Cybersecurity (Security+) and P4 Programmable Switches

Overview Cybersecurity Labs

Jorge Crichigno, Elie Kfoury
University of South Carolina
http://ce.sc.edu/cyberinfra

Western Academy Support and Training Center (WASTC)
University of South Carolina (USC)
Energy Sciences Network (ESnet)

June 19th, 2023

Cybersecurity Fundamentals Lab Series

Cybersecurity Fundamentals Lab Series

The labs are available on NDG’s NETLAB+ and provides hands-on experiences on:

- Reconnaissance and vulnerability assessment
- Infiltrating a victim’s device with malware (trojan, spyware, keylogger, etc.)
- Social engineering attacks (phishing emails, credential harvesting)
- Attacks on web applications (SQL injection, cross-site scripting)
- Network attacks (Denial of Service (DoS))
- Cryptography fundamentals (symmetric encryption, asymmetric encryption, digital certificates)
- Packet filtering and access control lists
- Brute force attacks on passwords
- Intrusion detection and prevention system

Cybersecurity Fundamentals Lab Series

The labs provide learning experiences on cybersecurity topics

- Lab 1: Reconnaissance: Scanning with NMAP, Vulnerability Assessment with OpenVAS
- Lab 2: Remote Access Trojan (RAT) using Reverse TCP Meterpreter
- Lab 3: Escalating Privileges and Installing a Backdoor
- Lab 4: Collecting Information with Spyware: Screen Captures and Keyloggers
- Lab 5: Social Engineering Attack: Credentials Harvesting and Remote Access through Phishing Emails
- Lab 6: SQL Injection Attack on a Web Application
- Lab 7: Cross-site Scripting (XSS) Attack on a Web Application
- Lab 8: Denial of Service (DoS) Attacks: SYN/FIN/RST Flood, Smurf attack, and SlowLoris
- Lab 9: Cryptographic Hashing and Symmetric Encryption
- Lab 10: Asymmetric Encryption: RSA, Digital Signatures, Diffie-Hellman
- Lab 11: Public Key Infrastructure: Certificate Authority, Digital Certificate
- Lab 12: Configuring a Stateful Packet Filter using iptables
- Lab 13: Online Dictionary Attack against a Login Webpage
- Lab 14: Intrusion Detection and Prevention using Suricata

Organization of Lab Manuals

Each lab starts with a section *Overview*

- Objectives
- Lab settings: passwords, device names
- Roadmap: organization of the lab

