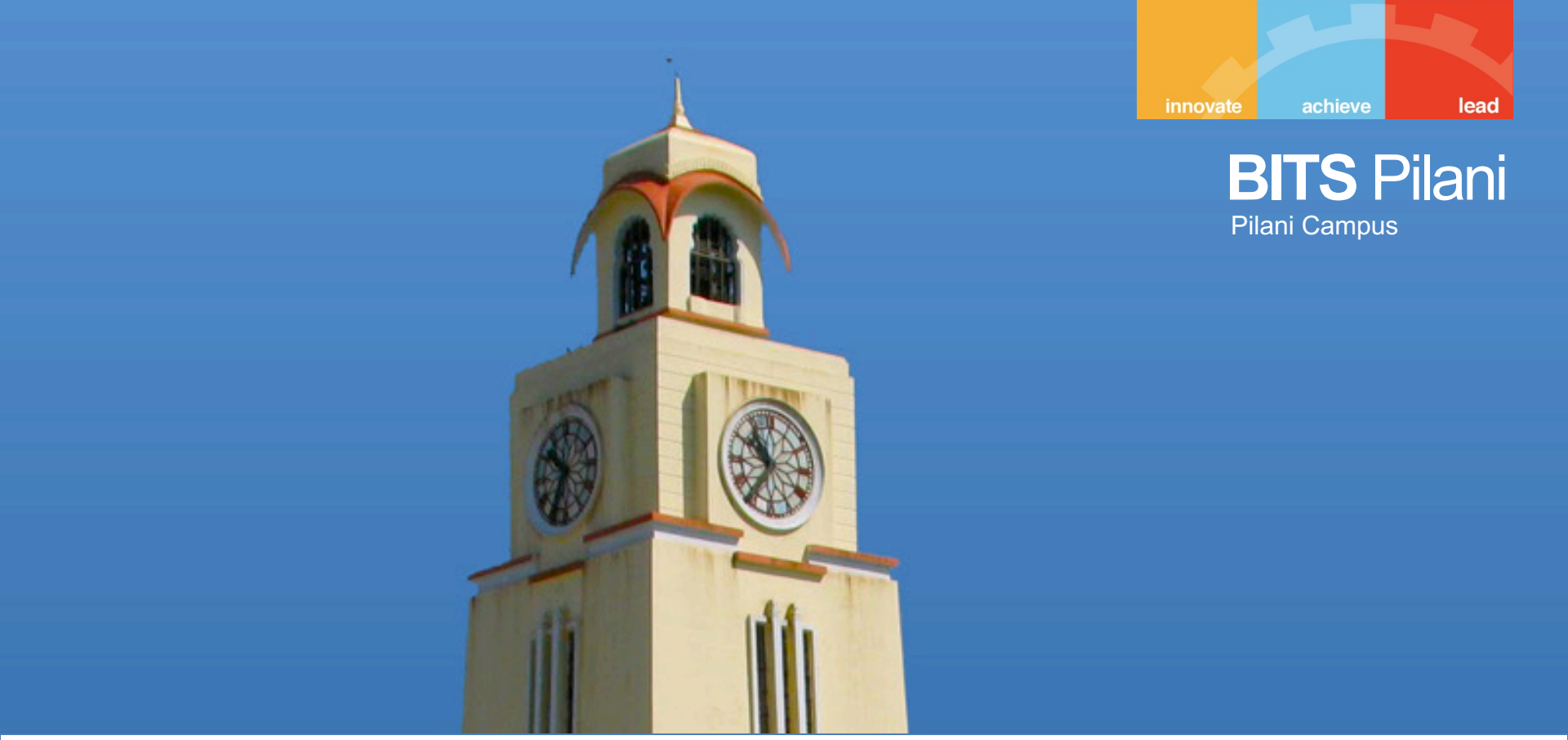
BITS Pilani Presentation

BITS Pilani
Pilani Campus

Jagdish Prasad
WILP



innovate achieve lead

BITS Pilani
Pilani Campus

SSZG575: Ethical Hacking
Session: 07 (Enumeration)

