CSE 3157: Penetration Testing Workshop

Weidman
Ch 7: Capturing traffic

Insider Attack

Introduction to ARP Cache Poisoning

- ARP (Address Resolution Protocol) maps IP addresses to MAC addresses in a local network.
- ARP cache poisoning allows an attacker to intercept traffic between a victim and a gateway.
- This attack is commonly used for man-in-the-middle (MITM) attacks.

Steps to Perform ARP Cache Poisoning Using Arpspoof

- **tep 1: Enable IP Forwarding**
- Before starting, enable IP forwarding so that packets can be forwarded between the victim and the gateway.
- echo 1 > /proc/sys/net/ipv4/ip_forward
- **Step 2: Identify Target and Gateway IP Addresses**
- Use ifconfig or ip a to check your network interface.
- Use arp -a to find the IP addresses of the target (victim) and the gateway.

Steps to Perform ARP Cache Poisoning Using Arpspoof

- **Step 3: Start Arpspoof**
- Open a terminal and execute the following command to poison the ARP cache of the victim:

```
arpspoof -i eth0 -t [Victim IP] [Gateway IP]
```

- In another terminal, execute the following command to poison the ARP cache of the gateway:
- `arpspoof -i eth0 -t [Gateway IP] [Victim IP]`

Steps to Perform ARP Cache Poisoning Using Arpspoof

- **Step 4: Capture Network Traffic (Optional)**
- Use Wireshark or tcpdump to capture the traffic between the victim and the gateway:
- `tcpdump -i eth0`
- **Step 5: Restore the Network (Cleanup)**
- After completing the attack, restore normal ARP functionality by running:
- `echo 0 > /proc/sys/net/ipv4/ip_forward`
- You can also clear the ARP cache on the victim machine by restarting the network interface or using:
- `arp -d [IP Address]`

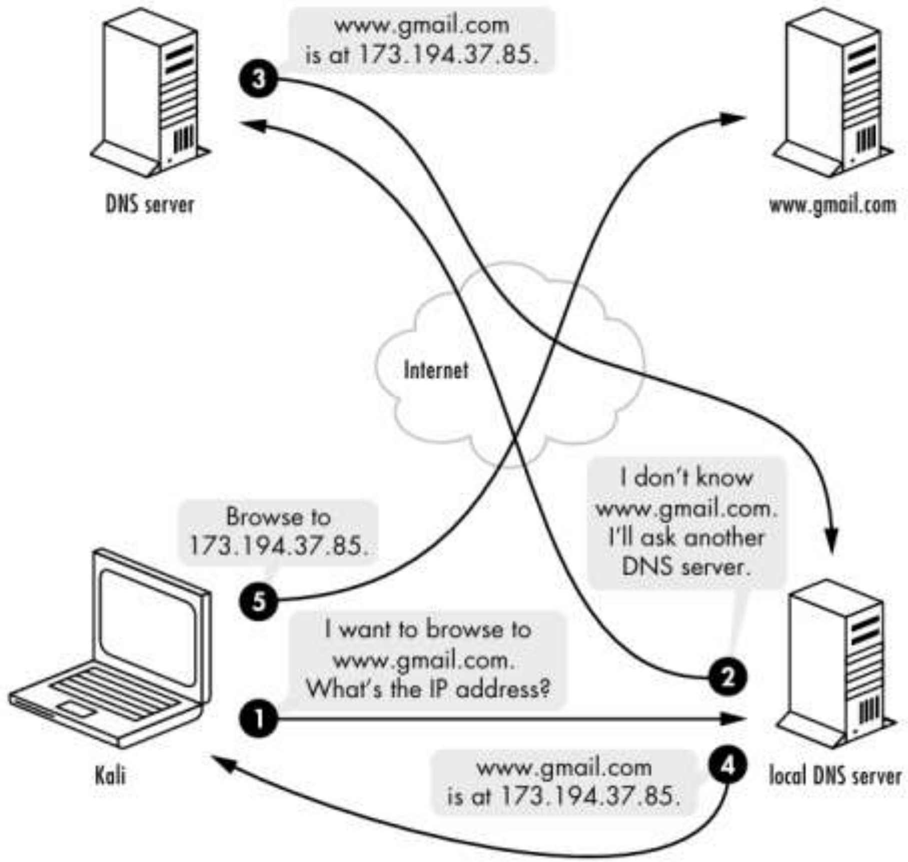
How DNS Works?