Section 1

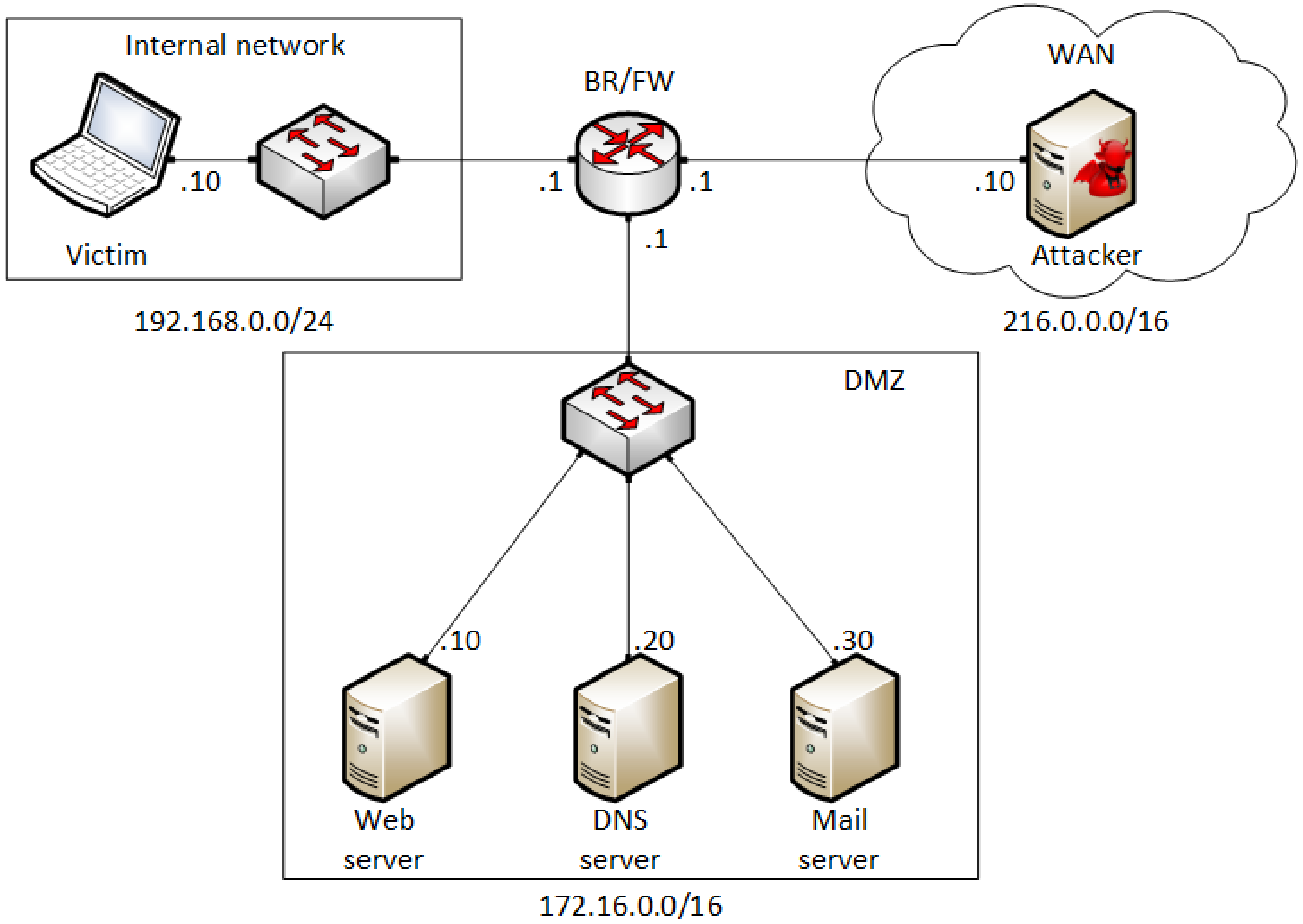
- Background information (theory) of the topic being covered (e.g., malware fundamentals)
- Section 1 is optional (i.e., the reader can skip this section and move to lab directions)