Agenda

innovate achieve lead

- Enumeration
- Sniffing
- DHCP
- DNS

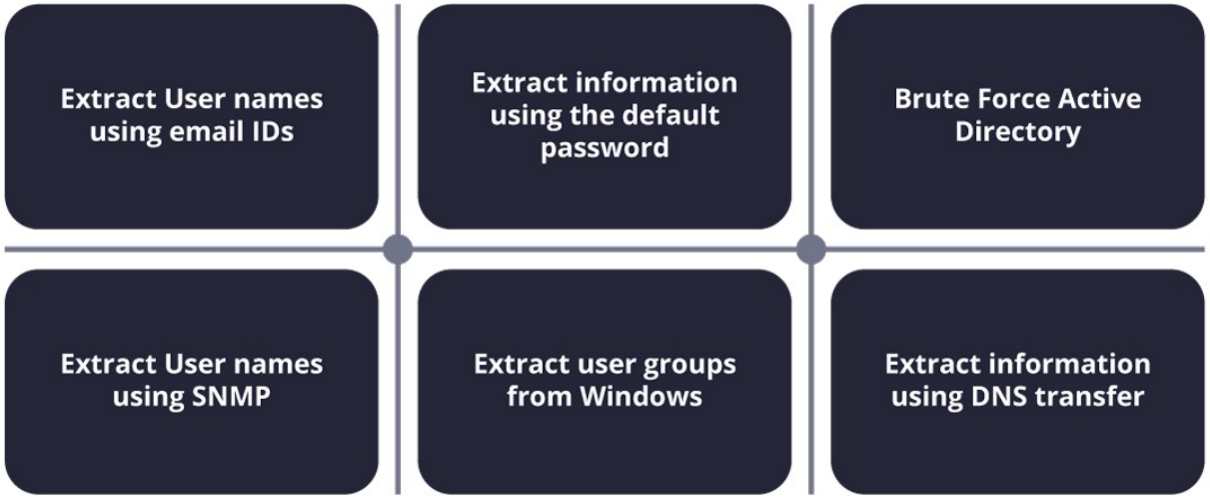
Enumeration

What is Enumeration?

innovate achieve lead

- A process which establishes an active connection to the target hosts to discover potential attack vectors in the system.
- The connection can be used for further exploitation of the system.
- Enumeration is the third step of information gathering about target – Footprinting, Scanning & Enumeration
  - **Footprinting:** Act of gathering information about target systems (active & passive footprinting)
  - **Scanning:** Using tools to find openings in target systems
  - **Enumeration:** Gaining complete access to the system by compromising the vulnerabilities identified during footprinting and scanning

Techniques for Enumeration



Information gathered thru enumeration:

- Network shares & services
- User and Group names
- Routing tables
- IP tables
- Audit settings
- Service configuration settings
- Machine/Host names
- Applications & Banners
- SNMP details
- DNS details

Enumeration Types

- Enumeration depends on the services that a system offers.
- Common enumeration types are:
  - NTP enumeration
  - NetBIOS enumeration
  - Windows enumeration
  - LDAP enumeration
  - Linux/Windows enumeration
  - SMB enumeration
  - RPC enumeration
  - SNMP enumeration
  - IPSec enumeration
  - VOIP enumeration

NTP Enumeration

- Network Time Protocol is for synchronizing time across network - especially important when utilizing Directory Services.
- Number of time servers exist throughout the world that can be used to keep systems synced to each other.
- NTP utilizes UDP port 123.
- Using NTP enumeration, one can gather lists of hosts connected to NTP server, IP addresses, system names, and OS running on the client system in a network.
- All this information can be enumerated by querying NTP server.
- Tools:
  - PRTG Network Monitor,
  - Nmap
  - Wireshark
  - udp-proto-scanner
  - NTP Time Server Monitor

