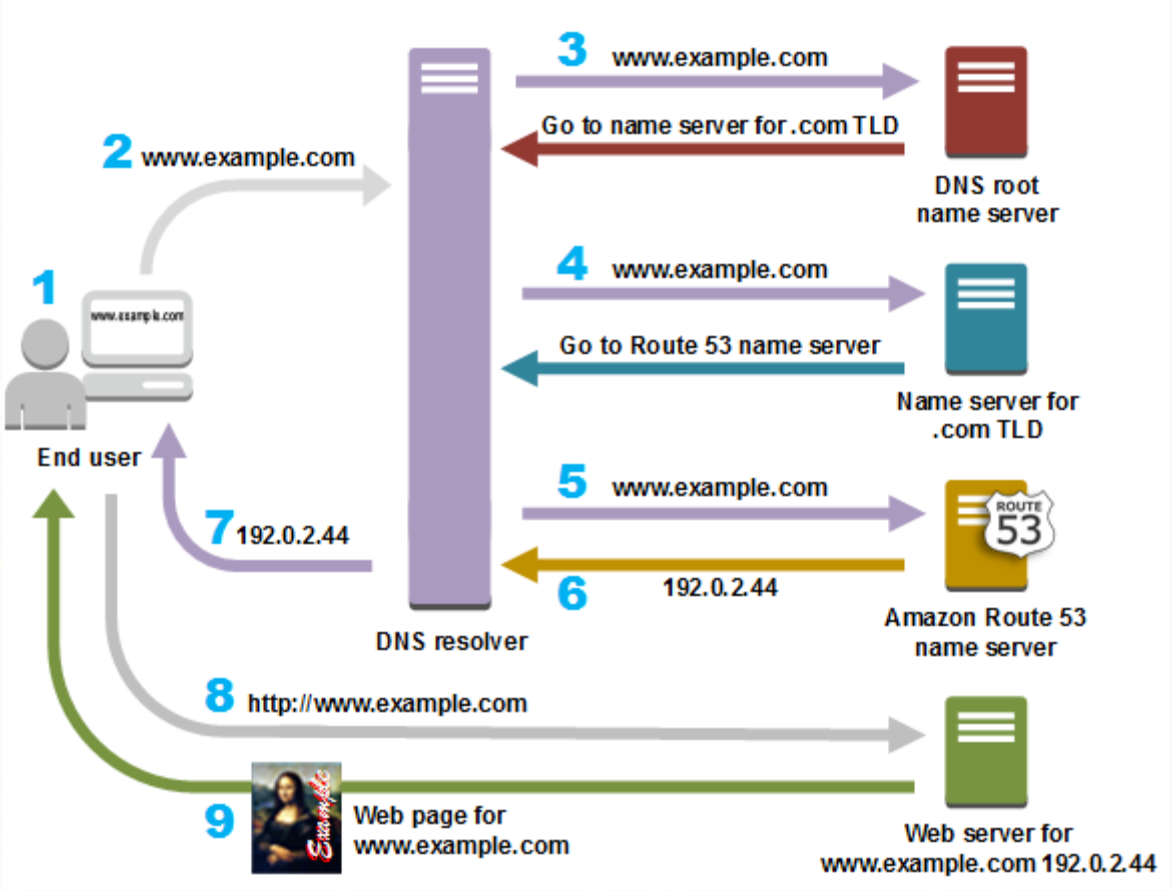
DNS Attacks

DNS (Domain Name Service)

- **Motivation**
  - Human prefer pronounceable names rather numeric IP addresses
  - Machines prefer numeric IP addresses
  - We need to have a mechanism to translate the pronounceable names to IP addresses, so the machines can understand.
- **Original Naming Scheme: flat structure.**
  - The original names formed a flat namespace without structure, A central site, the Network Information Center (NIC), administered the namespace. Later, the NIC was replaced by the INTERnet Network Information Center.
  - Advantage: names are convenient and short
  - Disadvantage: a flat namespace cannot generalize to large sets of machines for both technical and administrative reasons.
    - Potential conflict
    - Names are assigned by a center server
    - Maintaining correct copies of the entire list at each site is difficult
- **Hierarchical Names**
  - Decentralizing the naming mechanism: delegating authority and distributing responsibility
  - A hierarchical naming scheme works like the management of a large organization.
    - The namespace is partitioned at the top level