Section 2… n

- Step-by-step directions

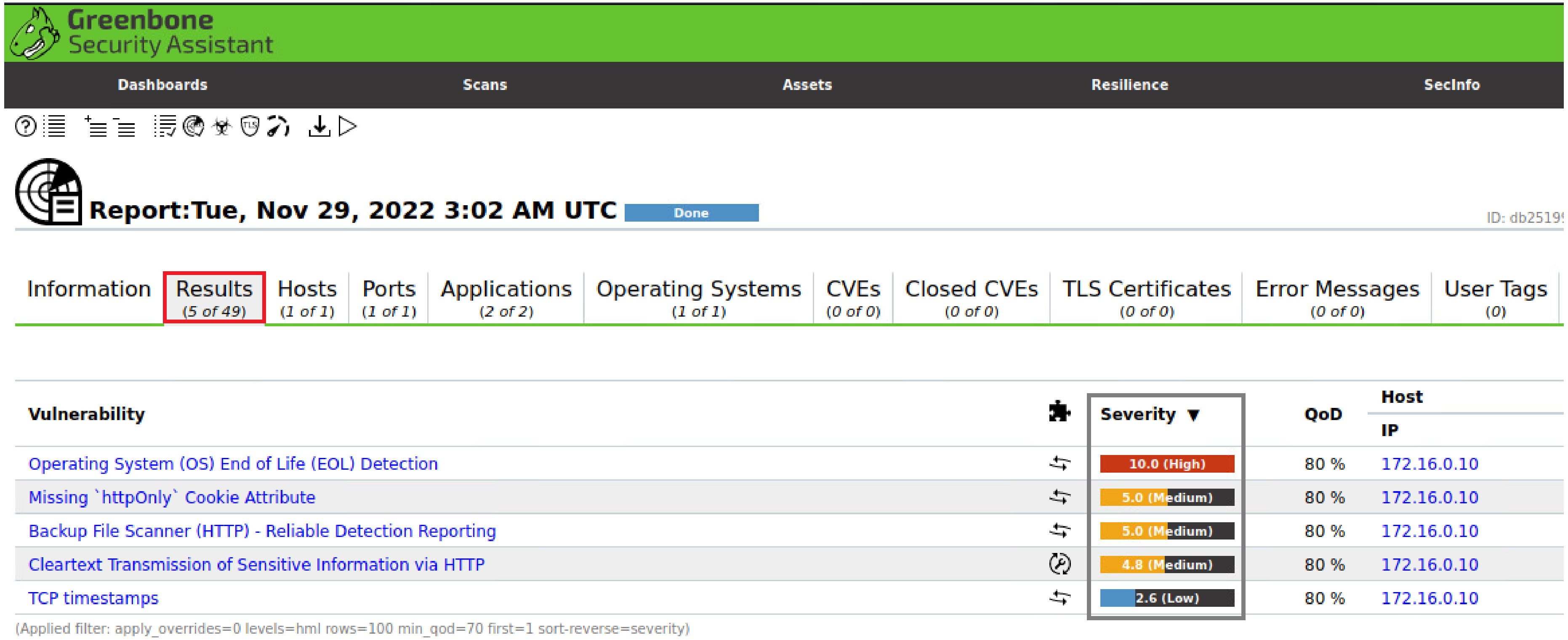
Pod Design

- Attacker in the WAN running Kali
- Victim in the internal network running Windows 10
- Web, DNS, and Mail servers in the DMZ zone
- Border router interconnect the networks
- Border router implements basic security policy:
  - Attacker cannot initiate connections to devices in the internal network