- - Machines need IP addresses to connect to other systems.
- - Remembering domain names (e.g., www.gmail.com) is easier than memorizing changing IP addresses.
- - DNS resolution translates human-readable domain names into IP addresses.

DNS Resolution Example

- - The `nslookup` command translates a domain name into an IP address.
- Example:
- root@kali~# nslookup www.gmail.com
- - Returns multiple IP addresses for redundancy and reliability.

DNS Resolution Example


DNS server
www.gmail.com
Internet
Kali
local DNS server
3
www.gmail.com is at 173.194.37.85.
2
I don't know www.gmail.com. I'll ask another DNS server.
5
Browse to 173.194.37.85.
1
I want to browse to www.gmail.com. What's the IP address?
4
www.gmail.com is at 173.194.37.85.

DNS Resolution Process

- 1. User Enters Domain Name
- 2. Query Sent to DNS Resolver
- 3. Checking Local Cache
- 4. Query Sent to Root Server
- 5. Root Server Response
- 6. Query Sent to TLD Server
- 7. TLD Server Response
- 8. Query Sent to Authoritative Server
- 9. Authoritative Server Response
- 10. IP Address Returned
- 11. Connection Established

DNS Cache Poisoning Attack

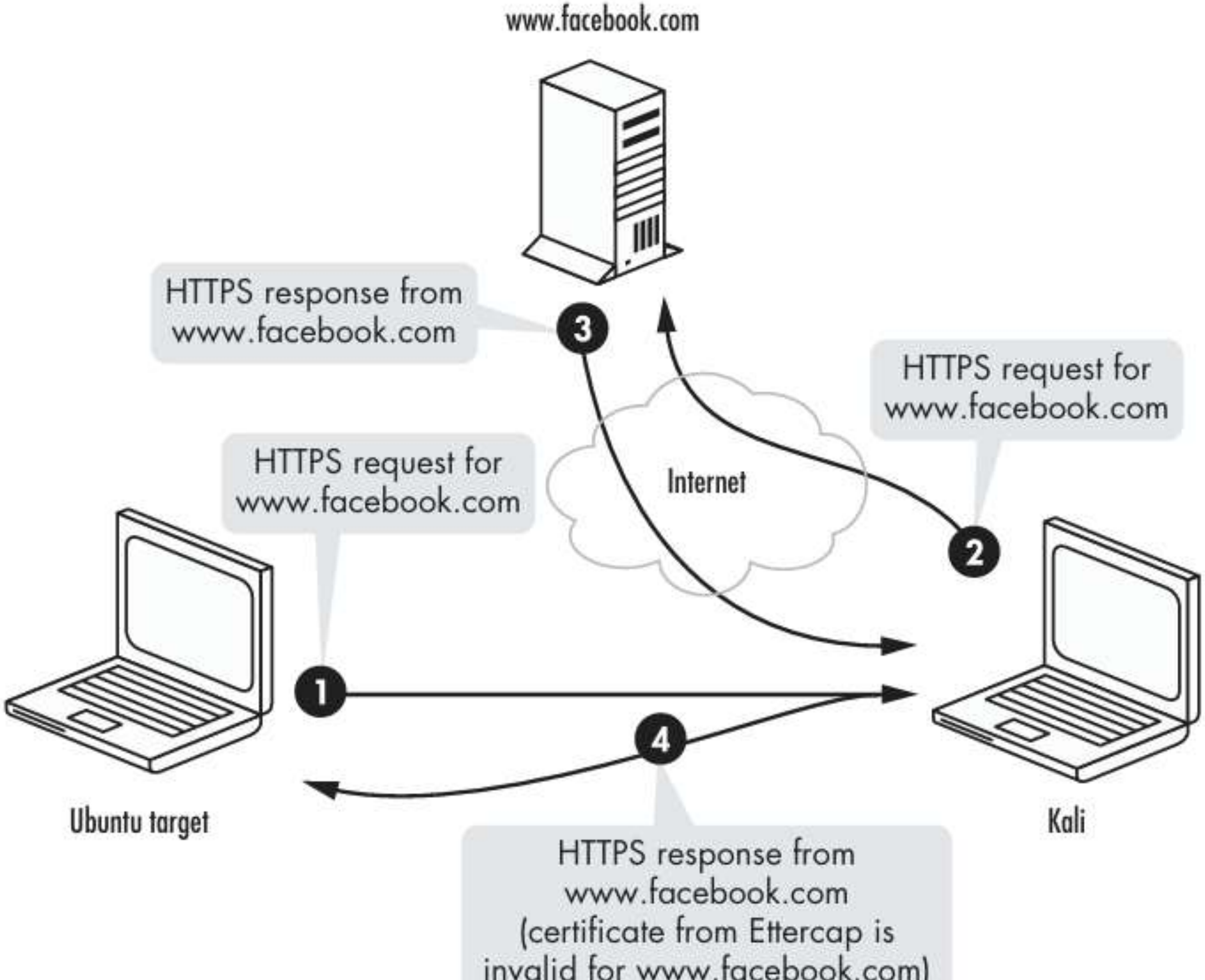
- - Similar to ARP cache poisoning.
- - An attacker sends bogus DNS responses pointing a domain name to the wrong IP.

