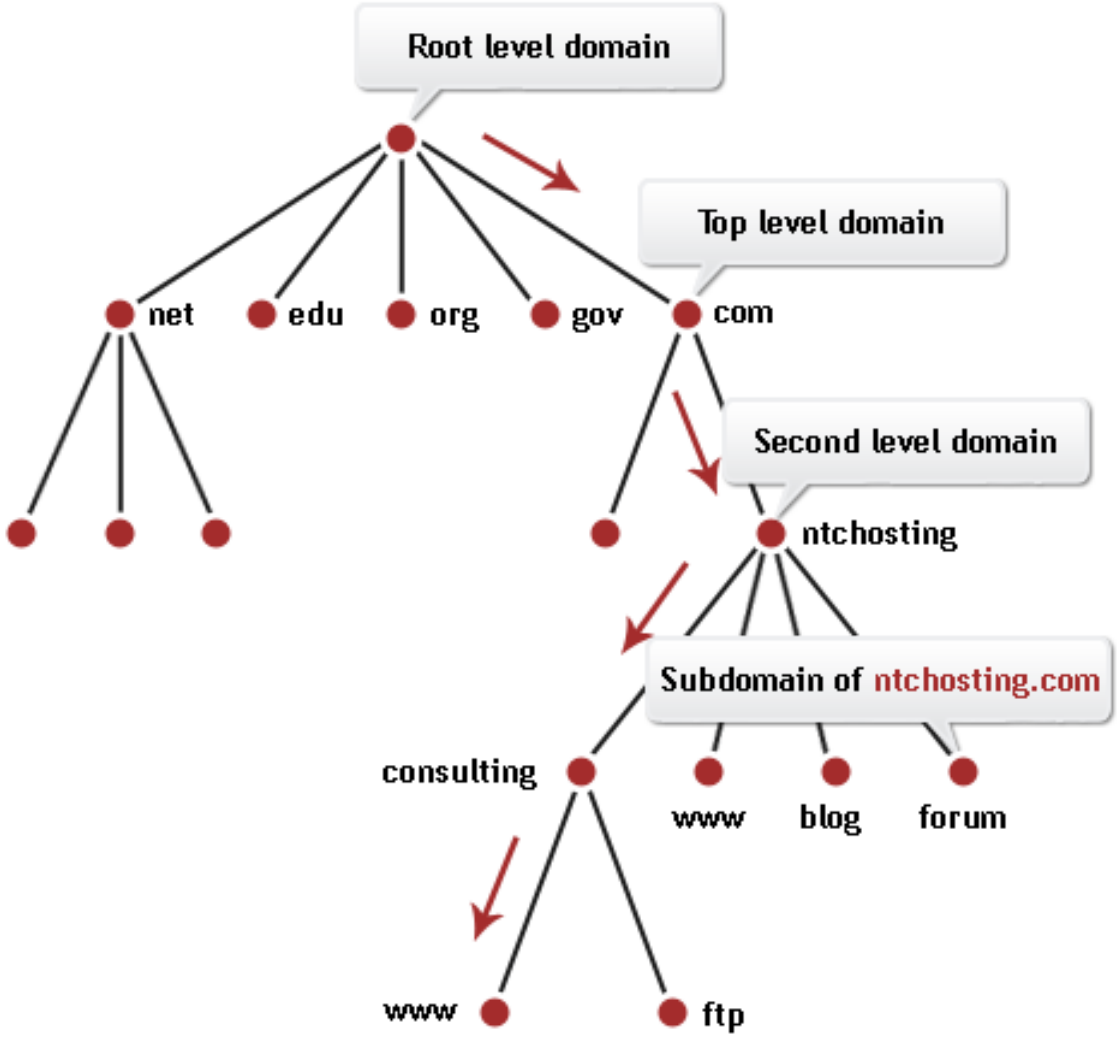
TIES327 – Network Security

MITM things

DNS

- DNS (Domain Name System) is naming system for computers and other resources.
- DNS is usually decentralized hierarchical system in Internet or private network.
- DNS server tells client where server resolved in given name is located.
- Server also spreads data between master and slave DNS servers and between other clusters so information of which server has particular domain data is found hierarchically.
- DNSSEC (Domain Name System Security Extension) is a security extension for DNS. It helps verifying and authenticating data. https://www.icann.org/resources/pages/dnssec-qaa-2014-01-29-en
- TSIG (Transaction Signature) enables authenticating updates in DNS. RFC2845, https://www.ietf.org/rfc/rfc2845.txt