Examples

Vulnerability assessment using OpenVAS



Report:Tue, Nov 29, 2022 3:02 AM UTC Done

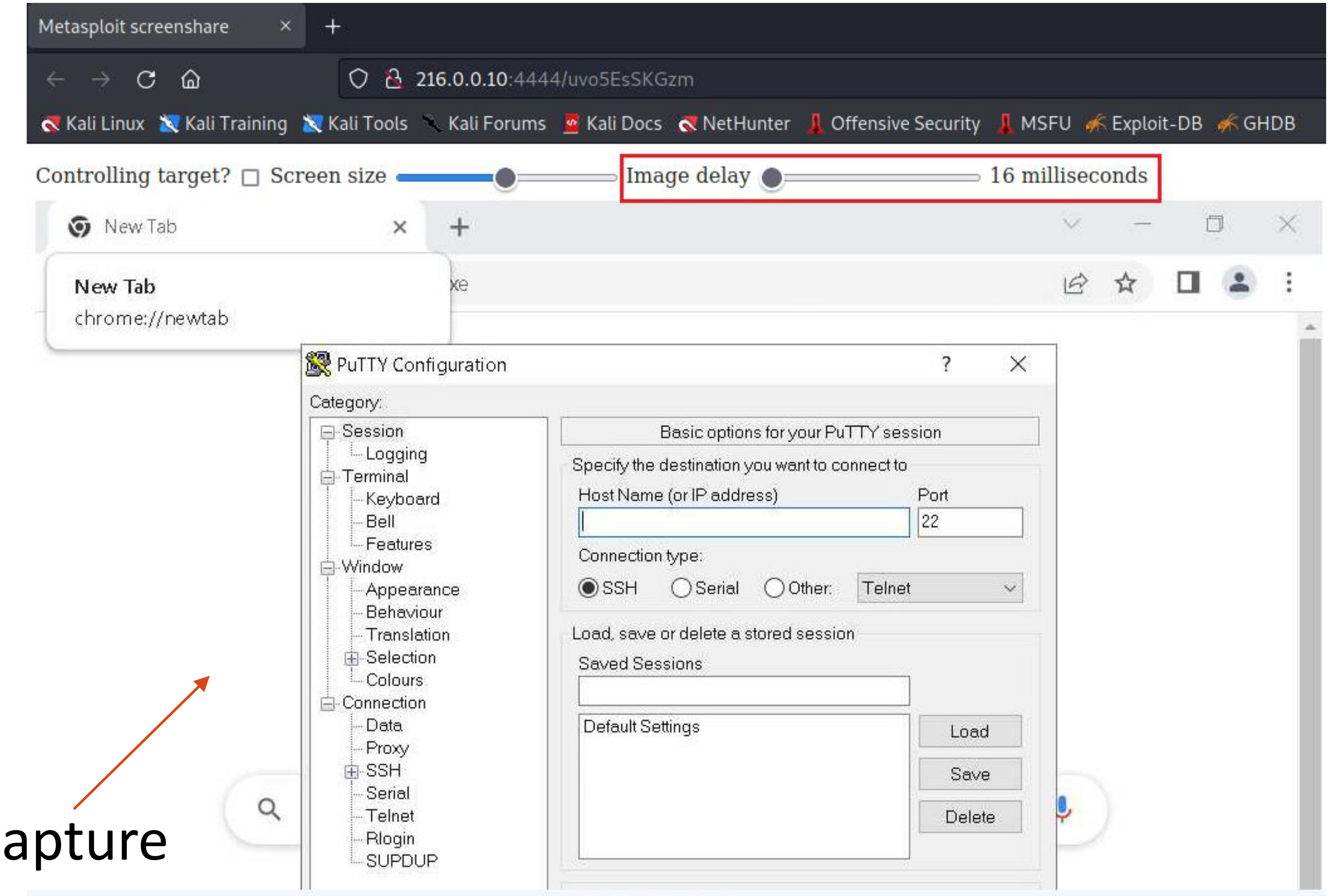
ID: db2519

Vulnerability		Severity ▼	QoD	Host
				IP
Operating System (OS) End of Life (EOL) Detection	⇆	10.0 (High)	80 %	172.16.0.10
Missing `httpOnly` Cookie Attribute	⇆	5.0 (Medium)	80 %	172.16.0.10
Backup File Scanner (HTTP) - Reliable Detection Reporting	⇆	5.0 (Medium)	80 %	172.16.0.10
Cleartext Transmission of Sensitive Information via HTTP	⊘	4.8 (Medium)	80 %	172.16.0.10
TCP timestamps	⇆	2.6 (Low)	80 %	172.16.0.10

(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)

Examples

Deploying a Spyware



Metasploit screenshare

216.0.0.10:4444/uvo5EsSKGzm

Controlling target? □ Screen size

Image delay 16 milliseconds

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address):