Setting Up DNS Spoofing in Kali

- 1. Ensure Apache server is running:
- root@kali:~# service apache2 start
- 2. Create a `hosts.txt` file with spoofed DNS entries:
- root@kali:~# echo "192.168.20.9 www.gmail.com" > hosts.txt
- 3. Run `dnsspoof` to hijack DNS queries:
- root@kali:~# dnsspoof -i eth0 -f hosts.txt

Demonstrating the Attack

- - If successful, `nslookup` returns the attacker's IP instead of the real Gmail IP.
- georgia@ubuntu:~$ nslookup www.gmail.com
- - The victim’s browser still shows `www.gmail.com` but connects to the attacker’s server.
- - The attacker can clone the actual Gmail website to trick users.



1 HTTPS request for www.facebook.com

2 HTTPS request for www.facebook.com

3 HTTPS response from www.facebook.com

4 HTTPS response from www.facebook.com (certificate from Ettercap is invalid for www.facebook.com)

DNS SUMMARY

- - DNS spoofing can redirect users to malicious sites.
- - To prevent attacks:
- - Use secure DNS protocols like DNSSEC.
- - Encrypt DNS traffic with DoH (DNS over HTTPS) or DoT (DNS over TLS).
- - Monitor DNS traffic for unusual activity.

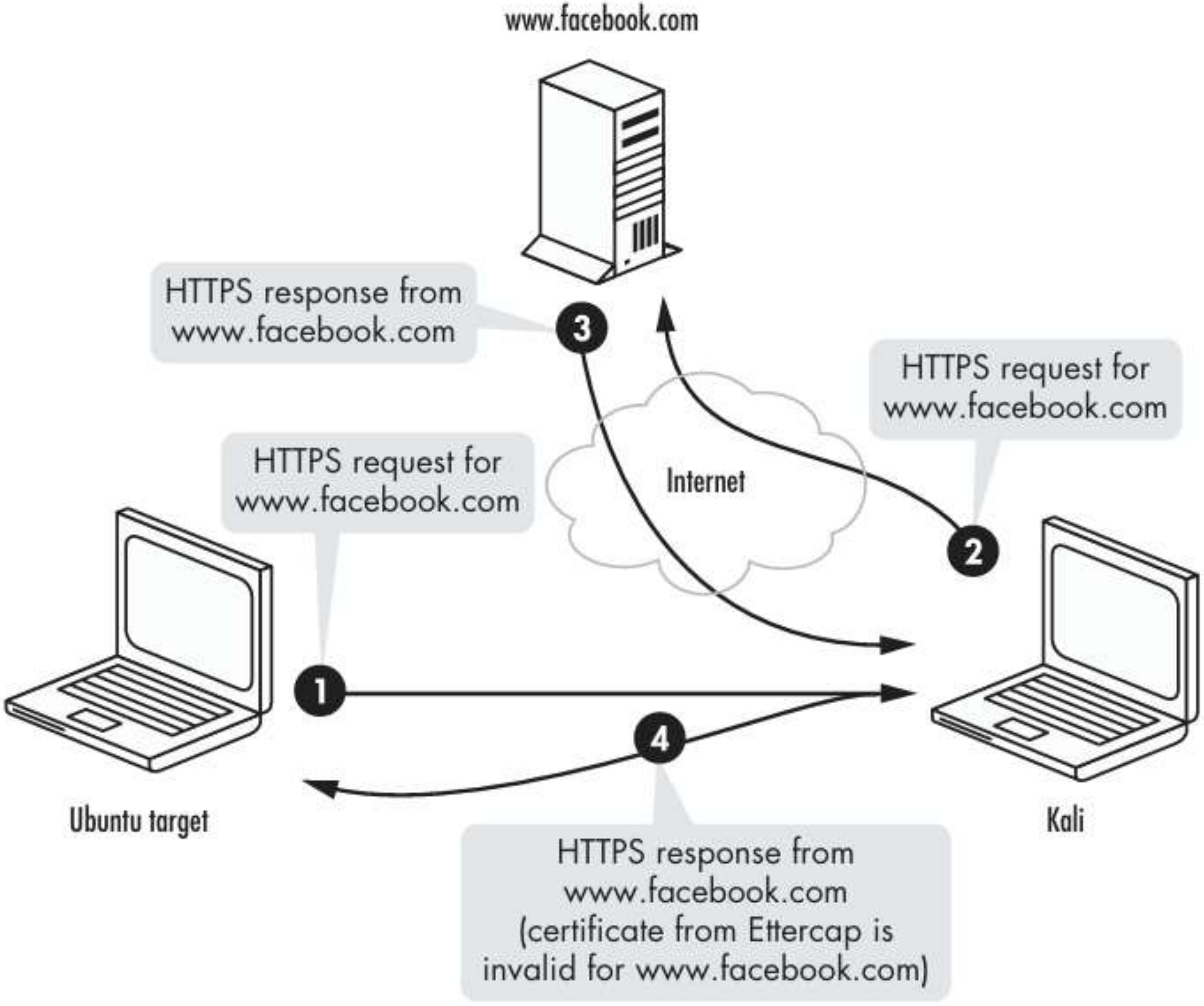
SSL Attacks Overview

- - SSL encrypts communication between a user and a website to protect data.
- - Attackers can intercept SSL traffic using man-in-the-middle techniques.
- - Users may bypass SSL warnings, exposing their data to attackers.

SSL Basics

- - SSL uses certificates to verify a website’s identity.
- - Browsers check if a site’s SSL certificate is trusted.
- - If the certificate is invalid, users see a warning message.
- - Attackers exploit users who ignore SSL warnings.

SSL Man in the Middle



www.facebook.com
HTTPS response from www.facebook.com
3
HTTPS request for www.facebook.com
2
Internet
HTTPS request for www.facebook.com
1
4
Ubuntu target
Kali
HTTPS response from www.facebook.com (certificate from Ettercap is invalid for www.facebook.com)

SSL Man-in-the-Middle Attack

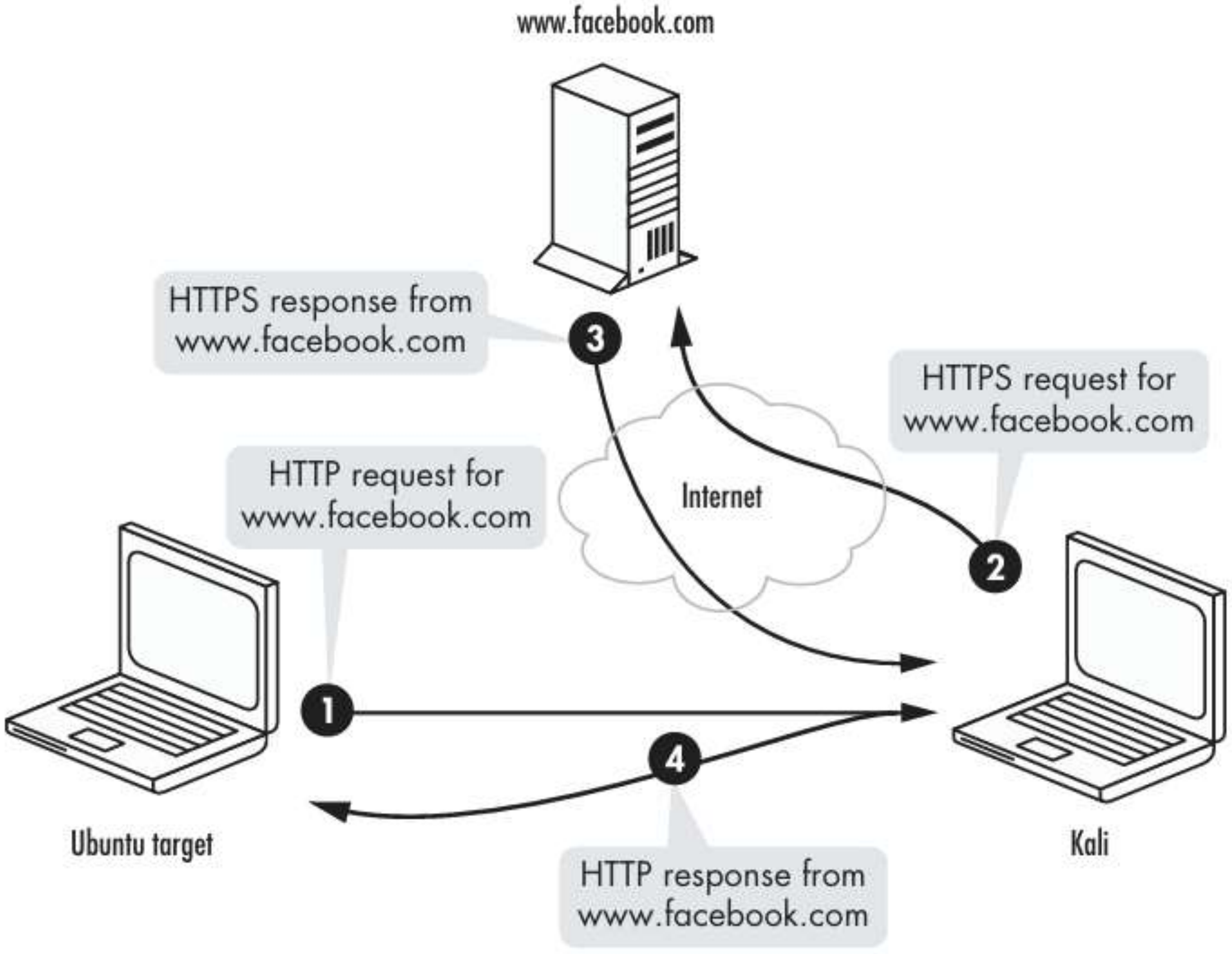
- 1. The attacker intercepts SSL traffic using ARP poisoning.
- 2. The user sees an SSL warning but may proceed anyway.
- 3. If the user ignores the warning, the attacker can decrypt their traffic.
- 4. Example attack using Ettercap:

