# CSCI369 Ethical Hacking

## Lecture 3-2 More on MITM with SSL Strip, DNS Attacks and NAT

A/Prof Joonsang Baek

School of Computing and Information Technology

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

# Protection against eavesdropping using MITM

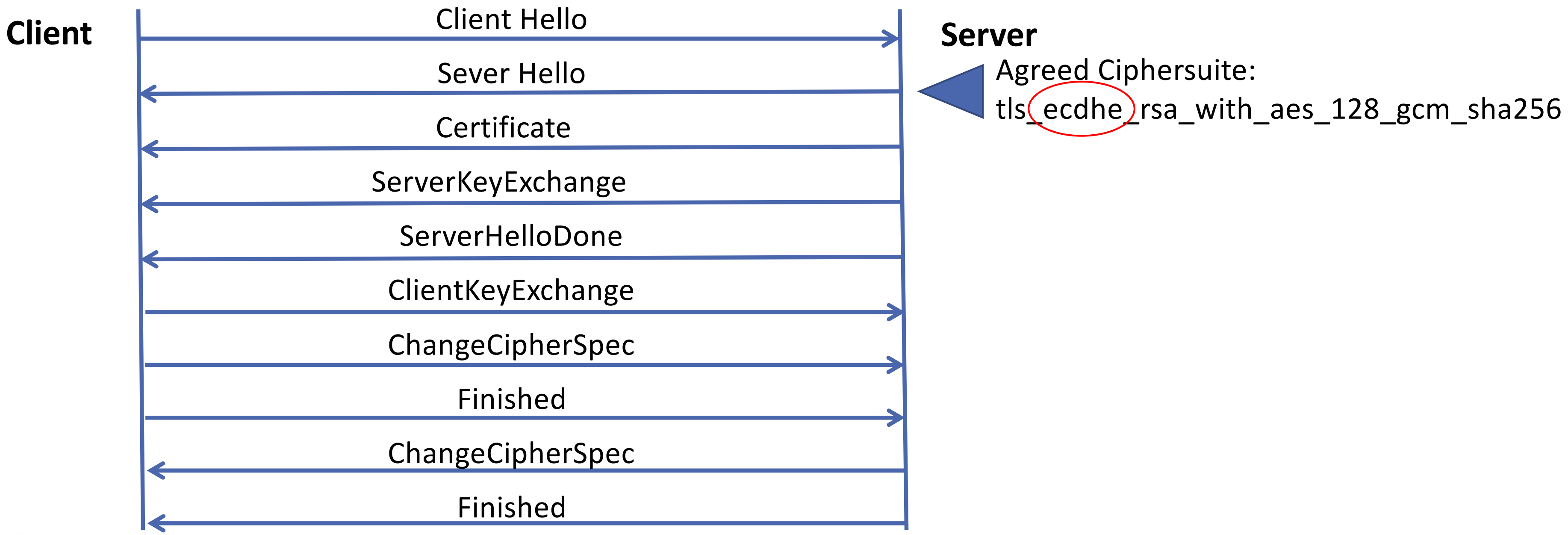
- The end-to-end encryption can be an effective solution against eavesdropping using MITM attacks.
  - ➢The end-to-end encryption successfully prevents the adversary from accessing the data in the middle.
  - ➢Even if all the data transmitted between the server and the target are captured, the attacker still cannot decrypt the data.
  - ➢The popular and most common end-to-end encryption is the SSL/TLS. However, insecure settings can give an opportunity to the attacker to compromise the target's security.
  - ➢This is a widely researched topic since the most popular websites enforce the TLS to their users.

# TLS (Transport layer Security)

- Data encryption over the network is an upward trend.
  - ➢According to the Google transparency report (https://transparencyreport.google.com/https/overview?hl=en), the percentage of HTTPS page loadings (in the Chrome browser) increases from 67 percent in May 2017 to 91 percent in July 2019 in the United States.
- Among the top 100 non-Google sites on the Internet, which account for about 25 percent of all website traffic worldwide, 96 websites support HTTPS and 90 websites set HTTPS as default.