Port: 22

Connection type: ● SSH ○ Serial ○ Other: Telnet

Load, save or delete a stored session

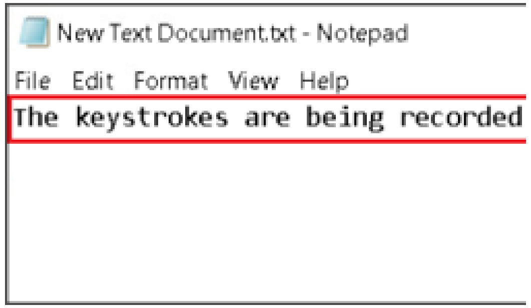
Saved Sessions

Default Settings

Screen capture

Keylogger

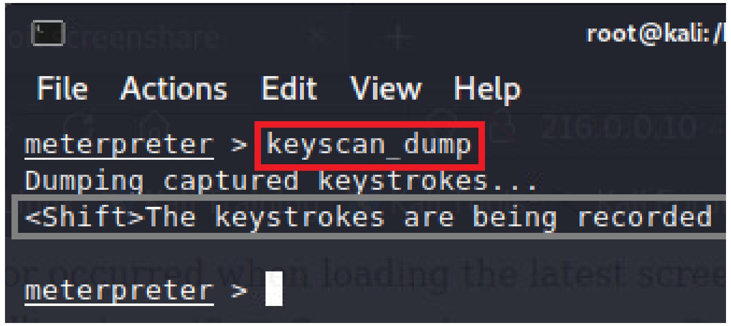
Victim



New Text Document.txt - Notepad

The keystrokes are being recorded

Attacke



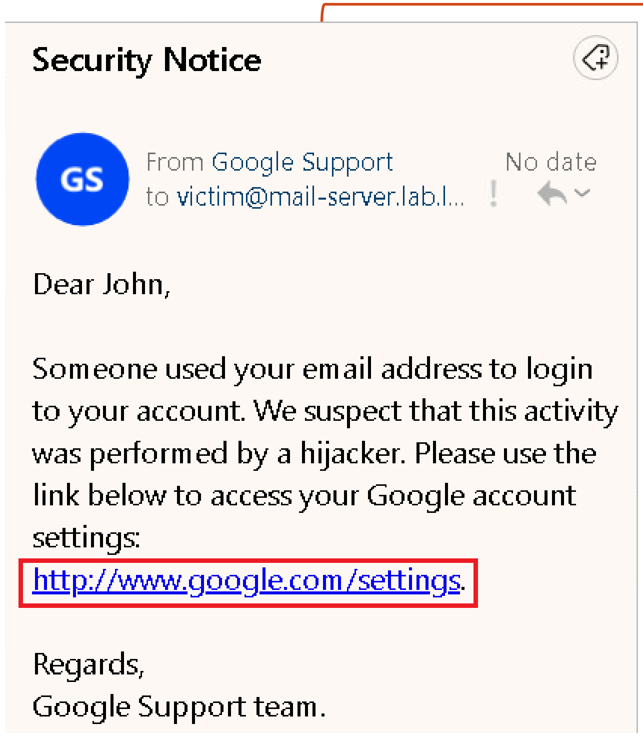
```
meterpreter > keyscan_dump
Dumping captured keystrokes...
<Shift>The keystrokes are being recorded

meterpreter > 
```

Examples

Social engineering and phishing emails

Victim



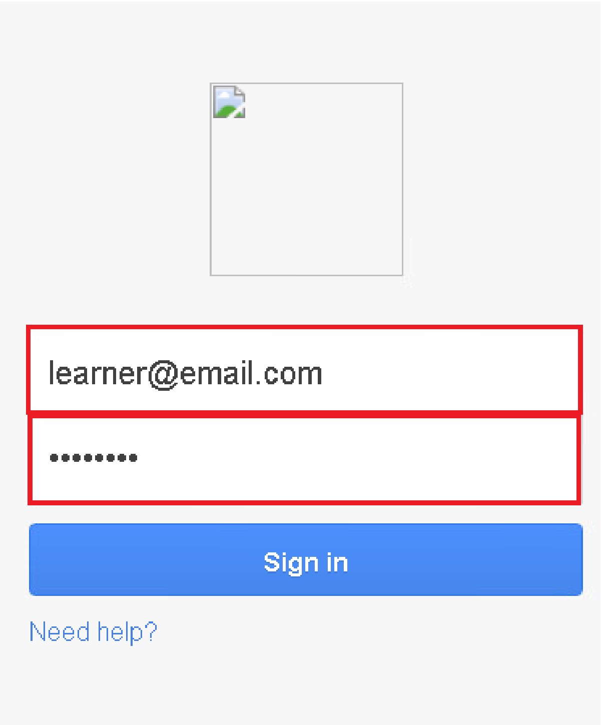
Security Notice

GS From Google Support No date
to victim@mail-server.lab.l...

Dear John,

Someone used your email address to login to your account. We suspect that this activity was performed by a hijacker. Please use the link below to access your Google account settings:
http://www.google.com/settings.

