EC7020: COMPUTER AND NETWORK SECURITY

LAB 06 – NETWORK SECURITY

A.Y.I.D. PERERA
2021/E009
24/09/2025

AIM

Students will learn the fundamental principles of computer and network security by studying attacks on computer systems, networks, and the Web. Students will learn how those attacks work and how to prevent and detect them.

OBJECTIVES:

- To understand Phishing attacks
- To understand tracing and routing
- To understand BGP and Secure BGP.

TASKS

1. Briefly Discuss about phishing attack. Draw flow diagram for initiating a phishing attack.

   Phishing attack is a form of cyber-attack in which adversaries impersonate legitimate and trusted entities in order to deceive victims into revealing sensitive information. The primary objective of such attacks is to obtain confidential data, including authentication credentials, financial details, or to deploy malicious software onto the victim's system. Phishing attacks are typically executed through fraudulent emails, counterfeit websites, or deceptive electronic communications that closely mimic authentic sources. The key characteristics of a phishing attack are adversaries often engage in impersonation, crafting false identities or replicating trusted organizations to establish credibility and evade suspicion. These attacks rely heavily on social engineering, where psychological factors such as trust, fear, or urgency are exploited to manipulate victims into making harmful decisions. In many cases, the attack delivers a malicious payload, redirecting victims to compromised websites, tricking them into downloading malware, or prompting the disclosure of confidential information. The consequences of such attacks can be severe, ranging from identity theft and financial fraud to large-scale data breaches and unauthorized access to critical systems.

   Phishing attacks can take multiple specialized forms. Email phishing relies on fake domain names and urgent messages to trick victims into clicking malicious links, downloading infected files, or disclosing personal information. Spear phishing refines this approach by targeting specific individuals using personal or professional details to increase credibility, often manipulating victims into sensitive actions such as transferring money. Whaling focuses on senior executives and privileged roles, employing highly personalized and subtle messages crafted from publicly available data to extract confidential information. Other variants include smishing and vishing, which exploit SMS or voice communication, with attackers impersonating trusted institutions to solicit payment details or account

credentials. Finally, angler phishing leverages fake social media accounts masquerading as customer support channels to deceive victims into providing sensitive information or visiting malicious sites.
(Phishing Attack - What is it and How Does it Work? - Check Point Software)

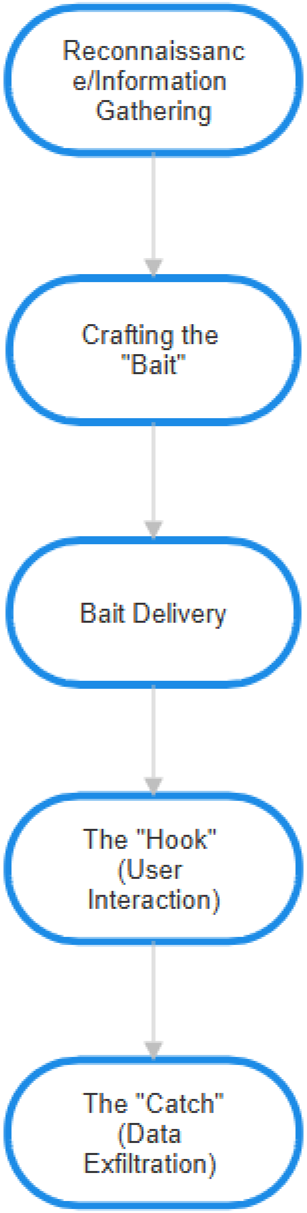

Reconnaissanc e/Information Gathering
Crafting the "Bait"
Bait Delivery
The "Hook" (User Interaction)
The "Catch" (Data Exfiltration)