NTP Enumeration Using Nmap

innovate achieve lead

- Find hosts with NTP listening

```
nmap -p123 -Pn -T4 -vv -n -sU -iR 10000 -oN nmap_ntp --open
```

- Nmap NSE Script – to extract information using NTP commands

```
nmap -sU -p123 -iL ntp_targ.txt --script ntp-info -Pn -n
```

- ntpq – command line tool to query remote NTPD daemons. Can run in interactive or command line mode
- ntpdc – interactive tool, provides information about conenctions to the NTP server
- ntptrace – attempts to trace the original source of NTP by continually requesting the upstream NTP server until it eventually gets to Stratum 1 (the highest level a computer can be in the NTP hierarchy – Stratum 0 is the actual clock)

NetBIOS Enumeration

- NetBIOS stands for Network Basic Input Output System.
- Allows computer communication over a LAN and share files and printers.
- NetBIOS names are used to identify network devices over TCP/IP (Windows).
- Must be unique on a network, limited to 16 characters where 15 characters are used for the device name and the 16th character is reserved for identifying the type of service running or name record type.
- Attackers use the NetBIOS enumeration to obtain:
  - List of computers that belong to a domain
  - List of shares on the individual hosts on the network
  - Policies and passwords
- NBTStat: Find protocol statistics, NetBIOS name table and name cache details
- NBTScan – Command line tool to scan network for NetBIOS shares and name
- Superscan: GUI tool used to enumerate windows machine
- Net View: Command line tool to identify shared resources on a network

Windows Enumeration

- Used for Windows operating systems
- Sysinternals is the tool set used for this
- Most basic enumeration and the hackers attack desktop workstations.
- Any file can be accessed and altered – confidentiality loss
- Can change the configuration of the desktop or operating system
- Can be **prevented** by using Windows firewall.

LDAP Enumeration

innovate achieve lead

- LDAP is a protocol used to access directory listings within Active Directory or from other Directory Services.
- A directory is compiled in a hierarchical and logical format like the levels of management and employees in a company.
- LDAP tends to be tied into the Domain Name System to allow integrated quick lookups and fast resolution of queries.
- LDAP generally runs on port 389 and like other protocols tends to usually conform to a distinct set of rules (RFC's).
- It is possible to query the LDAP service, sometimes anonymously to determine a great deal of information that could glean the tester, valid usernames, addresses, departmental details that could be utilised in a brute force or social engineering attack.
- Tools: Jexplorer, LDAP Admin Tool

Linux/UNIX Enumeration

- Hackers who need to enumerate a target host whose operating system is Linux/UNIX use this type of enumeration.
- Works in the same way as others and collects various sensitive data.
- Similar to Windows enumeration
- Can be **prevented** by configuring IPTables.

SMB Enumeration

- SMB represents Server Message Block.
- Convention for sharing assets like records, printers and any asset which should be retrievable or made accessible by the server.
- Runs on port 445 or port 139.
- Easily accessible in windows, so windows clients don't have to arrange anything extra as such other than essential set up.
- For Linux, a samba server is required as Linux locally doesn't utilize SMB convention.
- A confirmation will be set up like a username and secret word, and certain assets made shareable.
- Main defect is utilizing default certifications or effectively guessable or no verification for access of significant assets of the server.
- Administrators must make strong passwords mandatory for clients who need to get to assets utilizing SMB.
- Samba servers are infamous for being hugely vulnerable.

RPC Enumeration

- Remote Procedure Call permits customers and workers to impart in disseminated customer/worker programs.
- Counting RPC endpoints empower aggressors to recognize any weak administrations on these administration ports.
- In networks ensured by firewalls and other security establishments, this portmapper is regularly sifted.
- Hackers filter high port reaches to recognize RPC administrations that are available to coordinate an assault.