DNS zone & rDNS

- DNS Zone is part of domain name space. It has administrative responsibilities delegated to a single manager.
- There will be the following resource records:
  - SOA - "Start of Authority", containing the *serial number for the zone and the time-to-live values.*
  - NS - five or more NS records which point to the *nameservers* for the .name domain, and any secondary nameservers provided by either the Registry Operator or outsourced DNS providers.
  - A - one or more A records pointing to Registry Operator *WWW servers* for the purpose of providing information on the .name domain; these are intended to point end-users in the correct direction for registering names in the .name domain.
  - MX - one or more MX records which point to internal Registry Operator SLD *E-mail servers* for the purpose of providing a channel by which end-users may raise service queries and so forth. These MX records are aliases to the "smtp.nic.name" domain so that messages to "abuse@name" or "hostmaster@name" are redirected to the appropriate location.
  - NXT - DNS-SEC records, which are required for providing validation of NXDOMAIN responses.
  - SIG - DNS-SEC signature records used to validate responses from the .name domain.
    KEY - DNS-SEC public key for the .name zone

https://www.icann.org/resources/unthemed-pages/registry-agmt-appc-4-2001-07-02-en

Reverse DNS

- Reverse DNS (rDNS) is the method of resolving an IP address into a domain name, just as the domain name system (DNS) resolves domain names into associated IP addresses.

- Setting up reverse DNS for your domain can help e.g. ensure email delivery to mail servers which perform simple anti-spam measures which as a three-way handshake to determine that the forward DNS matches the reverse DNS which matches the fully qualified domain name (FQDN) of the email header.

DNS tunneling

- DNS tunneling is misuse of DNS protocol. Basically it means data will be transferred in DNS queries.
- Because of e.g. some wifi paywalls (or paid wifi's) has allowed DNS-queries to external servers user can create tunnel with DNS tunnel to external server and use it to route data without paying.
- Data exfiltration is basically stealing data.
- The detection techniques can be divided to two separate categories payload analysis and traffic analysis.
- For payload analysis the DNS payload for one or more requests and responses will be analyzed for tunnel indicators.
- For traffic analysis the traffic will be analyzed over time. The count, frequency and other request attributes are used.

DNS tunneling example https://www.youtube.com/watch?v=D4TDhGecB9A

Iodine: https://www.youtube.com/watch?v=WZ_c09AYPTc

Detecting DNS tunneling https://sansorg.egnyte.com/dl/r4ouqZy5dp

DNS Tunneling Detection Techniques – Classification, and Theoretical Comparison in Case of a Real APT Campaign https://jyx.jyu.fi/handle/123456789/55746

SSH tunneling/port forwarding

- SSH port forwarding is a mechanism in SSH for tunneling application ports from the client machine to the server machine, or vice versa.
- It can be used for *adding encryption to legacy applications*, *going through firewalls*, and some system administrators and IT professionals use it for *opening backdoors* into the internal network from their home machines.
- It can also be abused by hackers and malware to open access from the Internet to the internal network.
- https://www.ssh.com/ssh/tunneling/
- https://www.ssh.com/ssh/tunneling/example
- https://www.youtube.com/watch?v=ngNdmB2WySc

