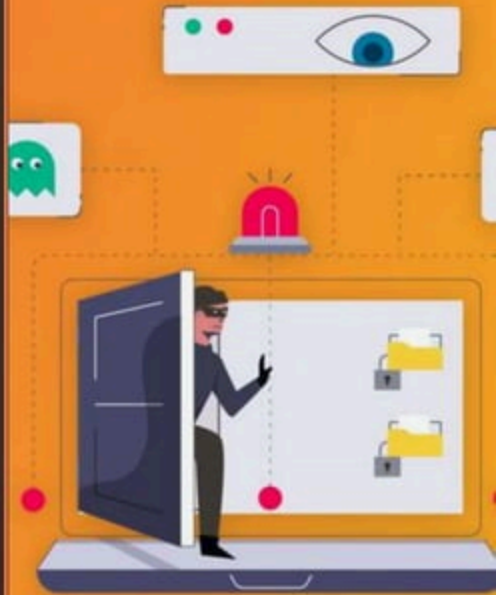
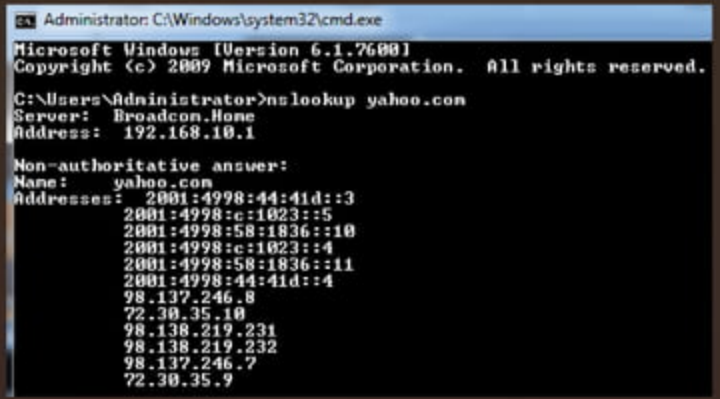
DNS Level Attack: DNS Spoofing / Poisoning

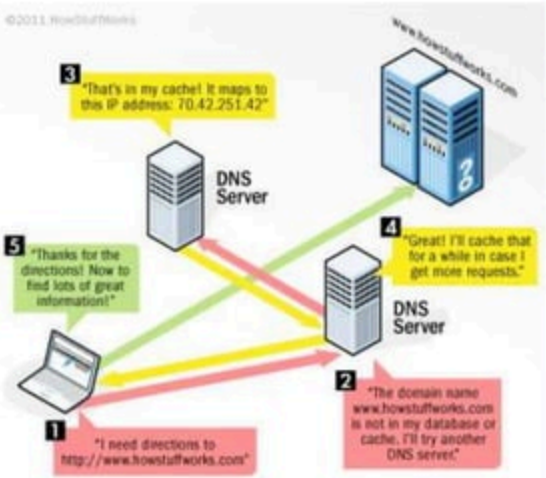
What is DNS?

- DNS means Domain Name Server.
- DNS are the Internet's equivalent of a phone book.
- They maintain a directory of domain names and translate them to Internet Protocol (IP) addresses.



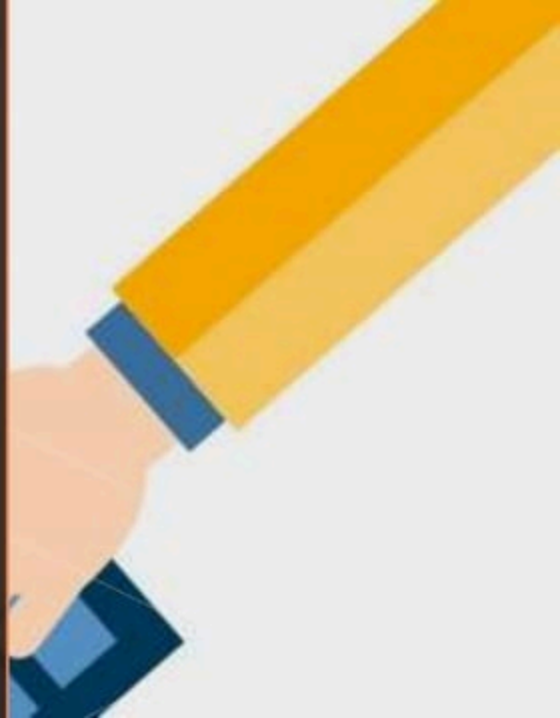

Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\Administrator>nslookup yahoo.com
Server: Broadcon.Home
Address: 192.168.10.1
Non-authoritative answer:
Name: yahoo.com
Addresses: 2001:4998:44:41d::3
2001:4998:c:1023::5
2001:4998:58:1836::10
2001:4998:c:1023::4
2001:4998:58:1836::11
2001:4998:44:41d::4
98.137.246.8
72.30.35.10
98.138.219.231
98.138.219.232
98.137.246.7
72.30.35.9

How DNS Works?