SNMP Enumeration

- SNMP (Simple Network Management Protocol) is an application layer protocol which uses UDP protocol to maintain and manage routers, hubs, switches and other network devices on an IP network.
- SNMP is a very common protocol found enabled on a variety of operating systems like Windows Server, Linux & UNIX servers and network devices like routers, switches etc.
- SNMP enumeration is used to enumerate user accounts, passwords, groups, system names, devices on a target system.
- Consists of three major components:
  - **Managed Device:** A managed device is a device or a host (node) which has the SNMP service enabled. These devices could be routers, switches, hubs, bridges, computers etc.
  - **Agent:** An agent can be thought of as a piece of software that runs on a managed device. Its primary job is to convert the information into SNMP compatible format for the smooth management of the network using SNMP protocol.
  - **Network Management System (NMS):** These are the software systems that are used for monitoring of the network devices.
- Tools: OpUtils, SolarWinds

IPSec Enumeration

- IPsec utilizes ESP (Encapsulation Security Payload), AH (Authentication Header) and IKE (Internet Key Exchange) to ensure the correspondence between VPN organizations.
- IPsec-based VPNs use the Internet Security Association and Key Management Protocol (part of IKE) to establish, arrange, alter and erase Security Associations and cryptographic keys in a VPN climate.
- A straightforward checking for ISAKMP at the UDP port 500 can demonstrate the presence of a VPN passage.
- Hackers can research further using an equipment like ‘IKE-output’ to identify the sensitive information like encryption and hashing keys, authentication type, key conveyance calculation etc.

VoIP Enumeration

- VoIP uses the SIP (Session Initiation Protocol) protocol to enable voice and video calls over an IP network.
- SIP administration uses UDP/TCP ports 2000, 2001, 5050, 5061.
- VoIP enumeration provides sensitive information such as VoIP gateway/servers, IP-PBX systems, client software, and user extensions.
- This information can be used to launch various VoIP attacks such as DoS, Session Hijacking, Caller ID spoofing, Eavesdropping, Spamming over Internet Telephony, VoIP phishing, etc.

enum4linux

- NTP Suite is used for NTP enumeration.
- In a network environment, one can find other primary servers that help the hosts to update their times and one can do it without authenticating the system.
- Refer following example:

```
ntpdate 192.168.1.100 01 Sept 12:50:49 ntpdate[627]:
adjust time server 192.168.1.100 offset 0.005030 sec
or
ntpdc [-ilnps] [-c command] [hostname/IP_address]

root@test]# ntpdc -c sysinfo 192.168.1.100
***Warning changing to older implementation
***Warning changing the request packet size from 160
to 48 system peer: 192.168.1.101

system peer mode: client
leap indicator: 00
stratum: 5

precision: -15
root distance: 0.00107 s
root dispersion: 0.02306 s
reference ID: [192.168.1.101]
reference time: f66s4f45.f633e130, Sept 01 2016
22:06:23.458
system flags: monitor ntp stats calibrate
jitter: 0.000000 s
stability: 4.256 ppm
broadcastdelay: 0.003875 s
authdelay: 0.000107 s
```

enum4linux

- enum4linux is used to enumerate Linux systems.
- Following example demonstrates how toe find usernames present in a target host.

```
root@kali:~# enum4linux -U -o 192.168.1.200
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ )

 ============================
|    Target Information    |
 ============================
Target ........... 192.168.1.200
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ======================================================
|    Enumerating Workgroup/Domain on 192.168.1.200    |
 ======================================================
```

smtp-user-enum

- smtp-user-enum tries to guess usernames by using SMTP service.
- Following screenshot demonstrates how is it done.

```
root@kali:~# smtp-user-enum -M VRFY -u root -t 192.168.1.25
Starting smtp-user-enum v1.2 ( http://pentestmonkey.net/tools/smtp-user-enum )

 ----------------------------------------------------------
|                   Scan Information                       |
 ----------------------------------------------------------

Mode ..................... VRFY
Worker Processes ......... 5
Target count ............. 1
Username count ........... 1
Target TCP port .......... 25
Query timeout ............ 5 secs
Target domain .............
```