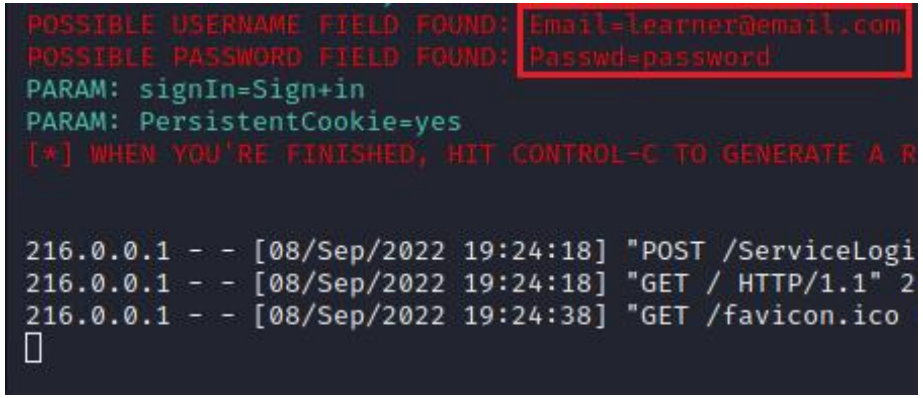
Regards,
Google Support team.



learner@email.com

••••••••

Attacker

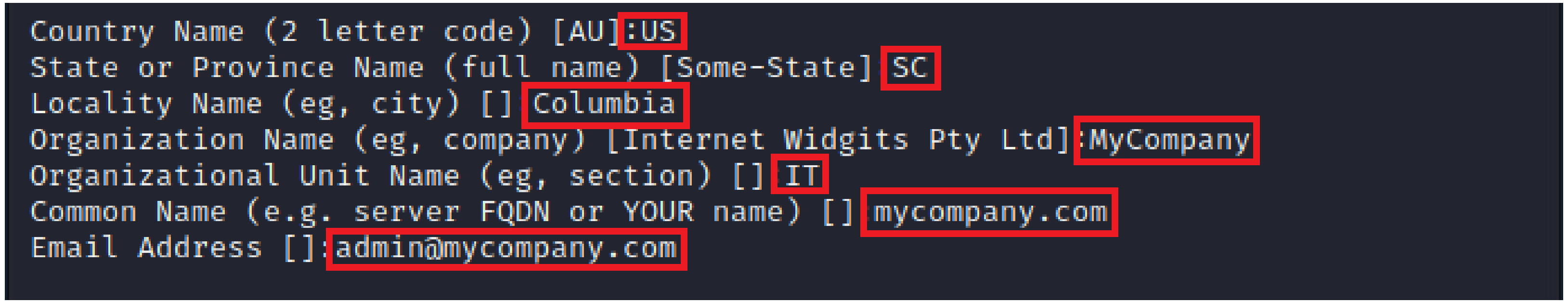


```
POSSIBLE USERNAME FIELD FOUND: Email=learner@email.com
POSSIBLE PASSWORD FIELD FOUND: Passwd=password
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A R


216.0.0.1 - - [08/Sep/2022 19:24:18] "POST /ServiceLogi
216.0.0.1 - - [08/Sep/2022 19:24:18] "GET / HTTP/1.1" 2
216.0.0.1 - - [08/Sep/2022 19:24:38] "GET /favicon.ico
```

