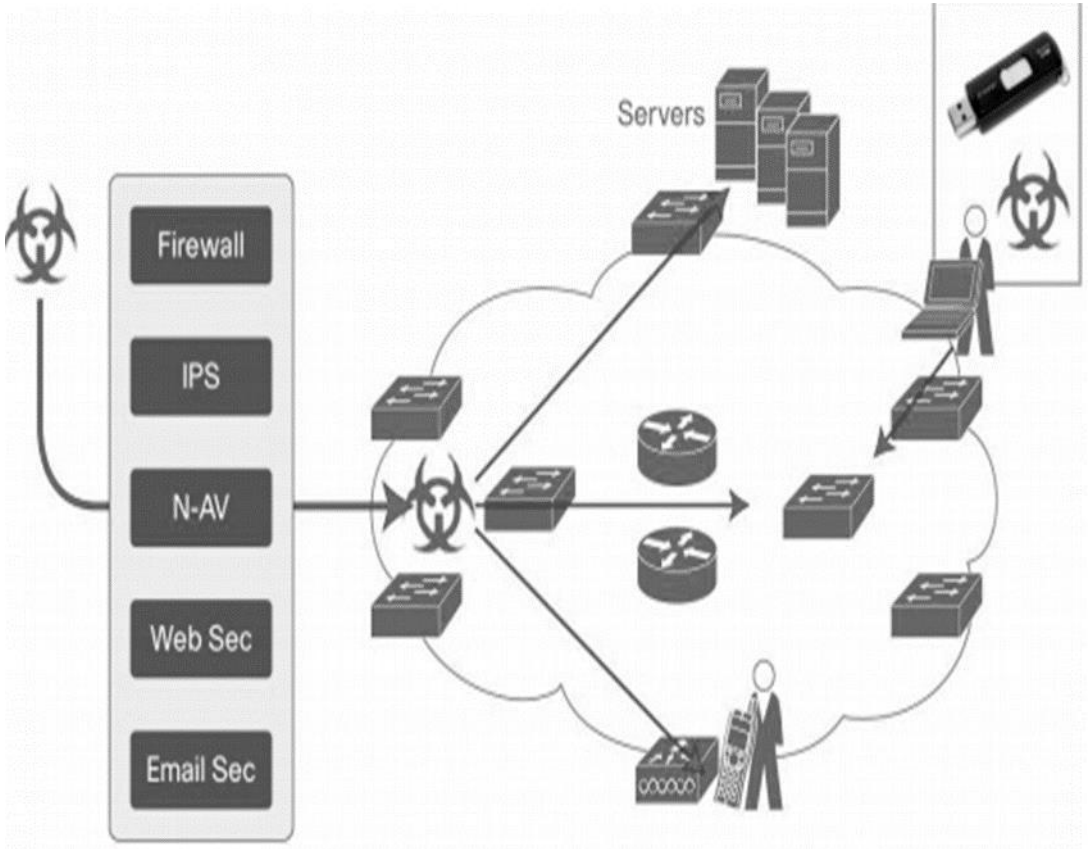
Day 5
Network Hacking

System Hacking (1/2)

- After completing first three phases.
  - Footprinting, Scanning, Enumeration.
- Process become much more complex.
  - Not a single pass.
  - Multiple trials and errors needed.
- More methodical approach.
  - Cracking password & Encryption, Escalating privileges, Running malware, Hiding applications, Covering tracks, Hiding evidence, etc.