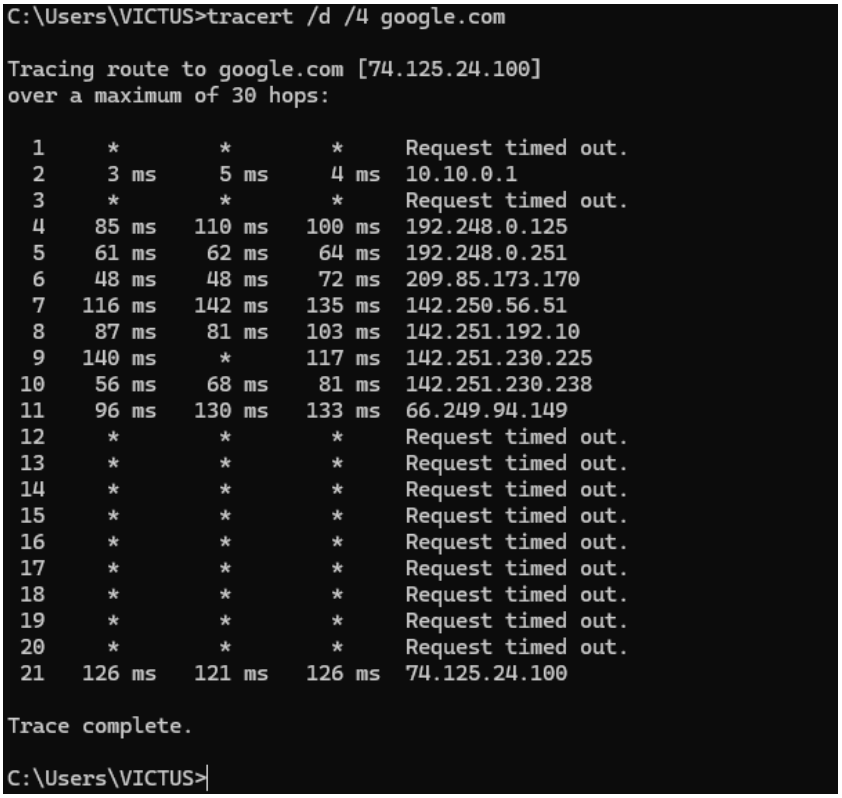
Figure 1: Flow chart for phishing attack

2. Briefly discuss about traceroute.

   Traceroute is a network diagnostic tool available in most OSs that maps the path data packets take from a source host to a destination host across an IP network. It operates by transmitting packets with incrementally increasing Time-To-Live (TTL) values, each intermediate router decrements the TTL by one, and when it reaches zero, the router returns an Internet Control Message Protocol (ICMP) "time exceeded" response. By analyzing these responses, traceroute identifies each hop along the route, providing details such as the router’s IP address, hostname (if resolvable), and the round-trip time (RTT) required for the packet to reach that hop and return. This process continues until the packet reaches the final destination or the maximum hop count is exceeded. Traceroute is commonly employed for diagnosing network latency, identifying routing bottlenecks, and detecting points of failure in end-to-end communication. (traceroute - Wikipedia)

3. Trace a website with IPv4 and another website with IPV6 then explain the routes.

   IPv4



```
C:\Users\VICTUS>tracert /d /4 google.com

Tracing route to google.com [74.125.24.100]
over a maximum of 30 hops:

  1     *        *        *     Request timed out.
  2     3 ms     5 ms     4 ms  10.10.0.1
  3     *        *        *     Request timed out.
  4    85 ms   110 ms   100 ms  192.248.0.125
  5    61 ms    62 ms    64 ms  192.248.0.251
  6    48 ms    48 ms    72 ms  209.85.173.170
  7   116 ms   142 ms   135 ms  142.250.56.51
  8    87 ms    81 ms   103 ms  142.251.192.10
  9   140 ms     *      117 ms  142.251.230.225
 10    56 ms    68 ms    81 ms  142.251.230.238
 11    96 ms   130 ms   133 ms  66.249.94.149
 12     *        *        *     Request timed out.
 13     *        *        *     Request timed out.
 14     *        *        *     Request timed out.
 15     *        *        *     Request timed out.
 16     *        *        *     Request timed out.
 17     *        *        *     Request timed out.
 18     *        *        *     Request timed out.
 19     *        *        *     Request timed out.
 20     *        *        *     Request timed out.
 21   126 ms   121 ms   126 ms  74.125.24.100

Trace complete.

C:\Users\VICTUS>
```

Figure 2: IPv4 trace

Command/options: tracert /d /4 google.com

/4 forces IPv4.
/d disables reverse-DNS, so you see only IPs (no hostnames).
Windows tracert sends ICMP Echo with increasing TTL; each router that decrements TTL to 0 should return ICMP Time Exceeded.