# TLS (Transport layer Security)

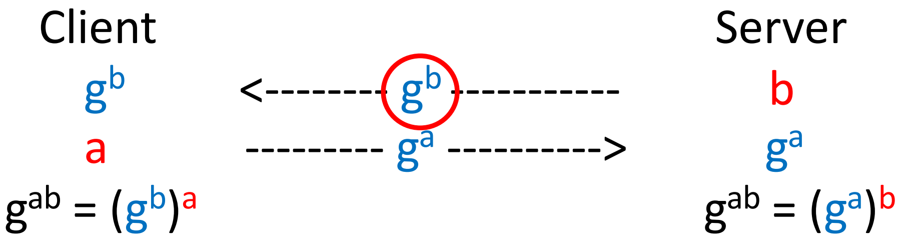
- TLS Handshake



Agreed Ciphersuite:
tls_ecdhe_rsa_with_aes_128_gcm_sha256

# TLS Handshake

- Key Exchange Protocol
  - DH (Diffie-Hellman) and ECDH: Its security is based on the discrete logarithm problem in Finite Groups (DH) or over Elliptic Curves (ECDH).



| Client |  | Server |
|---|---|---|
| $g^b$ | <-------- $\boxed{g^b}$ ----------- | $b$ |
| $a$ | --------- $g^a$ ----------> | $g^a$ |
| $g^{ab} = (g^b)^a$ |  | $g^{ab} = (g^a)^b$ |

(a and b are private keys; $g^a$ and $g^b$ are public keys)

  - DHE and ECDHE: “E” means ephemeral. In DH and ECDH, server’s public key ($g^b$) is fixed, but DHE and ECDHE, $g^b$ is generated on-the-fly.

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

# TLS Handshake

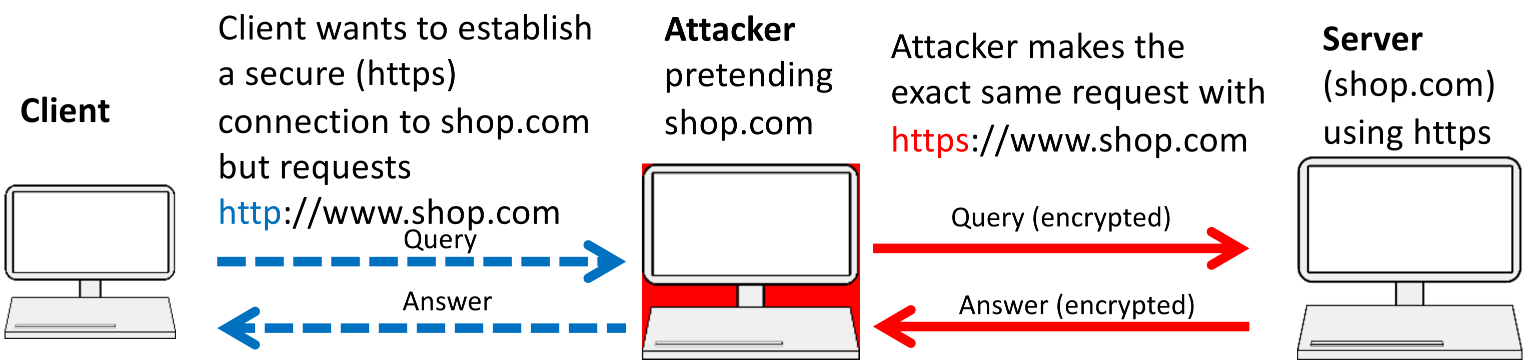
- In the end-to-end encryption, the secret parameters are not delivered in the traffic in a plaintext.
- In (EC)DH(E), the attacker can read $g^a$ and $g^b$. Note that it is very hard to compute $a$ or $b$ from $g^a$ and $g^b$ due to discrete logarithm problem.
- However, insecure settings enable the attacker to compromise the privacy of the target. → MITM

# SSL Strip

- Concept
  - ➢Users (clients) do not explicitly type https:// when they enter URL on the browser, e.g., www.shop.com (without specifying a protocol).
    - ✓If this happens, the website usually redirect that request to the secure https server https://www.shop.com (302 redirect directive)
    - ✓Then the user's browser connects to that https site.
  - ➢SSL strip is an MITM attack that makes use of this user behaviour: Users do not directly connect to the site with https but non-https, i.e., http. The attacker then captures the client's request acts as a proxy between the user and the secure https server.

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

# SSL Strip



Client wants to establish a secure (https) connection to shop.com but requests http://www.shop.com

**Attacker** pretending shop.com

Attacker makes the exact same request with https://www.shop.com

**Server** (shop.com) using https

- The attacker sends the (captured) queries from the client to the server through the TLS channel between him and the server. (The queries will be encrypted.)
- The attacker decrypts the encrypted queries  from the server and relay the decrypted results (answers) to the client.