System Hacking (2/2)

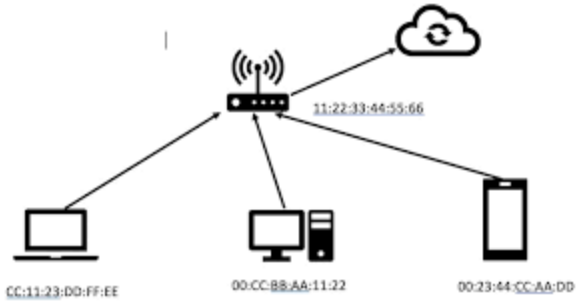
- Pre-connection attacks.
  - We aren't connected to the target network/system.
  - Gaining access is the priority.
  - Wi-Fi access point, fake access point, Social engineering & Malware.
  - Post-connection attacks.
- After connecting to the network (now within the perimeter).
  - Explore all the clients that are connected to a system.
  - MITM of communication.
  - Privilege escalation.



https://www.cisco.com/c/dam/en_us/solutions/industries/docs/gov/cyber_threat_defense_so.pdf

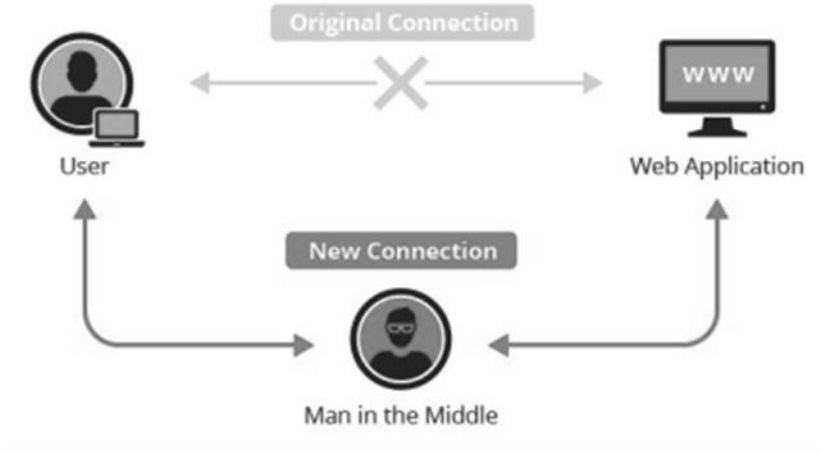
Pre-connection: Access via WiFi

- We will connect to the network.
  - To launch more powerful attacks.
- If no encryption → we can just connect to it.
- If the network is wired → use a cable & change the MAC
- If target use encryption → Break it!.
  - WEP → collect a large number of IVs (Initialization Vector).
    - random number in plain text, statistical attack to find the key.
  - WPA/WPA2 → each packet is encrypted using a unique key.
  - The number of packets is irrelevant, only four-way handshake packets are useful.
  - Can use a wordlist using the aircrack-ng to compare MIC.
- Read more at https://www.javatpoint.com/pre-connection-attacks