Hop 1 → * * * Request timed out.

The first L3 device on the segment didn't send a TTL-expired reply (common: home/enterprise gateways silently drop TTL-expired/ICMP or rate-limit it).

Intermediate routers do not always respond consistently to probes. Many home gateways, enterprise firewalls, and ISP edge devices are configured to silently discard packets when their Time-To-Live (TTL) expires or to rate-limit ICMP Time Exceeded messages. This behavior is intentional: routers are optimized primarily for forwarding user traffic, and generating diagnostic ICMP responses is treated as a low-priority task. As a result, certain hops may appear as "request timed out" in traceroute output, even though data packets continue to traverse the path normally without disruption.

Hop 2 → 10.10.0.1 (3–5 ms)

Default gateway (RFC1918/private). This is the NAT device handing the traffic upstream toward the ISP.

Hop 3 → timeout

Likely the ISP's first aggregation/edge node suppressing TTL-expired ICMP (or rate-limited). Core/edge devices often deprioritize ICMP control-plane responses.

Hops 4–6 → public transit toward Google

192.248.0.125 / 192.248.0.251 then 209.85.173.170.

These are upstream/transit and then a Google edge/peering IP (209.85/142.250/66.249/74.125 are Google address blocks). RTT rises to ~48–110 ms as packet leave the access network.

Hops 7–11 → inside Google (AS15169) backbone

142.250.56.51, 142.251.192.10, 142.251.230.225, 142.251.230.238, 66.249.94.149.

Traversing Google's internal network toward the serving front end. Variability (56–142 ms) reflects different queues/paths and per-hop ICMP handling.

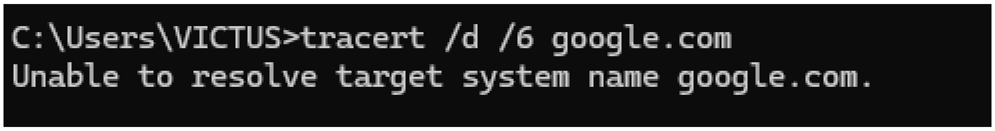
Hops 12–20 → timeouts

Intermediate routers did not respond (policy, ACL, or ICMP rate-limit

Hop 21 → 74.125.24.100 (~121–126 ms) — Trace complete

Final destination replied with ICMP Echo Reply. End-to-end reachability is good; ~120–130 ms is the round-trip latency to that Google anycast endpoint from the network.

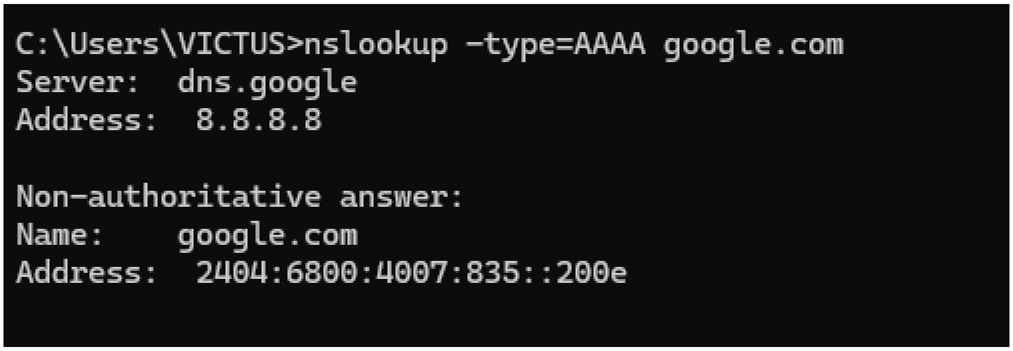
<u>IPv6</u>



```
C:\Users\VICTUS>tracert /d /6 google.com
Unable to resolve target system name google.com.
```

Figure 3: IPv6 trace

Traceroute failed: Unable to resolve target system name google.com



```
C:\Users\VICTUS>nslookup -type=AAAA google.com
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:    google.com
Address:  2404:6800:4007:835::200e
```

Figure 4: Troubleshooting IPv6 connectivity

Used nslookup -type=AAAA google.com command to check if the DNS can resolve IPv6 address to google.com. According to the response, DNS is working but the network can’t route to them. ISP has not enabled IPv6.