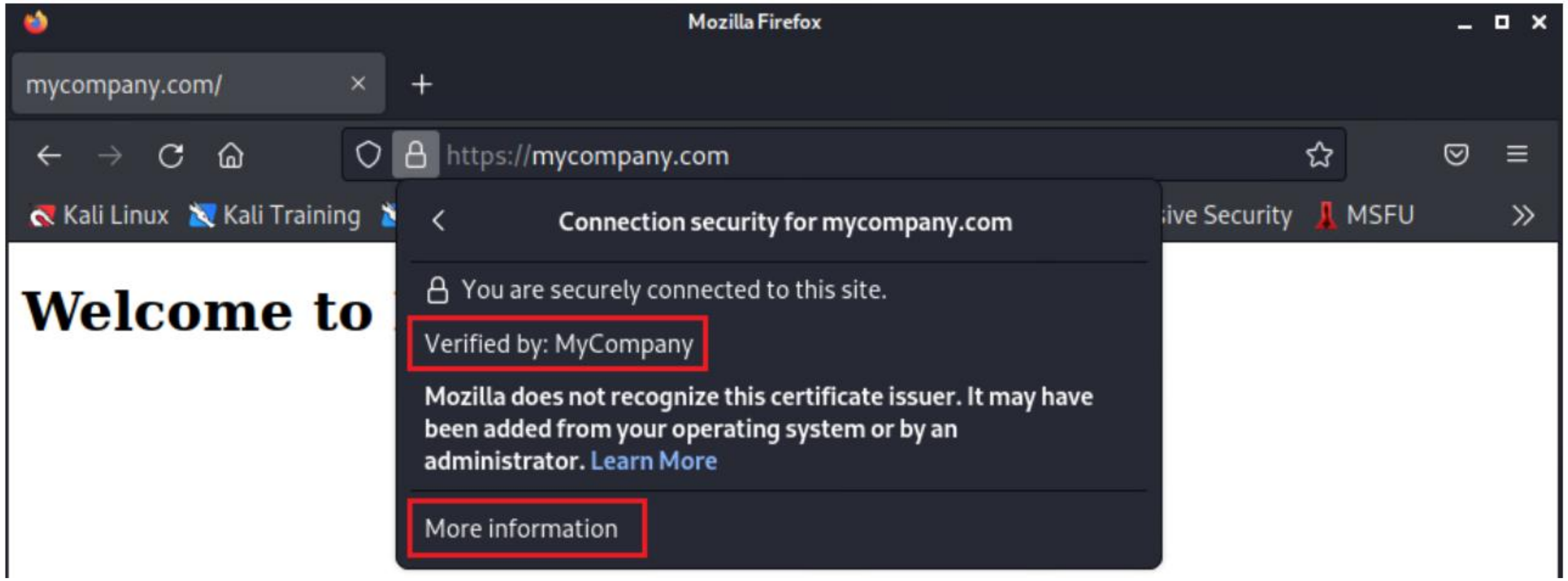
Examples

Creating a digital certificate and deploying it on an Apache web server



```
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State] SC
Locality Name (eg, city) [] Columbia
Organization Name (eg, company) [Internet Widgits Pty Ltd]:MyCompany
Organizational Unit Name (eg, section) [] IT
Common Name (e.g. server FQDN or YOUR name) [] mycompany.com
Email Address []:admin@mycompany.com
```

X.509 certificate



Connection security for mycompany.com

You are securely connected to this site.

Verified by: MyCompany

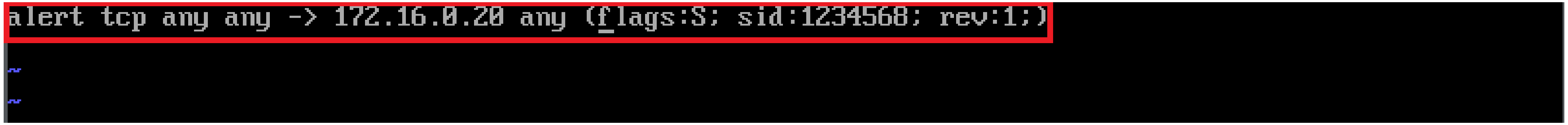
Mozilla does not recognize this certificate issuer. It may have been added from your operating system or by an administrator. Learn More

More information

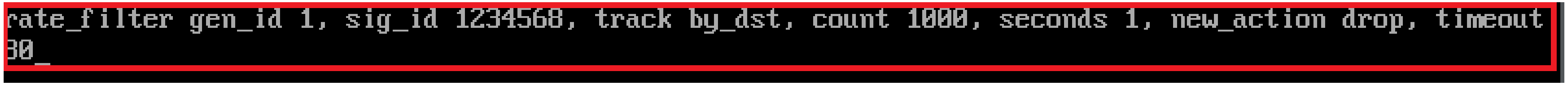
Certificate deployed on a production grade web server