Post-connection: MITM

- Useful for passive online attacks
  - Packet sniffing
    - Capture within a single collision domain
      - If a switch→ you won't see traffic from the target in passive way
  - Vulnerable protocols
    - HTTP, Telnet, FTP, rlogin, SNMPv1
      - Anything send credentials in clear text
  - Exploits design weaknesses
    - E.g. ARP poisoning, DNS poisoning
- Tools
  - MITMf, SSL Strip, Burp Suite, BeEF, Ettercap, Bettercap




```
\Users\IEUser>arp -a

Interface: 192.168.1.69 --- 0x13
  Internet Address      Physical Address      Type
  192.168.1.1           e4-48-c7-5d-aa-1f     dynamic
  192.168.1.11          00-c0-ca-6c-ca-12     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

ARP Table – Before

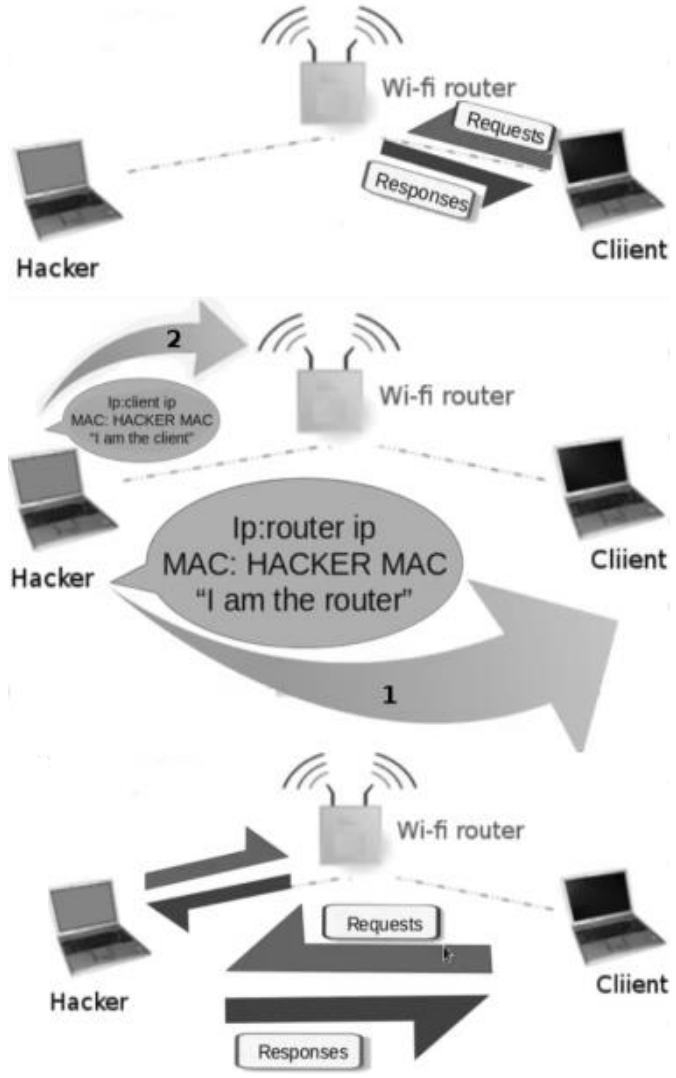
```
\Users\IEUser>arp -a

Interface: 192.168.1.69 --- 0x13
  Internet Address      Physical Address      Type
  192.168.1.1           00-c0-ca-6c-ca-12     dynamic
  192.168.1.11          00-c0-ca-6c-ca-12     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

ARP Table – After

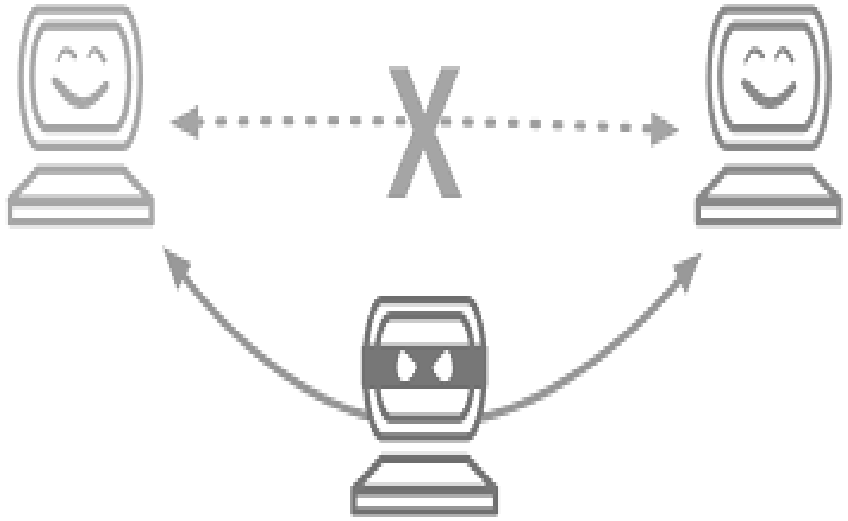
MITM: ARP Poisoning

- Ethernet devices refer to an ARP table (ARP cache) in the RAM to find the MAC address that is mapped to the IPv4 address
- ARP security issues
  - Each ARP request/response is trusted, client accepts responses even not requested
  - Can be exploited to redirect the flow of packets
    - First send an ARP response to the client saying that device with the router IP has my MAC address
    - Then send an ARP response to the router saying that device with the client IP has my MAC address
    - My (attacker) device in the middle
    - Every packets going to/from client to router will go through my device
- Read more https://www.javatpoint.com/man-in-the-middle-attacks