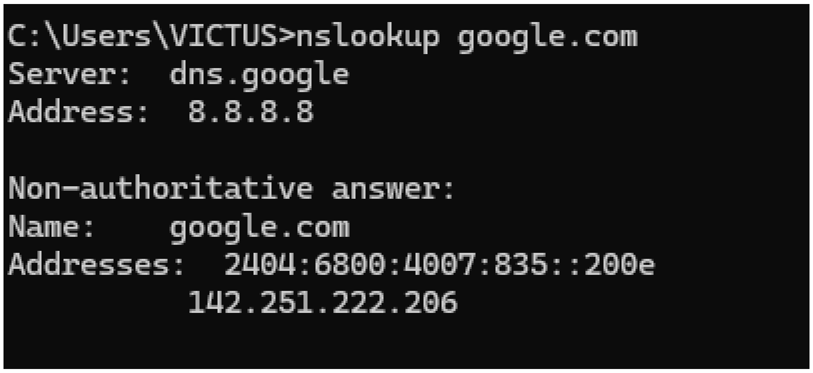
4. Briefly explain what is DNS lookup and MX lookup

A DNS lookup is the process of resolving a human-readable domain name (e.g., google.com) into its corresponding IP address so that network clients can locate and communicate with the correct server. It involves querying the Domain Name System (DNS), which may contact recursive resolvers, authoritative servers, or cached records to return the correct mapping.

An MX lookup (Mail Exchange) is a specific type of DNS query used to identify the mail servers responsible for accepting email messages on behalf of a domain. MX records not only list the mail servers but also define their priority values, ensuring that email delivery systems know the correct and most efficient route for message transmission.

5. Check DNS lookup and MX lookup for the same web sites used in "3" then report what are the useful information use found.

DNS Lookup

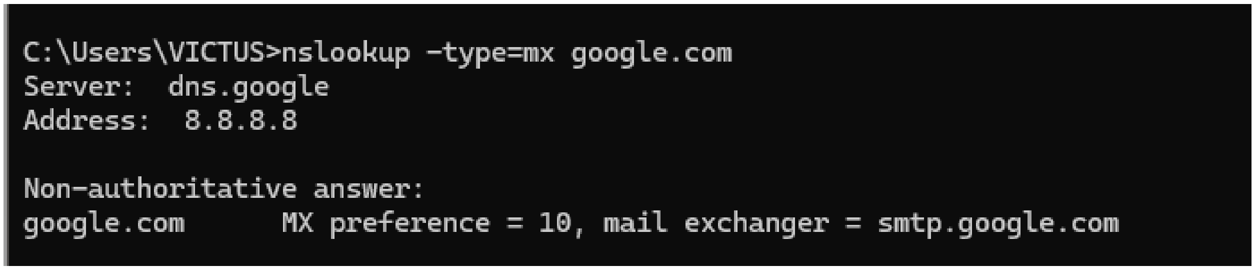


```
C:\Users\VICTUS>nslookup google.com
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:    google.com
Addresses:  2404:6800:4007:835::200e
          142.251.222.206
```

Returns the IPv4 addresses and possibly IPv6 addresses associated with google.com. It identifies the server IPs that clients will connect to when accessing the website and confirms whether the domain supports both IPv4 and IPv6 connectivity. It also helps in troubleshooting network reachability issues.

MX Lookup



```
C:\Users\VICTUS>nslookup -type=mx google.com
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
google.com      MX preference = 10, mail exchanger = smtp.google.com
```

Returns the mail servers responsible for handling email for the domain, along with priority values. It reveals the infrastructure handling email delivery for the domain and priority values show which servers will be tried first, ensuring reliable email routing. It helps administrators verify if a domain is using secure or external mail services

6. Explain Border Gateway Protocol (BGP)

The Border Gateway Protocol is the core routing protocol of the Internet that enables data exchange between different autonomous systems (AS), which are large networks or collections of networks under a common administrative domain such as ISPs, data centers, or large enterprises. Border Gateway Protocol is classified as a path vector protocol, meaning it makes routing decisions based on network paths, policies, and rules rather than simply on shortest distance.

