|  |  |  |
| --- | --- | --- |
| Name: Adarsh Kumar | SRN No: PES2UG20CS016 | Assignment No:05 |
| Section: B | Date: 10/10/2022 |

|  |  |
| --- | --- |
|  | **Verification of the DNS setup** |
| Screenshots | Get the IP address of ns.attacker32.com    From the zone file we get IP of the attacker 10.9.0.153    Get the IP address of [www.example.com](http://www.example.com)    There are two entries in the answer section one is the official name server and other one is the attacker’s name-server.    We requested the attacker’s name-server we got IP as 1.2.3.5 |
| **Task1:** | **Directly Spoofing Response to User** |
|  | Clearing the cache on the local DNS Server    Just checking the cache before lab-start  Before performing the attack.      Here you can observe that we are getting legitimate output. |
|  | On attacker terminal after successful attack, we got one packet    On User terminal after attack we can observe that in answer section we are getting IP as 1.1.1.1      This still has legal entry it is because we targeted the user not the local host |
|  | In case the attack fails which is not my case:  // Delay the network traffic by 100ms  # tc qdisc add dev eth0 root netem delay 100ms  // Delete the tc entry  # tc qdisc del dev eth0 root netem  // Show all the tc entries  # tc qdisc show dev eth |
| **Task 2:** | **DNS Cache Poisoning Attack – Spoofing Answers** |
| Attacker Terminal | As we can see that in attacker terminal 1 packet is sent in IPv4 type. |
| User Terminal | Example.com has IP of 1.1.1.1 |
| Wireshark  Observation | In answer section we can observe the address as 1.1.1.1 |
| Local – DNS cache | As we can see that here cache entry is also found with attacker IP unlike previous one. |
| **Task 3:** | **Spoofing NS Records** |
| Attacker Terminal | On attacker terminal one packet sent |
| User Terminal |  |
| Wireshark  output | We can see that in Authoritative nameserver an entry as ns.attacher32.com |
|  | We can see that the cache entries that contains example.com linked to attacker’s name server this time and check the corresponding forge attacker’s IP in [www.example.com](http://www.example.com) and its subdomain [ftp.example.com](ftp://ftp.example.com) as well.  This cache poising attack takes control of major domain including the sub-domain of example.com |
| **Task 4:** | **Spoofing NS Records for Another Domain** |
| Attacker Terminal |  |
| User Terminal |  |
|  | As we can see that Authoritative nameserver has two entries now |
|  | Cache entry’s after diging [www.google.com](http://www.google.com) is still legal |
| **Task 5:** | **Spoofing Records in the Additional Section** |
| Attacker Terminal |  |
| User Terminal |  |
|  | Here in Authoritative nameserver multiple entry are also created |
|  | Only one entry is visible because we used grep command for example only. |