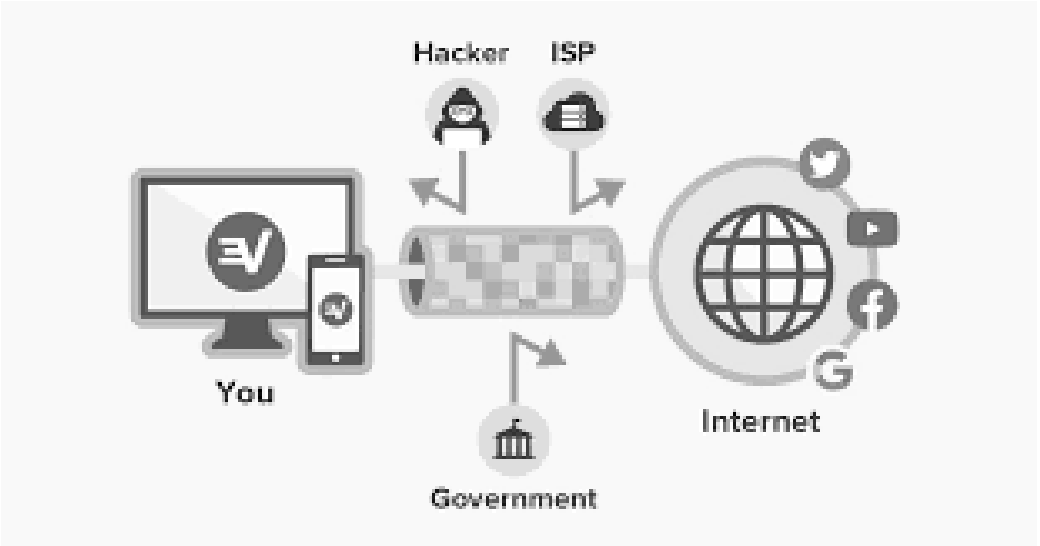
Bypassing HTTPS

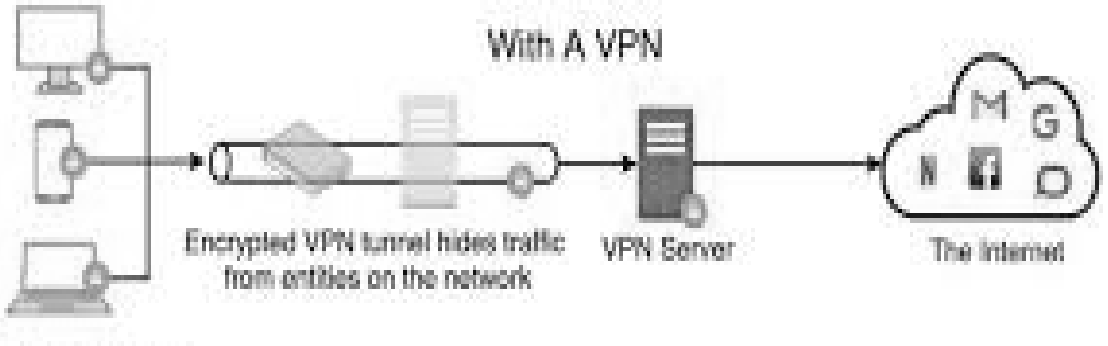
- Packets sent over HTTP requests can be read.
  - User credentials and other information visible.
- Transport Layer Security (TLS)/SSL introduced.
  - Data is encrypted - we are encrypting payload but not all layers.
  - Still IP address, domain information can be found.
  - DNS spoof attacks.
- SSLstrip to downgrade HTTPS → HTTP.
  - HSTS → pre-hardcoded list of websites in the browser.