DNS Query

- **DNS**
  - **Specifies the name syntax and rules for delegating authority over names**
  - **Specifies the implementation of distributed computing system that efficiently map names to addresses.**
- **DNS Syntax**
  - **Set of labels separated by delimiter character (period)**
  - **Example: ecs.syr.edu**
  - **syr.edu is also a domain**
  - **The top-level domain is edu**
- **Mapping Domain Names to Addresses**
  - **Name server: supplies name-to-address translation**
  - **Client: uses one or more name servers when translating a name**
  - **DNS uses a set of on-line servers**
  - **Servers arranged in tree**
  - **A given server can handle entire subtree. For example, a sever at ECS manages the domain names within the ecs.syr.edu domain.**
- **Type of DNS queries**
  - **Recursive: often used by the client**
  - **Iterative: often used by the local DNS server**
- **Recursive query and Iterative query:**
  - A **recursive DNS** lookup is where one **DNS** server communicates with several other **DNS** servers to hunt down an IP address and return it to the client. This is in contrast to an iterative **DNS query**, where the client communicates directly with each **DNS** server involved in the lookup.


1
www.example.com
End user
2 www.example.com
DNS resolver
3 www.example.com
Go to name server for .com TLD
DNS root name server
4 www.example.com
Go to Route 53 name server
Name server for .com TLD
5 www.example.com
6 192.0.2.44
ROUTE 53
Amazon Route 53 name server
7 192.0.2.44
8 http://www.example.com
9
Web page for www.example.com
Web server for www.example.com 192.0.2.44

DNS Caching

- **DNS caching: After the local DNS server obtains the query results from another DNS server, it will store the results in its cache for certain period of time. The timeout duration can be specified in the DNS response.**
- **An example of DNS query process: The process is straightforward. Here's one example in which a local name server uses iterative queries to resolve an address for a client:**
  - **The local name server receives a name resolution request from a client system for a host name (such as www.google.com).**
  - **The local name server checks its records. If it finds the address, it returns it to the client. If no address is found, the local name server proceeds to the next step.**
  - **The local name server sends an iterative request to the root (the "." in .com) name server.**
  - **The root name server provides the local name server with the address for the top-level domain (.com, .net, etc.) server.**
  - **The local name server sends an iterative query to the top-level domainserver.**
  - **The top-level domain server replies with the IP address of the name server that manages the host name's domain (such as google.com).**
  - **The local name server sends an iterative request to the host name's domain name server.**
  - **The host name's domain name server provides the IP address for the host name (www.google.com) being sought.**
  - **The local name server passes that IP address to the client.**

DNS Ports

- DNS Port
  - The DNS uses TCP and UDP on port 53 to serve requests.
  - Almost all DNS queries consist of a single UDP request from the client followed by a single UDP reply from the server.
  - TCP typically comes into play only when the response data size exceeds 512 bytes, or for such tasks as zone transfer.

DNS Protocol Attacks

- **Unrelated Data Attack**
  - **To improve performance, DNS servers can send back more information than what the client has asked for. For example, if the client asks for the IP address of www.mysite.com, the DNS server can also send back the IP addresses for ftp.mysite.com and mail.mysite.com to avoid another likely DNS lookup.**
  - **In the older version of DNS servers, the validity of the extra information is not verified. The actual information does not even need to be related to the original query. Therefore, a malicious DNS server from mysite.com can send back the faked IP addresses for Citibank.com, tricking users to go to the malicious site when they try to connect to Citibank.**
  - **This problem has been fixed in BIND, by forbidding anything that is not related to the original request to be cached.**
- **Related Data Attack**
  - **The process is the same as the unrelated data attack**
  - **The hacker has to make the extra information related to the original query**
    - **MX: mail server for a domain**
    - **CNAME: canonical name for an alias**
    - **NS: DNS servers for a domain**
  - **The above information is "related" to the original request, but they can point to totally different information the hacker wants to be cached.**

DNS Protocol Attacks

- Reverse DNS attacks
  - Assume nyx.syr.edu and apollo.syr.edu trust each other, and the trust is based on name, not the IP address.
  - Also assume that you are from hacker.com, and you have the control of your own DNS server.
  - How can you exploit the trust relationship between nyx and apollo?
    - When nyx receives a connection from an IP address, it needs to use the reverse DNS lookup to find out the hostname of the IP address.
    - The reverse lookup will start from the root, and eventually goes to the DNS server of the owner of the IP address. If the IP address is the attacker's machine, the query will go to the DNS server of hacker.com, which will tell you anything that they want, including saying that the IP address's hostname is apollo.syr.edu.