When two BGP routers known as peers establish a connection, they exchange information about the networks (prefixes) they can reach. Each advertised route contains an autonomous systems path, which is a list of autonomous systems the route has traversed. Routers then use this path information, along with configurable attributes such as local preference, MED, route filtering, to select the best path to a destination.

BGP operates over TCP port 179 to ensure reliable session management. There are two main types of BGP as External BGP (eBGP) which is used between different autonomous systems and Internal BGP (iBGP) which is used within a single AS to distribute external route information internally.

Because BGP is policy-driven, it gives network operators fine-grained control over routing decisions, supporting load balancing, traffic engineering, and route prioritization. The flexibility also makes BGP complex and sometimes vulnerable to misconfigurations or attacks such as route hijacking.

7. Explain Secure Border Gateway Protocol (sBGP)

The Secure Border Gateway Protocol (sBGP) is a security extension to the standard Border Gateway Protocol (BGP) designed to address vulnerabilities such as route hijacking, prefix spoofing, and misconfigurations that threaten the stability of Internet routing. Standard BGP does not include strong authentication or integrity checks, which allows malicious or accidental announcements of incorrect routes. sBGP introduces cryptographic mechanisms to ensure that routing information is both authentic and verifiable. sBGP integrates with a Public Key Infrastructure (PKI) to validate three key elements as Origin Authentication which verifies that an Autonomous System (AS) is authorized to advertise a particular IP prefix. AS Path Validation which ensures that each AS listed in the path actually forwarded the route advertisement, preventing insertion or modification of false paths and message Integrity that uses digital signatures to protect BGP update messages from tampering in transit.

This allow sBGP to provide stronger trust in inter-domain routing decisions, significantly reducing the risk of malicious attacks such as BGP hijacking. eBGP deployment has been limited due to the complexity of establishing a global PKI, increased computational overhead for cryptographic verification, and the challenge of incremental adoption across thousands of autonomous systems

DISCUSSION

During this laboratory exercise, the fundamental concepts of computer and network security were explored through practical demonstrations. Phishing attacks were studied first, highlighting how attackers use deceptive techniques such as fake websites, fraudulent emails, and social engineering tactics to extract sensitive information. The analysis showed that phishing remains one of the most common and effective attack vectors because it exploits human behavior rather than technical weaknesses. Different variants, including email phishing, spear phishing, and website forgery, were reviewed to understand their mechanisms and potential countermeasures.

Hands-on experiments with tracing and routing provided practical insights into how network traffic travels from a source to a destination. The use of the tracert command demonstrated how packets traverse multiple hops, moving through local gateways, ISP infrastructure, and eventually reaching servers hosted by global service providers. The presence of timeouts at certain hops was observed, which is a normal result of routers suppressing or rate-limiting ICMP responses. DNS and MX lookups were also performed to identify the IP addresses and mail exchange servers associated with specific domains. These results showed how DNS infrastructure supports both web communication and email routing, and how such information is useful in troubleshooting and security analysis.

The concepts of Border Gateway Protocol (BGP) and Secure BGP (sBGP) were then studied to understand routing at the inter-domain level. BGP was identified as the backbone protocol that enables communication between autonomous systems on the Internet. However, its vulnerabilities, such as route hijacking and prefix spoofing, were also examined. The extension sBGP was introduced as a cryptographic enhancement designed to provide origin authentication, path validation, and message integrity. Although effective in theory, the challenges of deployment were recognized, particularly the requirement for a global Public Key Infrastructure and the associated overhead.

CONCLUSION

The experiments confirmed phishing as a major threat and demonstrated the practical use of tracing, routing, and DNS analysis in understanding Internet communication. BGP's role in global routing and its weaknesses were recognized, while sBGP was identified as a potential but difficult-to-deploy solution. The objectives of the lab were successfully met, reinforcing both theoretical knowledge and practical skills in network security.