MITM Countermeasures

- Analyse ARP table.
  - e.g. XARP http://www.xarp.net/#download
  - Wireshark.
- Encrypt traffic.
  - HTTPS Everywhere extension.
  - https://chrome.google.com/webstore/detail/https-everywhere/gcbommkclmclpchllfjekcdonpmejbdp?hl=en-GB
  - Only work with HTTPS site.
- Use VPN + SSL.
  - Protection from most MITM attacks.





Password Cracking (1/3)

- Obtain the credential of a given account from.
  - Transmitted, stored or processed data.
- Can use usernames collected at enumeration phase.
- Weak passwords.
  - Only numbers, only letters, proper names, dictionary words, short passwords, etc.
- Multi-factor authentication.
  - Smart cards, biometrics, RSA token, etc.

Password Cracking (2/3)

- Dictionary attacks.
  - Uses a list of known words including the entire dictionary.
- Brute force attacks.
  - Every possible combination of characters.
- Hybrid attacks.
  - Build on the dictionary attack, but modified with special characters
  - Eg. P@ssw0rd).
- Rule based attacks.
  - Assume user has created the password according to a certain policy.

Password Cracking (3/3)

- Passive online attacks.
  - Sitting back and listening (Eg. using Wireshark, Man in the middle attacks).
- Active online attacks.
  - Actively engage (Eg. password guessing, Trojan/spyware/key loggers, phishing).
- Offline attacks.
  - Try to exploit the way passwords are stored.
- Nonelectronic attacks.
  - Shoulder surfing, social engineering, dumpster diving.

Rainbow Tables

- Pre-compiled hashes in a Database.
- Creating a Rainbow table.
  - Compute every possible combination of characters with hash values.
  - Taking a significant amount of time.
  - Tool: winrtgen.exe.
- Extracting Hashes from a System.
  - Password are not stored in clear text.
  - Instead in a hashed format, can be extracted.
  - Tool: pwdump7.exe.
- Working with Rainbow crack.
  - Compare the captured hash to the ones in the Database.
  - Allows revealing the password in a few moments.
  - Tool: rcrack_gui.exe.
- Salting a hash.
  - Can reduce the speed of the crack.

Malware (1/3)