DNS Protocol Attacks

- **DNS Pharming Attacks: aiming to redirect a websites traffic to another, bogus website. Many techniques can be used, and mostly target DNS.**
  - **Insider attack: corrupted insiders can modify the local DNS servers to mislead users to bogus websites.**
  - **Corrupted hosts: if a host is already corrupted, there are many things attackers can do to affect the DNS. Users of the corrupted machines can go to bogus websites when they visit their favorite sites. Here are some popular tactics by attackers:**
    - **Modify the /etc/hosts file in Unix systems.**
    - **Modify Windows Hosts file to map specific domain names to specific IP addresses.**
    - **Modify Windows registry settings to reference specific (rogue) DNS servers.**
    - **Create a scheduled task under Mac OS X to reference specific (rogue) DNS servers**
    - **Exploit cross-site request forgery vulnerabilities in routers to overwrite the DNS server configuration offered to local area network clients.**
  - **DHCP attack: Serving the rogue DNS server configuration over DHCP, the protocol responsible for distributing dynamic IP addresses, as well as other information, including DNS settings.**

DNS Protocol Attacks

- Domain Registration Attacks: when a domain registration expires and the owner forgot to renew it, attackers can buy that domain legally and hijack the domain. Attackers can also buy the domain names that are similar to their targets. If users misspell the domain names, they might become victims.
- Corrupting DNS servers. Change the mappings on the corrupted DNS servers.
- DNS cache Poisoning.
  - Victim DNS server asks other DNS servers for mappings if it doesn't have them. It then caches the mappings.
  - DNS cache poisoning is to poison the clients cache.
- Dan Kaminsky Attack: An elegant attack that bypass the cache effect. The idea is not to send a request for www.example.com if your target is www.example.com. Instead, send a.example.com, b.example.com, In the spoofed reply, attach the IP address for www.example.com in the *additional field*. This way, if the spoofed replies lose to the legitimate replies, the IP address for www.example.com will not be cached, because the IP address is unlikely to be included in the legitimate replies. Therefore, the attackers can keep trying, until its own spoofed replies beat the legitimate replies. As long as the attackers' chance of winning the race is not zero, sooner or later, the attackers will succeed.

References

1. J. Paul Guyer, P.E., R.A, "An Introduction to Intrusion Detection Systems", The Clubhouse Press, California, 2018.
2. Weaver, Randy, Dawn Weaver, and Dean Farwood. Guide to network defense and countermeasures. Cengage Learning, 2013.
3. G. Dileep Kumar, "Network Security Attacks and Countermeasures", IGI Global, 2016.
4. Nagendra Kumar Nainar, Yogesh Ramdoss, and Yoram Orzach, "Network Analysis Using Wireshark 2 Cookbook: Practical recipes to analyze and secure your network using Wireshark 2, 2nd Edition, Packt, 2018.
5. Andrei Miroshnikov, "Windows Security Monitoring: Scenarios and Patterns", Wiley, 2018.
6. Steve Suehring, "Linux Firewalls: Enhancing Security with nftables and Beyond", Addison-Wesley, 2015.
7. Easttom II, William Chuck. Network defense and countermeasures: principles and practices. Pearson IT Certification, 2013.
8. Snort 3.0 User manual, httpw://www.snort.org
9. Internet security http://www.cis.syr.edu/~wedu/Teaching/cis758/readings.html
10. Open Learn https://www.open.edu/openlearn/ocw/mod/oucontent/view.php?id=48261
11. IDPS https://cloudacademy.com/course/intrusion-detection-and-prevention-on-amazon-web-services/ids-ips-in-detail-1/
12. SVNIT course structure http://www.svnit.ac.in/web/department/computer/CO624.php
13. Detecting and Mitigating Cyber Threats and Attacks https://www.coursera.org/learn/detecting-cyber-attacks/home/welcome
14. Secure Networked System with Firewall and IDS https://www.coursera.org/learn/secure-networked-system-with-firewall-ids/home/welcome
15. https://www.coursera.org/learn/secure-networked-system-with-firewall-ids#syllabus
16. Customizable Network intrusion dataset creator https://github.com/nrajasin/Network-intrusion-dataset-creator
17. https://www.researchgate.net/post/Is_there_any_tool_to_convert_pcap_tcpdump_file_into_KDD_dataset_format
18. Information Security and Assurance https://people.eecs.ku.edu/~saiedian/710/
19. http://ranger.uta.edu/~dliu/courses/cse6392-ids-spring2007/
20. SNORT Tutorial https://www.youtube.com/watch?v=W1pb9DFCXLw&list=PLpPXZRVU-dX33VNUeqWrMmBNf5FeKVmi-