# SSL Strip

- The automated SSL strip tool was developed by Moxie Marlinspike in 2009.
- What is the benefit to the attacker maintaining the http connection?
  - ➢The attacker can capture every data from the client as they are not encrypted.
- Possible prevention methods
  - ➢User awareness: If possible, type the full https URL, e.g. https://www.shop.com

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

# SSL Strip

- Possible prevention methods (continued)
  - ➢HSTS (HTTP Strict Transport Security)
    - ✓It instructs browser that shop.com should always be HTTPS.
  - ➢HSTS preloading
    - ✓The problem is the very first time the client has typed http://site , there could be a chance that the 302 redirection directives have not yet provided to the client's browser. → SSL strip can happen
    - ✓Solution: The client's browser preloads the static list of websites that no matter what should always be visited over https (even on the first visit).
  - ➢You can check your HSTS setting of your chrome browser by navigate to https://www.chromium.org/hsts/

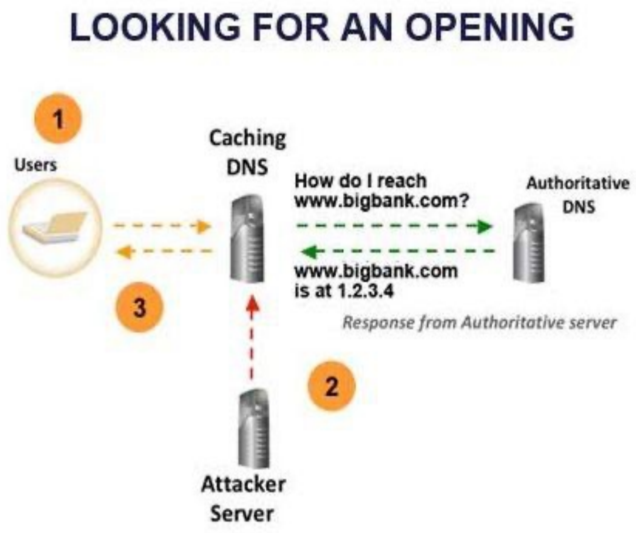
UNIVERSITY OF WOLLONGONG AUSTRALIA

# Domain Name System (DNS)

- The DNS is used for translating hostnames into IP addresses and vice versa.
  - ➢All internet working applications require DNS to function.
- DNS makes use of  a hierarchical naming scheme: Queries work in a top-down manner, beginning at the top of the DNS tree and working their way down. (Root → TLD → Authoritative)
- Traditional firewalls leave port 53 open for DNS queries. It is difficult to protect against DNS-based DDoS attack such as amplification and reflection. Therefore, it becomes a primary target to slow down or disable the target network.

# Domain Name System (DNS)

- How DNS works
  - ➢Normally, if a DNS server does not know a requested translation, it will ask another DNS server, and the process continues recursively.
  - ➢To increase performance, a DNS server will typically remember these translations for a certain amount of time in the DNS records. This means if it receives another request for the same translation, it can reply without needing to ask any other servers until that record expires.


LOOKING FOR AN OPENING
1
Users
Caching DNS
How do I reach www.bigbank.com?
Authoritative DNS
www.bigbank.com is at 1.2.3.4
3
Response from Authoritative server
2
Attacker Server

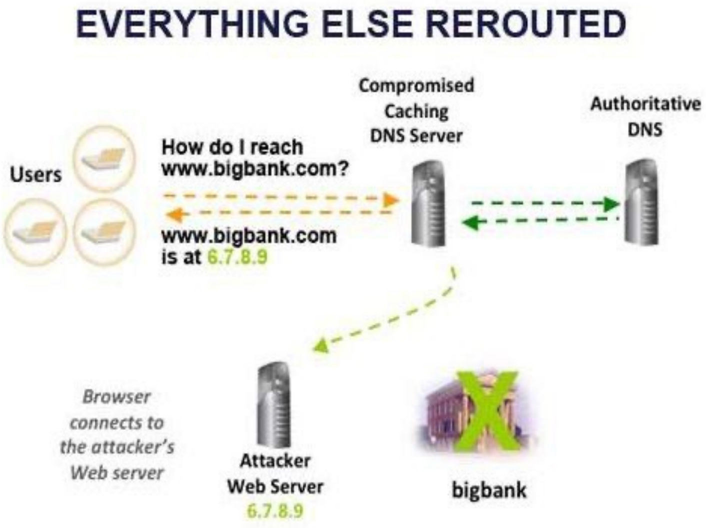
UNIVERSITY OF WOLLONGONG AUSTRALIA

# DNS Records

- A Record
  - ➢The "A" stands for "address" and this is the most fundamental type of DNS record: it indicates the IP address of a given domain.
- CNAME
  - ➢A "canonical name" (CNAME) record points from an alias domain to a "canonical" domain. A CNAME record is used instead of an A record, when a domain or subdomain is an alias of another domain.
  - ➢All CNAME records must point to a domain, never to an IP address.