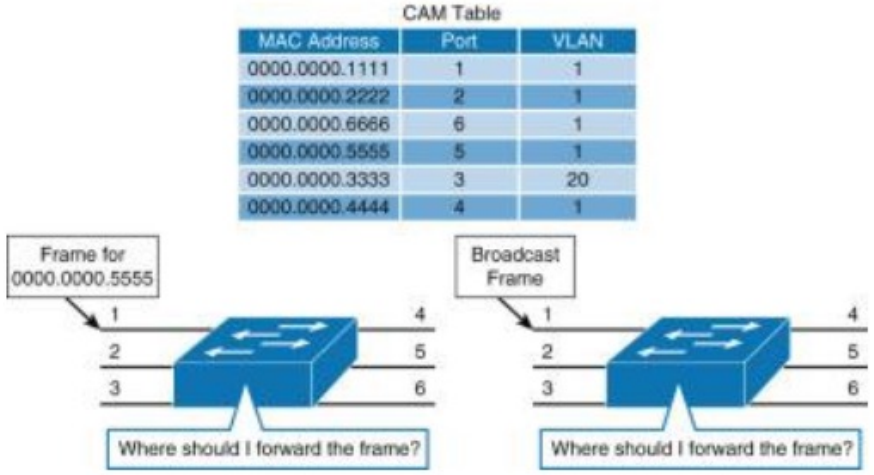
Sniffing

What is Sniffing?

- Process of monitoring and capturing all data packets that are passing through a computer network using packet sniffers.
- Helps Network administrators to keep track of data traffic passing through their network using network protocol analyzers.
- Malicious attackers use packet sniffing tools to capture data packets in a network.
- Data packets captured from a network are used to extract and steal sensitive information such as passwords, usernames, credit card information, etc.
- Sniffing tools: Wireshark, Ettercap, BetterCAP, Tcpdump, WinDump, dSniff, Debookee etc

Sniffing Types

- **Active sniffing**
  - Conducted on a switched network (switch connects two networks)
  - Switch has CAM table containing MAC addresses of destinations to forward traffic to a right destination
  - Attacker sends huge fake traffic to a switch so that the CAM table gets full.
  - Once CAM table gets full, switch start sending traffic to all destinations
  - Attackers connects to one of the ports to carry out sniffing.
- **Passive sniffing**
  - Passive sniffing uses hubs instead of switches (hubs redirects received traffic to all other ports)
  - An attacker needs to connect to LAN and he is able to sniff data traffic in that network.
- Attackers sniff email & web traffic, passwords, router configuration, chats, DNS traffic etc.



DHCP

What is DHCP?

- DHCP stands for Dynamic Host Configuration Protocol
- DHCP server automatically assigns an IP address and other information to each host on the network so they can communicate efficiently with other endpoints.
- DHCP also assigns the subnet mask, default gateway address, domain name server (DNS) address and other pertinent configuration parameters.
- DHCP simplifies the management of IP addresses on networks.