Examples

Detecting and blocking SYN Flood attack using Suricata IDS/IPS

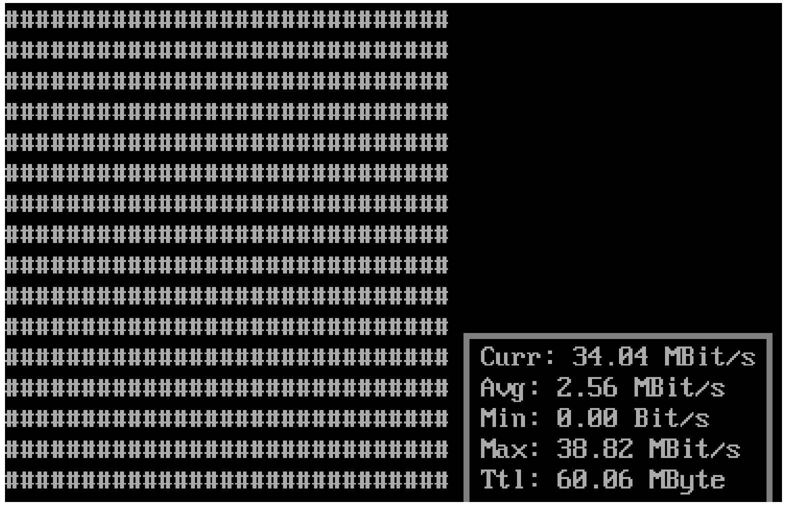


```
alert tcp any any -> 172.16.0.20 any (flags:S; sid:1234568; rev:1;)
~
~
```



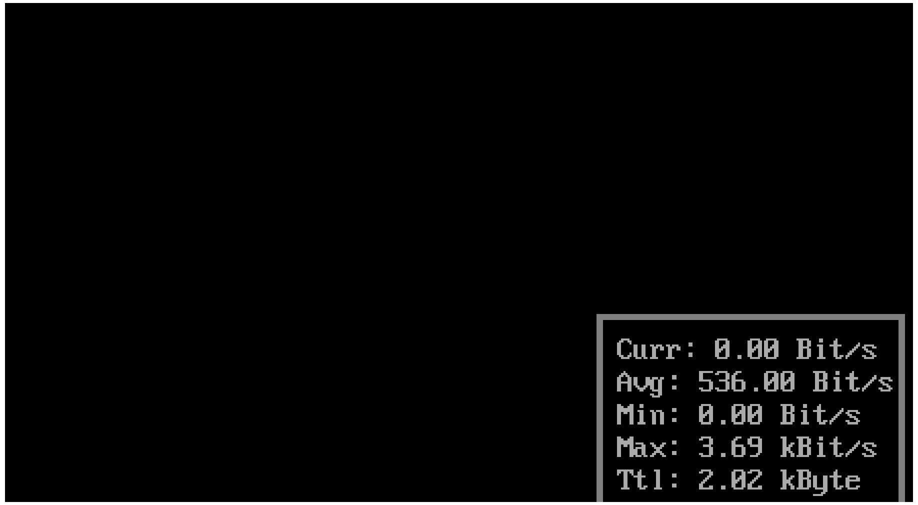
```
rate_filter gen_id 1, sig_id 1234568, track by_dst, count 1000, seconds 1, new_action drop, timeout
30_
```

Incoming rate before mitigation



```
#############################
#############################
#############################
#############################
#############################
#############################
#############################
#############################
#############################
#############################
#############################
############################# Curr: 34.04 MBit/s
############################# Avg: 2.56 MBit/s
############################# Min: 0.00 Bit/s
############################# Max: 38.82 MBit/s
############################# Ttl: 60.06 MByte
```

Incoming rate after mitigation



```
Curr: 0.00 Bit/s
Avg: 536.00 Bit/s
Min: 0.00 Bit/s
Max: 3.69 kBit/s
Ttl: 2.02 kByte
```