# DNS Attacks

- Attack 1: DNS Poisoning (DNS Spoofing)
  - ➢Attacker breaks into a local DNS server and modifies the DNS record so that it can return an incorrect IP address, diverting traffic to another computer.
  - ➢Here, we say the DNS record is poisoned. → This modified record gives the victim a false translation of hostnames.


EVERYTHING ELSE REROUTED
Users
How do I reach www.bigbank.com?
Compromised Caching DNS Server
Authoritative DNS
www.bigbank.com is at 6.7.8.9
Browser connects to the attacker's Web server
Attacker Web Server 6.7.8.9
bigbank

# DNS Attacks

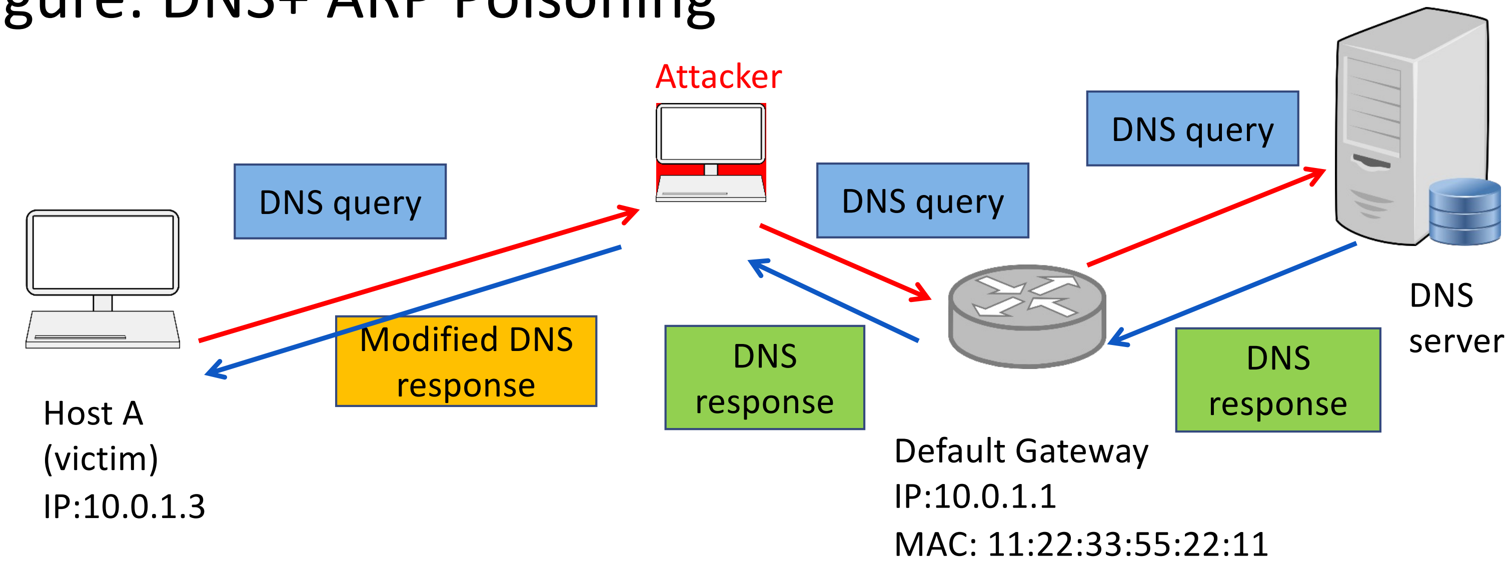
- ➢The attacker can redirect users from a website to the one they own.
  - ✓Attacker spoofs the IP address/DNS entries for a target website on a given DNS server and replaces them with the IP address of a server under their control.
  - ✓Usually, the server under the  attacker's control has been infected by malware.
  - ✓This technique can also be used for phishing attacks, where a fake version of a genuine website is created to collect personal details such as bank and credit card details.