- root@kali:~# ettercap -Ti eth0 -M arp:remote /192.168.20.1/ /192.168.20.11/

SSL Stripping Attack

- - Attackers remove HTTPS encryption before the traffic reaches the user.
- - Instead of an SSL warning, users unknowingly send sensitive data over HTTP.
- - The attacker captures credentials in plaintext without triggering security alerts.
- Most users don’t enter https://www.facebook.com or even http://www.facebook.com into their browsers; they type www.facebook .com or sometimes just facebook.com. And that’s why this attack is possible.

SSL Stripping Attack



www.facebook.com
HTTPS response from www.facebook.com
3
HTTPS request for www.facebook.com
HTTP request for www.facebook.com
Internet
2
1
4
Ubuntu target
Kali
HTTP response from www.facebook.com

SSL Stripping Attack

- we need to set an Iptables rule to pass traffic that is headed to port 80 through SSLstrip.
- We’ll run SSLstrip on port 8080, as shown next, then restart Arpspoof and spoof the default gateway.
- root@kali:# iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 8080
- Now start SSLstrip, and tell it to listen on port 8080 with the -l flag. root@kali:# sslstrip -l 8080

SSL Stripping Attack

- Next, browse to a site that uses SSL (try any Internet site that requires login credentials) from your Linux target, like the Twitter login page.
- As you can see, HTTP has replaced HTTPS in the address bar. When you log in, your credentials will be reported in plaintext by SSLstrip. (No, my Twitter password isn’t really “password.”)
- This attack is more sophisticated than a straight SSL man-in-the-middle attack.
- We are able to avoid the certificate warning because the server is completing an SSL connection with SSLstrip rather than the browser. (Check browser GET/POST)

Defending Against SSL Attacks

- - Always verify SSL certificates before proceeding.
- - Enable HTTPS Everywhere extensions in browsers.
- - Use secure network connections (avoid public Wi-Fi for sensitive transactions).
- - Monitor and log unusual network activity.

Assignment

- Demonstrate Man-in-the-Middle attack with

1. ARP Cache poisoning
2. DNS Cache poisoning
3. SSL Attack

Instruction for screenshot / browser logs:

i. Write your IP, Victim IP, Gateway IP

ii. Show what data transferred from victim IP.

iii. Sow the same data, in Wireshark.

iv. For DNS cache poisoning, show that you browse gmail from victim IP, but it shows a custom page.

v. Steal login data from Victim X login by SSL attack