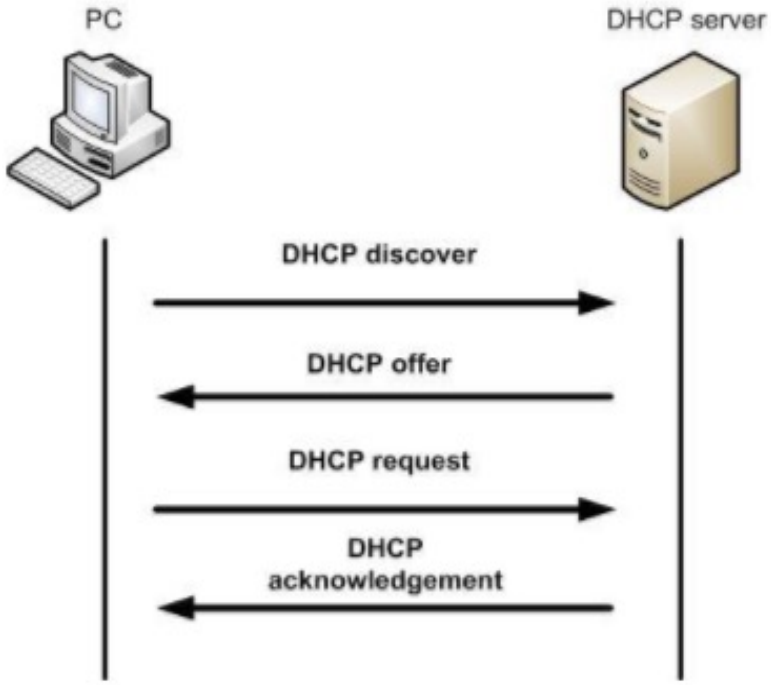
DHCP Components

innovate achieve lead

- **DHCP server:** A networked device running the DCHP service that holds IP addresses and related configuration information.
- **DHCP client:** The endpoint that receives configuration information from a DHCP server.
- I**P address pool:** The range of addresses that are available to DHCP clients.
- **Subnet:** IP networks can be partitioned into segments known as subnets. Subnets help keep networks manageable.
- **Lease Time:** The length of time for which a DHCP client holds the IP address information.
- **DHCP relay:** A router or host that listens for client messages being broadcast on that network and then forwards them to a configured server.

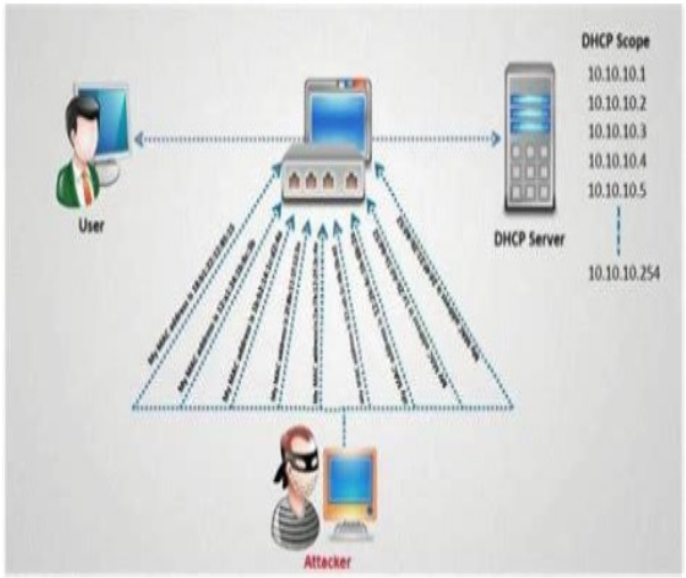
How Does DHCP Work?

- **DHCP Discovery:** Client sends a packet with the default broadcast destination of **255.255.255.255** or the specific subnet broadcast address if any configured. 255.255.255.255 means “this network”
- **DHCP Offer:** DHCP server sends an offers containing the proposed IP address for DHCP client, IP address of the server, MAC address of the client, subnet mask, default gateway, DNS address, and lease information.
- **DHCP Request:** In response to the offer, the client sends a **DHCP Request** requesting the offered address from one of the DHCP servers.
- **DHCP Acknowledgment:** The server sends Acknowledgment to the client confirming the DHCP lease to the client.
- At this step, the IP configuration is completed and the client can use the new IP settings.