Types of DNS Attacks

- (DOS) Denial of Service attack
- DNS Amplification Attack
- BIND9 Spoofing
- DNS Spoofing/ Poisoning



DNS Attacks:

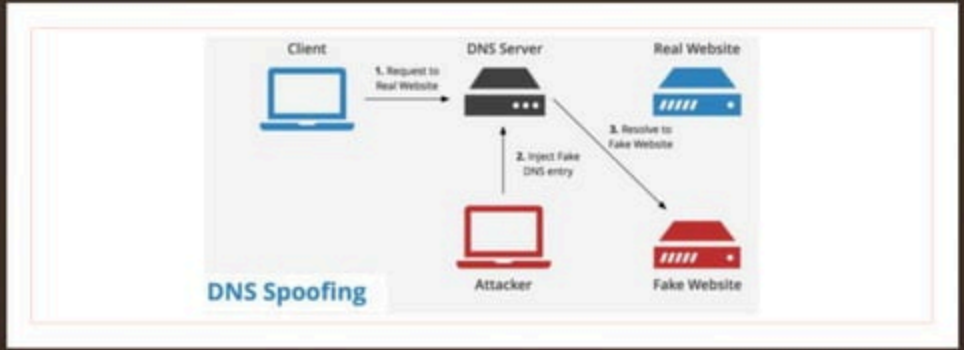
- Denial-of-service Attack typically flood servers systems or networks with traffic in order to overwhelm the victim's resources and make it difficult or impossible for legitimate users to access them.
- DNS Amplification Attack: is a reflection-based volumetric distributed denial-of-service (DDoS) attack in which an attacker break the functionality of open DNS resolvers in order to overwhelm a target server or network with an amplified amount of traffic.

Conti….

DNS resolvers like BIND use unpredictable values with each generated query. Since the corresponding values in the response must match the values sent in the query, it is difficult for a blind attacker, who does not see the query, to forge a valid response and insert a new name.

DNS Spoofing/Poisoning

- DNS spoofing, also referred to as DNS tampering, DNS redirection or DNS hijacking.
- It is a form of computer security hacking in which corrupt Domain Name System data is introduced into the DNS resolver 's cache.
- Causing the name server to return an incorrect result record, e.g. an IP address.
- This results in traffic being diverted to the attacker's computer



How Does DNS Spoofing Work?

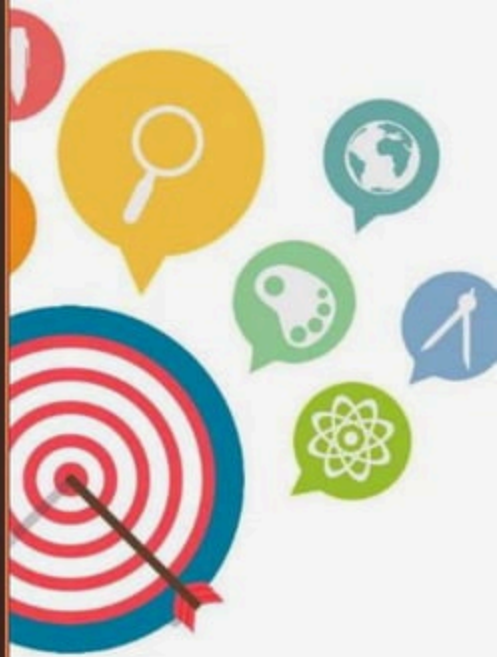
How DNS Spoofing Occurs?

DNS spoofing is an overarching term and can be carried out using various methods such as:

1. DNS cache poisoning
2. Compromising a DNS server
3. Implementing a Man in the Middle Attack

Aims of Attackers

- **Launch an attack:** By changing the IP address for a popular domain like Google.com, for example, a hacker could divert a large amount of traffic to a server incapable of handling so much traffic.
- **Redirection:** A corrupted DNS entry can redirect users to websites they do not intend to visit. A hacker might use this to send victims to a phishing site.
- **Censorship:** Browsing the web is nearly impossible without DNS, so whoever controls the DNS server controls who sees what on the web.



DNS Spoofing Mitigation Using Domain Name Server Security (DNSSEC)

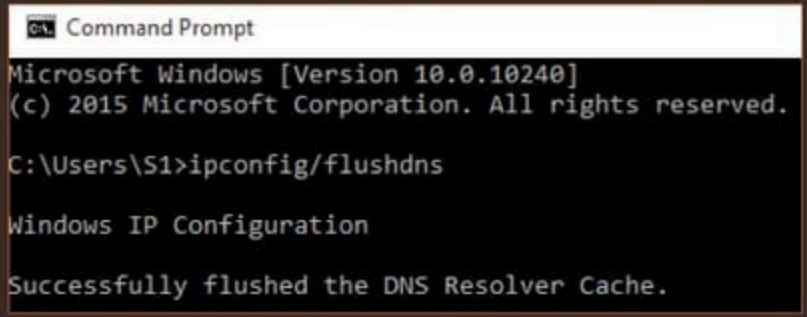
DNSSEC is a protocol designed to secure your DNS by adding additional methods of verification. The protocol creates a unique cryptographic signature stored alongside your other DNS records, e.g., A record and CNAME. This signature is then used by your DNS resolver to authenticate a DNS response, ensuring that the record wasn't tampered with.

Ways to Exploit

In order to achieve DNS Amplification attack, the attacker performs two malicious tasks,

- The attacker spoofs the IP address of DNS Resolver (converts domain name to IP address) and replaces it with the victims IP address. This is because all reply of the DNS server will respond back to victims' server.
- The attacker finds Internet domain registered with many DNS records. Ex domain.example.com, domain1.example.com etc. Then the attacker DNS query to get all records of example.com.

Prevention


Command Prompt
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.
C:\Users\S1>ipconfig/flushdns
Windows IP Configuration
Successfully flushed the DNS Resolver Cache.

How to Prevent?

- Always check for HTTPS
- Encrypted DNS
- VPN
- Antivirus
- Disable JavaScript and WebRTC
- DNSSEC

- Only cache information from authoritative servers
- Cross-check IP DNS mappings
- Transaction signatures for zone transfer, dynamic updates
- Split-split strategy: Advertising name server for DNS servers
- No cache to poison
- Only allow internal traffic

Cont…

Firewalls can be utilized to minimize attacks against the DNS protocol.

- Query and Response Verification
- Transaction ID randomization
- DNS Header Flag Filtering
- DNS message size limitations

DNS Spoofing Attack