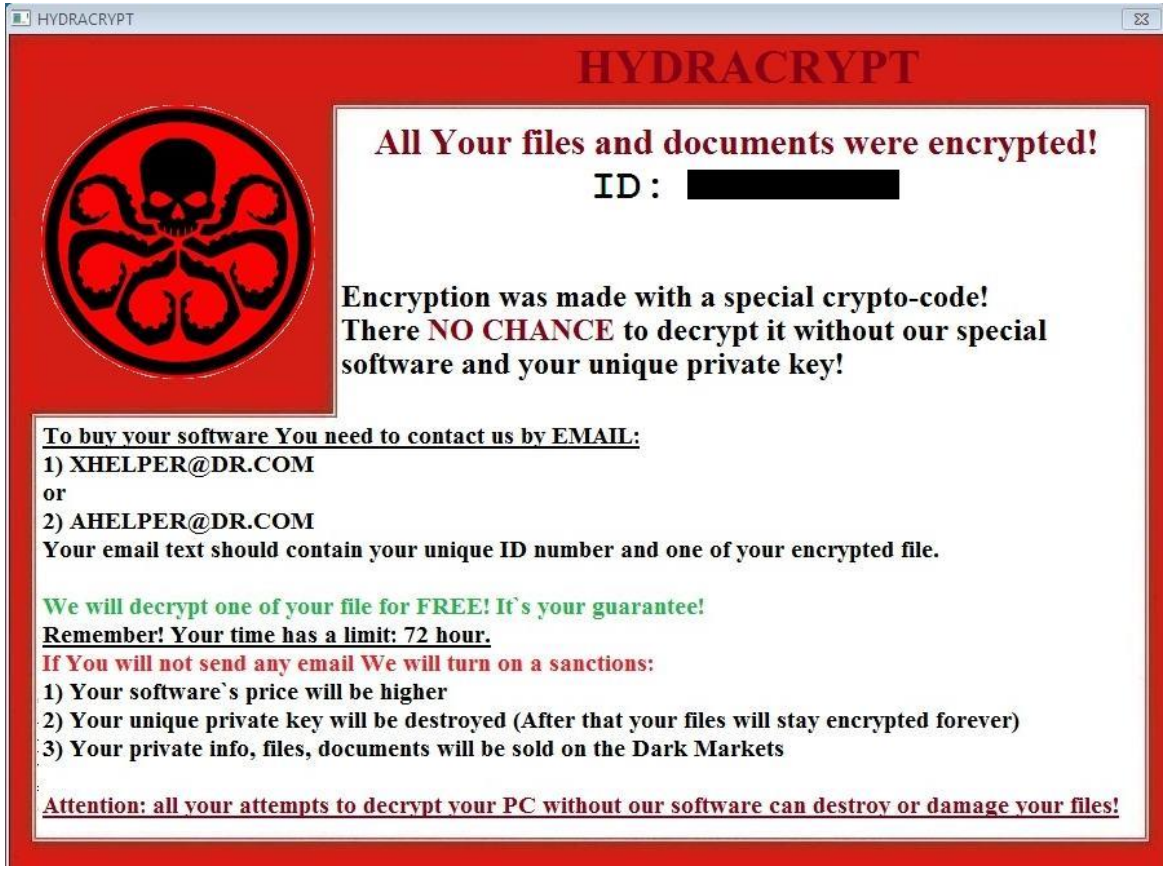
- **Adware**
  - The least dangerous, most lucrative Malware, displays ads on your PC.
- **Spyware**
  - Software spies on you, tracking your internet activities.
- **Virus**
  - Piece of code attaches to legitimate software.
  - Reproduces itself when the legit software is run.
  - Spread by sharing software or files between computers.
- **Trojan**
  - Misleads users of its true intent, generally spread by some form of social engineering.
  - Try to access users' personal information, e.g. banking information, passwords, personal identity.
  - Generally, do not attempt to inject/propagate themselves.

Malware (2/3)

- **Worm**
  - Replicates itself and destroys data and files on the computer.
  - “Eat” the system operating files and data files.
- **Rootkit**
  - Hidden deep inside your computer and remain undetectable.
  - Hide the intrusion as well as to maintain privilege (root) access.
  - You may need to completely wiping your hard drive and reinstalling everything.
- **Backdoors**
  - Backdoors are much the same as Trojans or worms.
  - Open a “backdoor”, providing a network connection for hackers/ other Malware.
- **Keylogger**
  - Records everything you type on your PC (e.g. log-in names, passwords).
  - Send it on to the source of the keylogging program.
  - Often used by corporations and parents to acquire computer usage information.

Malware (3/3)

- **Ransomware**
  - The request for money is often a fake
- **Browser Hijacker**
  - Unwanted software modifies a web browser's settings without a user's permission
  - Inject unwanted advertising into the user's browser
  - Redirect your normal search activity
  - Intention is to make money off your web surfing



https://malwaretips.com/blogs/remove-hydracrypt-virus/

Points of Ingress

- Instant Messenger/Chat.
- Removable Devices.
- Attachments.
- ‘Legitimate’ software repackaged by employee.
- Browser and Software bugs.
- NetBIOS (File Shares).
- Fake (Trojan) Software.
- Untrusted sites and freeware.
- Downloads.
- etc.

Distribution Techniques

- Blackhat SEO.
  - Used to get a site ranking higher in search results.
- Malvertising.
- Compromise Legitimate Websites.
- Social Engineer Click-Jack.
- Spearphishing Sites.
- Drive-by Downloads.

Further Readings

- https://www.javatpoint.com/ethical-hacking-tutorial

Summary

- System Hacking.
- Password Cracking.
- Malware.

Q&A