DHCP Starvation Attack

- In a DHCP Starvation attack, a hostile actor sends a ton of bogus DISCOVER packets until the DHCP server thinks they've expended their available pool.
- Clients looking for IP addresses find that there are no IP addresses for them, and they're denied service.
- Additionally, they may look for a different DHCP server, one which the hostile actor may provide.
- Using a hostile or dummy IP address, the hostile actor can read all the traffic that client sends and receives.
- Ref: https://www.youtube.com/watch?v=jiSl89al4nI&feature=emb_title



DHCP Security Risks

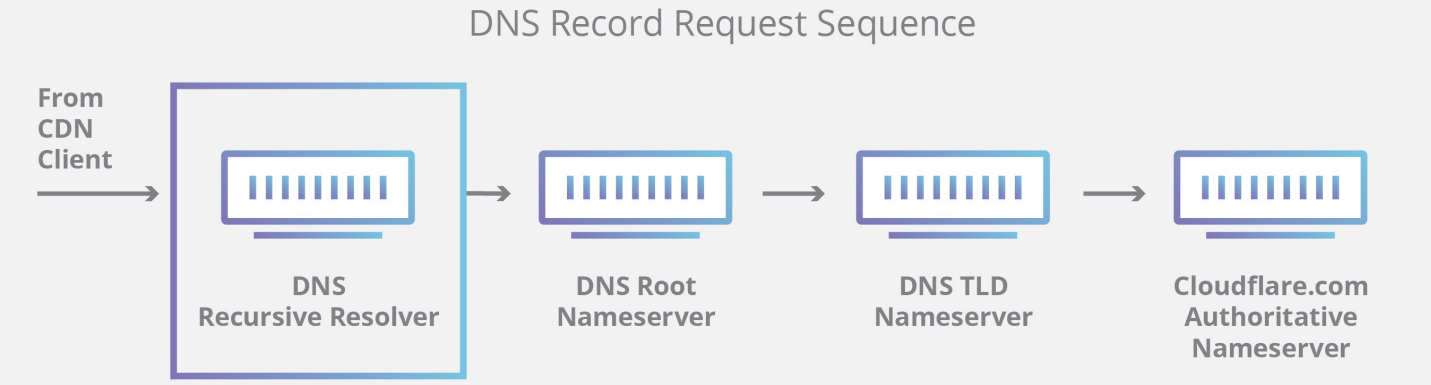
- DHCP protocol requires no authentication so any client can join a network quickly.
- Client has no way of validating the authenticity of a DHCP server, rouge ones can be used to provide incorrect network information.
  - Can cause denial-of-service attacks or man-in-the-middle attacks where a fake server intercepts data that can be used for malicious purposes.
- DHCP server can not authenticate a client, it hands out IP address information to any device that makes a request.
  - A threat actor could configure a client to continually change its credentials and quickly exhaust all available IP addresses in the scope, preventing company endpoints from accessing the network

DNS

What is DNS?

- Domain Name System (DNS) is the phonebook of the Internet.
- Humans access information online through domain names like google.com, nytimes.com or espn.com etc.
- Web browsers interact through IP addresses.
- DNS translates domain names to IP addresses so browser can load Internet resources.
- The process of DNS resolution involves converting a hostname (i.e. www.example.com) into a computer-friendly IP address (i.e. 192.168.1.1).

