo apt-get install snort

2. Setup:

- Download PCAP files for testing Snort's intrusion detection capabilities. These files contain network traffic data.
- Create a custom rule file named `<rulefile_roll_no>.rules` in the `/etc/snort/rules` directory.

Example (Linux):

sudo touch /etc/snort/rules/<rulefile_roll_no>.rules

3. Rule Creation:

- Write Snort rules in the rule file to specify conditions for detecting specific network events or patterns.

Example Rules:

alert tcp any any -> any 21 (flags: S; msg: "Attempt to FTP to server.")

alert icmp any any -> any (msg: "Attempt to ping the server.")

alert tcp any any -> any 23 (flags: S; msg: "Attempt to telnet to server.")

alert tcp any any -> any 22 (msg: "Attempt to SSH to server."; content: "SSH-2";)

alert tcp any any -> any 80 (flags: S; msg: "Attempt to http to server.")

alert udp any any -> any 53 (msg: "DNS Query Ubuntu."; content: "ubuntu";)

alert any any -> any any (msg: "Found secret.txt."; content: "secret.txt"

alert tcp any any -> any 22 (flags: FA; msg: "F/A for SSH teardown.")

4. Execution:

- Run Snort using the custom rule file against the PCAP files.

Example Command:

sudo snort -c /etc/snort/snort.conf -R /etc/snort/rules/<rulefile_roll_no>.rules -r <pcap_file>

5. Output

1. For alert on any ftp traffic with the SYN flag set to the server. Message should read: "Attempt to FTP to server."

snort -c /opt/home/etc/snort/snort.lua -r /Users/hritik/iiitg/semester/6th_sem/Computer_security/Assignment2_snort/all_traffic.pcap --alert-before-pass -A alert_fast > /Users/hritik/iiitg/semester/6th_sem/Computer_security/Assignment2_snort/ftp_output_file.txt

Output message: Attempt to FTP to server.

2. For alert on any incoming pings to the server. Message should read: "Attempt to ping the server."

snort -c /opt/home/etc/snort/snort.lua -r /Users/hritik/iiitg/semester/6th_sem/Computer_security/Assignment2_snort/all_traffic.pcap --alert-before-pass -A alert_fast > /Users/hritik/iiitg/semester/6th_sem/Computer_security/Assignment2_snort/ping_output_file.txt

Output message: Attempt to ping the server.

3. For alert on any telnet traffic with the SYN flag set to the server.Message should read: "Attempt to telnet to server."

snort -c /opt/home/etc/snort/snort.lua -r /Users/hritik/iiitg/semester/6th_sem/Computer_security/Assignment2_snort/all_traffic.pcap --alert-before-pass -A alert_fast > /Users/hritik/iiitg/semester/6th_sem/Computer_security/Assignment2_snort/telnet_output_file.txt

Output message: Attempt to telnet to server.

4. For alert on any ssh traffic containing keyword “SSH-2” to the server. Message should read: “Attempt to SSH to server.”

snort -c /opt/home/etc/snort/snort.lua -r /Users/hritik/iiitg/semester/6th_sem/Computer_security/Assignment2_snort/all_traffic.pcap --alert-before-pass -A alert_fast > /Users/hritik/iiitg/semester/6th_sem/Computer_security/Assignment2_snort/ssh2_output_file.txt

Output message: “Attempt to SSH to server.”

5. For Alert on any http traffic with the SYN flag set to the server.Message should read: “Attempt to http to server.”

snort -c /opt/home/etc/snort/snort.lua -r /Users/hritik/iiitg/semester/6th_sem/Computer_security/Assignment2_snort/all_traffic.pcap --alert-before-pass -A alert_fast > /Users/hritik/iiitg/semester/6th_sem/Computer_security/Assignment2_snort/http_output_file.txt

Output message: Attempt to http to server.

6. For alert on any DNS traffic to the local DNS server that contains the keyword “ubuntu”. Message should read: “DNS Query Ubuntu.”

snort -c /opt/home/etc/snort/snort.lua -r /Users/hritik/iiitg/semester/6th_sem/Computer_security/Assignment2_snort/all_traffic.pcap --alert-before-pass -A alert_fast > /Users/hritik/iiitg/semester/6th_sem/Computer_security/Assignment2_snort/dns_output_file.txt

Output message: DNS Query Ubuntu.

7. For alert on any packet to the server that contains the text “secret.txt”. Message should read: “Found secret.txt.”

snort -c /opt/home/etc/snort/snort.lua -r /Users/hritik/iiitg/semester/6th_sem/Computer_security/Assignment2_snort/all_traffic.pcap --alert-before-pass -A alert_fast >

/Users/hritik/iiitg/semester/6th_sem/Computer_security/Assignment2_snort/secret_output_file.txt
Output message: Found secret.txt

8. For alert on any SSH traffic to the server with the FIN and ACK flags set. Message should read: "F/A for SSH teardown."

snort -c /opt/home/etc/snort/snort.lua -r /Users/hritik/iiitg/semester/6th_sem/Computer_security/Assignment2_snort/all_traffic.pcap --alert-before-pass -A alert_fast > /Users/hritik/iiitg/semester/6th_sem/Computer_security/Assignment2_snort/ssh_finack_output_file.txt

Output message: F/A for SSH teardown

This will save all console outputs to `output_file.txt`, which includes alerts triggered by your rules