WiFi Security

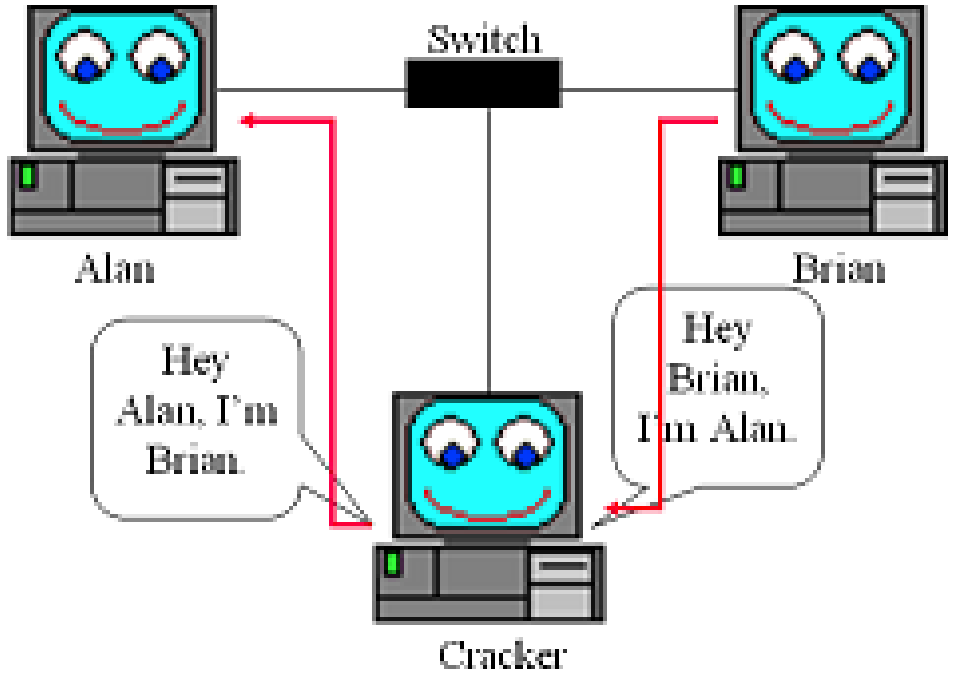
- wifi https://krebsonsecurity.com/2017/10/what-you-should-know-about-the-krack-wifi-security-weakness/
- https://www.krackattacks.com/
- https://www.krackattacks.com/followup.html

Arpspoofing/Arppoisoning

- ARP stands for Address Resolution Protocol and it allows the network to translate IP addresses into MAC addresses.
- ARP works like this: When one host using IP on a LAN is trying to contact another it needs the MAC address (aka: hardware address) of the host it is trying to contact.
- It first looks in it's ARP cache (to see your ARP cache in windows type in "arp –a" at the command line) to see if it already has the MAC address, but if not it broadcasts out an ARP request asking "who has this IP address I'm looking for?"
- If the host that has that IP address hears the ARP query it will respond with it's own MAC address and a conversation can begin using IP.
- In common bus networks like Ethernet using a hub or 801.11b all traffic can be seen by all hosts who's NICs are in promiscuous mode, but things are a bit different on switched networks.
- A switch looks at the data sent to it and tries to only forwards packets to its intended recipient based on MAC address. Switched networks are more secure and help speed up the network by only sending packets where they need to go.
- There are ways around switches though ;).
- Using a program like Arpspoof, Ettercap or Cain we can lie to other machines on the local area network and tell them we have the IP they are looking for, thus re-directing their traffic through us.

Arpspoofing/Arppoisoning

- The attacker is telling Alan's box that he has the IP that corresponds to Brian's box and vice versa.
- By doing this the attacker receives all network traffic going between Alan and Brian.
- Once you have *Arpspoofed* your way between two machines you can sniff the connection with whatever tool you like (TCPDump, Ethereal, Ngrep, etc.)
- By arpspoofing between a machine and the LANs gateway you can see all the traffic it's sending out to the Internet.



Some Kali tools, hints

- Dsniff, https://www.kali.org/tools/dsniff/
- Ettercap, https://www.kali.org/tools/ettercap/
-

- How to detect ARP spoof
- https://github.com/uiucseclab/arpspoofdetect

Sparta
https://null-byte.wonderhowto.com/how-to/discover-attack-services-web-apps-networks-with-sparta-0167255/

NMAP
https://www.youtube.com/watch?v=4t4kBkMsDbQ

Let's hack your home network // FREE CCNA // EP 9
https://www.youtube.com/watch?v=80vIin4xGp8

DHCP Spoofing

- DHCP stands for Dynamic Host Control Protocol (usually server or service on network), which is basically used to assign IP address to all the hosts.
- The working of DHCP is simple, the client user queries to DHCP server for assigning IP address and DNS and DHCP server provides the IP address and DNS services Server IP with lease time. Lease time is given by DHCP for IP address valid time.

- DHCP spoofing has 2 attacks
  1. DHCP starvation attacks is similar to DOS attack, where attacker floods the fake MAC address and fake users on a network until the DHCP database becomes full and confuses to give IP address so that legitimate user don’t get connection.
  2.DHCP rouge server attack. There the attacker create a fake DHCP server and intercept the DHCP requests and providing fake IP address by poisoning DHCP responses.

DHCP Starvation attack and mitigation

https://www.youtube.com/watch?v=8cgCITtOU20

How to find “rogue” DHCP server
https://www.youtube.com/watch?v=uyvEa7Nh80A