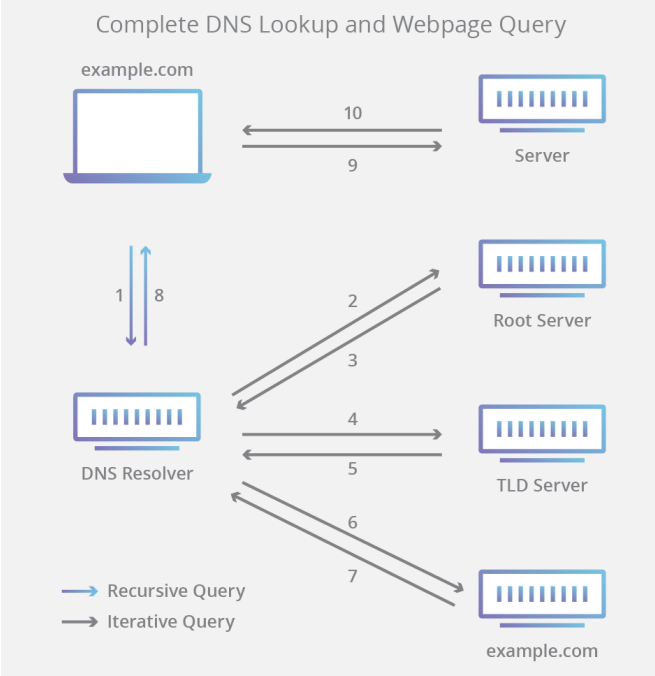
Types of DNS



- **DNS Recursor:** The recursor is like a librarian who is asked to find a particular book in a library. The DNS recursor is a server designed to receive queries from client machines through applications such as web browsers.
- **Root Nameserver:** The root is the first step in translating human readable host names into IP addresses. It is like an index in a library that points to different racks of books.
- **TLD Name Server:** The top level domain server (TLD) is a specific rack of books in a library. This nameserver is the next step in the search for a specific IP address, and it hosts the last portion of a hostname (In example.com, the TLD server is “com”).
- **Authoritative Nameserver:** This nameserver is a dictionary on a rack of books which can translated a specific name into its definition. If the authoritative name server has access to the requested record, it will return the IP address for the requested hostname back to the DNS Recursor.

DNS Lookup

- A user types ‘example.com’ into a web browser and the query is received by a DNS recursive resolver.
- The resolver then queries a DNS root nameserver.
- The root server then responds to the resolver with the address of a Top Level Domain (TLD) DNS server (such as .com or .net), which stores the information for its domains. When searching for example.com, this request is pointed toward the .com TLD.
- The resolver then makes a request to the .com TLD.
- The TLD server then responds with the IP address of the domain’s nameserver, example.com.
- The recursive resolver sends a query to the domain’s nameserver.
- IP address for example.com is returned to the resolver from the nameserver.
- DNS resolver then responds to the web browser with the IP address of the domain requested initially.
- The browser makes a HTTP request to the IP address.
- Server at that IP returns the webpage to be rendered in the browser (step 10).



DNS Server 8.8.8.8

- While your ISP sets a default DNS server, you're under no obligation to use it.
- Some users may have reason to avoid their ISP's DNS — for instance, some ISPs use their DNS servers to redirect requests for non-existent addresses to pages with advertisements.
- As an alternative, you can point to a public DNS server that will act as a recursive resolver.
- One of the most prominent public DNS servers is Google’s 8.8.8.8.
- Google's DNS services tend to be fast and while there are certain questions about the ulterior motives Google has for offering the free service, they can't really get any more information from you that they don't already get from Chrome.
- Google has a page with detailed instructions on how to configure your computer or router to connect to Google's DNS.

DNS Attacks

- **DNS reflection attacks**
  - DNS reflection attacks floods victims with high-volume messages from DNS resolver servers.
  - Attackers request large DNS files from all the open DNS resolvers they can find and do so using the spoofed IP address of the victim.
  - When the resolvers respond, the victim receives a flood of unrequested DNS data that overwhelms their machines.
- **DNS cache poisoning**
  - DNS cache poisoning can divert users to malicious Web sites.
  - Attackers manage to insert false address records into the DNS so when a potential victim requests an address resolution for one of the poisoned sites, the DNS responds with the IP address for a different site, one controlled by the attacker.
  - Once on the fake site, victim may be tricked into giving up passwords or suffer malware downloads.

DNS Attacks

innovate achieve lead

- **DNS resource exhaustion**
  - DNS resource exhaustion attacks can clog the DNS infrastructure of ISPs, blocking the ISP's customers from reaching sites on the internet.
  - This can be done by attackers registering a domain name and using the victim's name server as the domain's authoritative server.
  - So if a recursive resolver can't supply the IP address associated with the site name, it will ask the name server of the victim.
  - Attackers generate large numbers of requests for their domain and toss in non-existent subdomains to boot, which leads to a torrent of resolution requests being fired at the victim's name server, overwhelming it.

Thank You