# DNS Attacks

- ➢Example: DNS Poisoning with MITM
  - ✓MITM attacker captures a DNS response from the DNS server and replaces it with a modified one so that the DNS response will result in forcing the victim to visit the attacker's server.
  - ✓One example is a combination of DNS spoofing and MITM (such as ARP poisoning).

# DNS Attacks

- Figure: DNS+ ARP Poisoning



# DNS Attacks

- Attack 2: Subdomain takeover
  - ➢A process of registering a non-existing domain name to gain control over another domain
  - ➢Idea
    1) Assume that the attacker targets `ethicalhacking.com`.
    2) The attacker found that `code.ethicalhacking.com` uses a CNAME record to refer to third-party service domain, e.g., `ethicalhacking.github.io`.
    3) The ethicalhacking.com admin decides to delete the GitHub account associated with `ethicalhacking.github.io`.
    4) The problem is if the CNAME record is not deleted from `ethicalhacking.com`'s DNS server, the attacker who creates a new GitHub account with `ethicalhacking.github.io` will have a full control over `code.ethicalhacking.com`.

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

# DNS Attacks

- Attack 3: DNS Tunnelling
  - An attacker's malware in the victim's machine wants to transfer data from it to the attacker's server (i.e. The attacker tries data exfiltration).
  - If the attacker uses a ftp, for example, it will be detected by the victim's firewall.
  - The attacker acquires some domain such as `attacker.com` and runs local DNS server.
  - The malware in the victim's machine makes DNS queries of the form <data>.attacker.com, where <data> is the data the attacker wants to exfiltrate.

# DNS Attacks

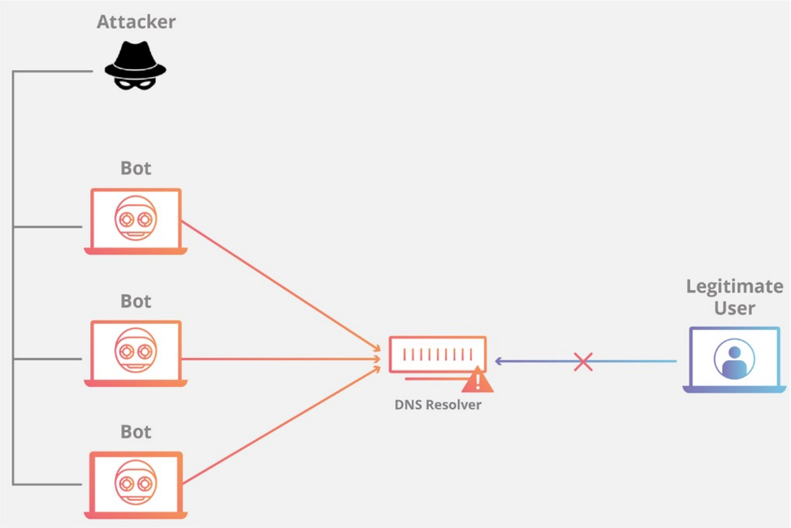
- ➢If the query reaches the attacker's DNS server, the DNS response will be sent to the victim's machine.

- What is the problem?
  - ➢DNS query/response is completely legitimate, going through port 53.
  - ➢This enables the attacker's malware to bypass firewall. → It makes covert data exfiltration possible!

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

# DNS Attacks

- Attack 4: DNS flood attack
  - ➢DNS flood is a type of Distributed Denial of Service (DDoS) attack where the attacker targets one or more DNS servers belonging to a given zone, attempting to impede resolution of resource records of that zone and its sub-zones.



source: https://www.cloudflare.com/learning/ddos/dns-flood-ddos-attack/

# DNS Attacks

- ➢This attack attempts to exhaust server-side assets (e.g., memory or CPU) with a flood of UDP requests, generated by scripts running on several compromised botnet machines.
  - ✓These scripts send malformed packets from spoofed IP addresses.

- ➢Since DNS servers *rely on the UDP protocol* for name resolution, a full communication circuit is never established unlike TCP queries and flooding is more easily accomplished: The attacker can send packets that are neither accurate nor even correctly formatted.

# DNS Attacks

- Attack 5: DNS amplification attack
  - ➢The attacker obtains a victim’s IP address.
  - ➢The attacker identifies a website with large number of DNS records.
  - ➢The attacker crafts fake DNS queries for the host with a large amount of DNS data with the victim’s IP (as a receiver) so that DNS responses with the large number of DNS records are returned to the victim.
  - ➢The victim’s machine cannot handle the large amount of DNS responses. → The machine is down.

# NAT (Network Address Translation)

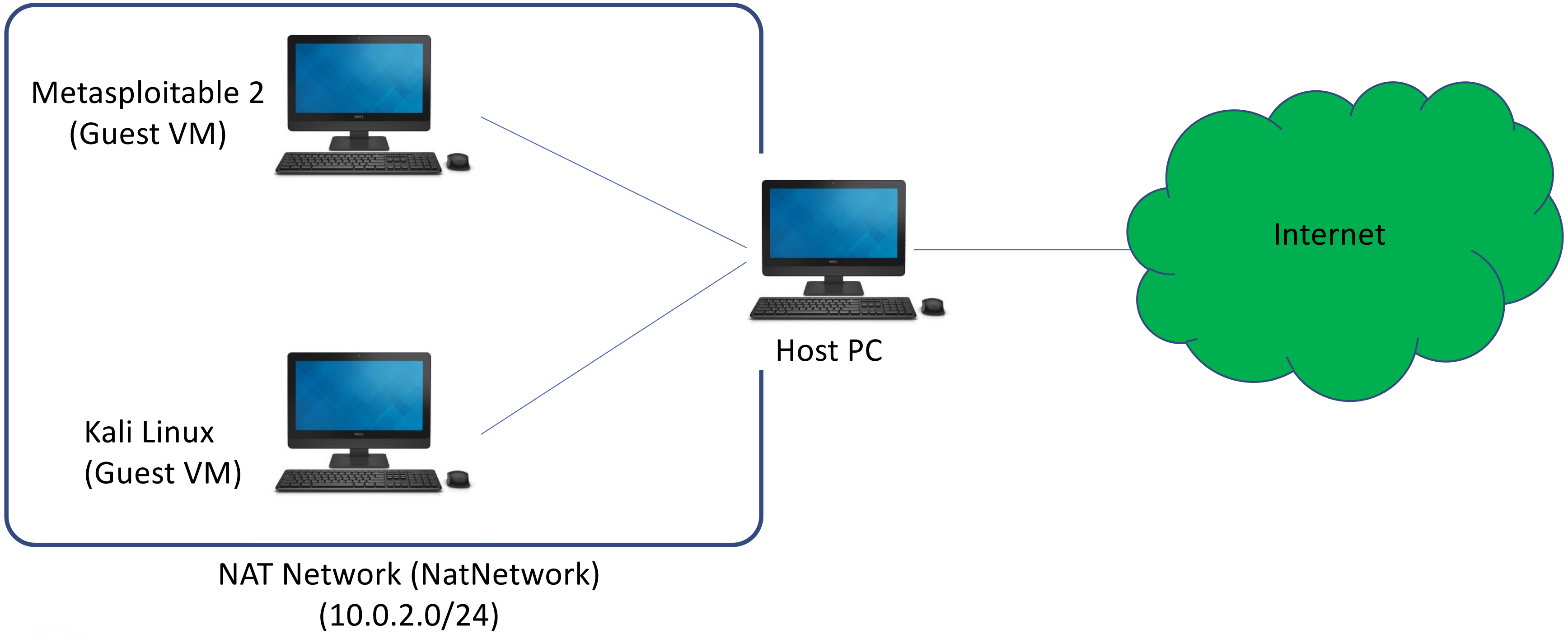
- What is NAT?
  - ➢Network Address Translation (NAT) is designed for IP address conservation. It enables private IP networks that use unregistered IP addresses to connect to the Internet.
  - ➢NAT operates on a router, usually connecting two networks together, and translates the private (not globally unique) addresses in the internal network into legal addresses, before packets are forwarded to another network.

# NAT vs NAT Network in VB

- NAT
  - ➢The VM (Kali) can use the network of the host machine (Windows).
  - ➢The VM (Kali) cannot access to other VMs using NAT interface.
- NAT Network
  - ➢The VM (Kali) can use the network of the host machine (Windows).
  - ➢The VM (Kali) can access to other VMs using the same NAT Network interface.
- If you are developing a server and a client using two different VMs in a single host machine and want to test them through the network, you should use NAT Network.

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

# NAT Network in VB



# UTM

- On UTM, “Shared Network” = “Nat Network”

UNIVERSITY
OF WOLLONGONG
AUSTRALIA