NDS Final Project

Team: Alpha

Abhay Raj Singh (110040822)
Sahil Sharma (110056972)
Rahul Meghani (110026313)

Project overview

Concepts/features inspired from class

- Packet sniffing
- Packet spoofing
- DNS Manipulation
- Environment setup with docker
- Scapy and python

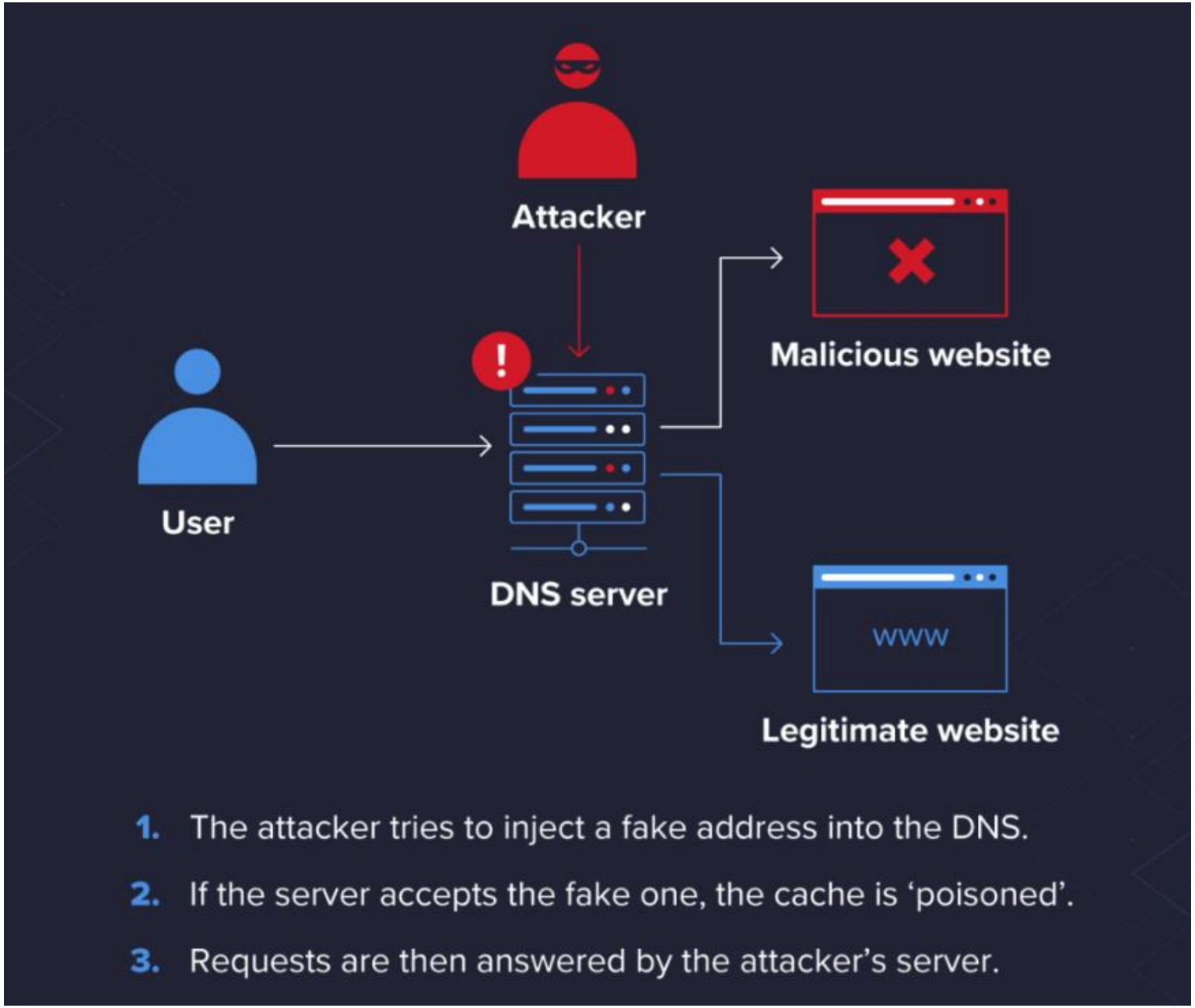
- In this Network security attack, we try to exploit the DNS resolutions in a local network
- Our local DNS attack manipulates the address resolution, with an intent to misdirect the victim to a malicious destination (website).
- This is difficult to detect. The victim can easily be fooled due to the correct URL and similar looks of the malicious website helping the attacker gain sensitive information from the victim.

Scenario

The attacker is in the same local network as the victim (with local DNS as its primary DNS server)

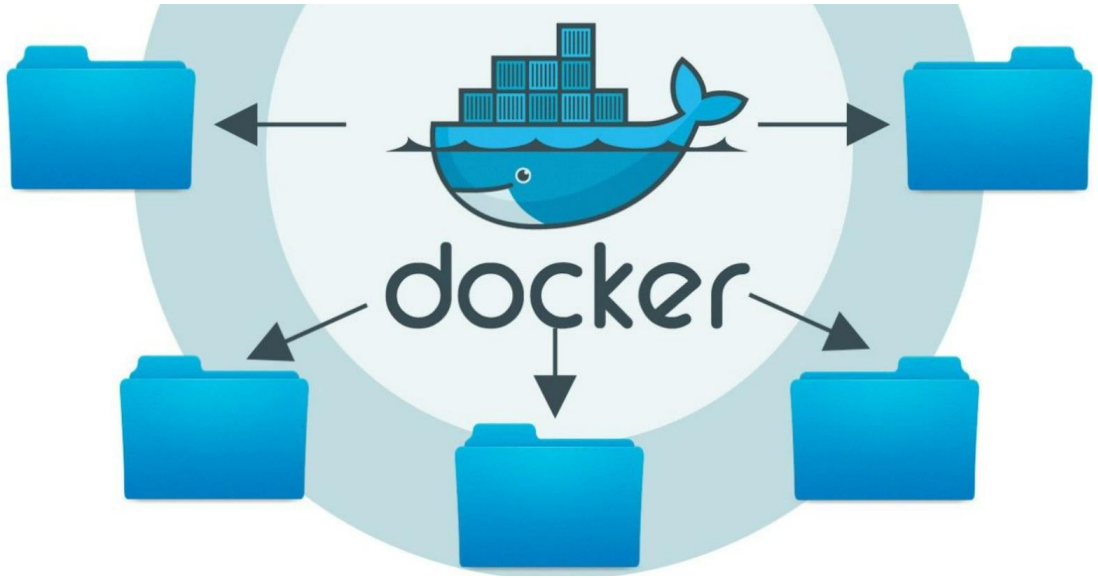
The attacker can trace all the packets in this local network.

The local DNS server has predictable source port number, DNSSEC turned off and the Attacker zone entry


Attacker
Malicious website
!
User
DNS server
www
Legitimate website
1. The attacker tries to inject a fake address into the DNS.
2. If the server accepts the fake one, the cache is 'poisoned'.
3. Requests are then answered by the attacker's server.

How it works?

Environment



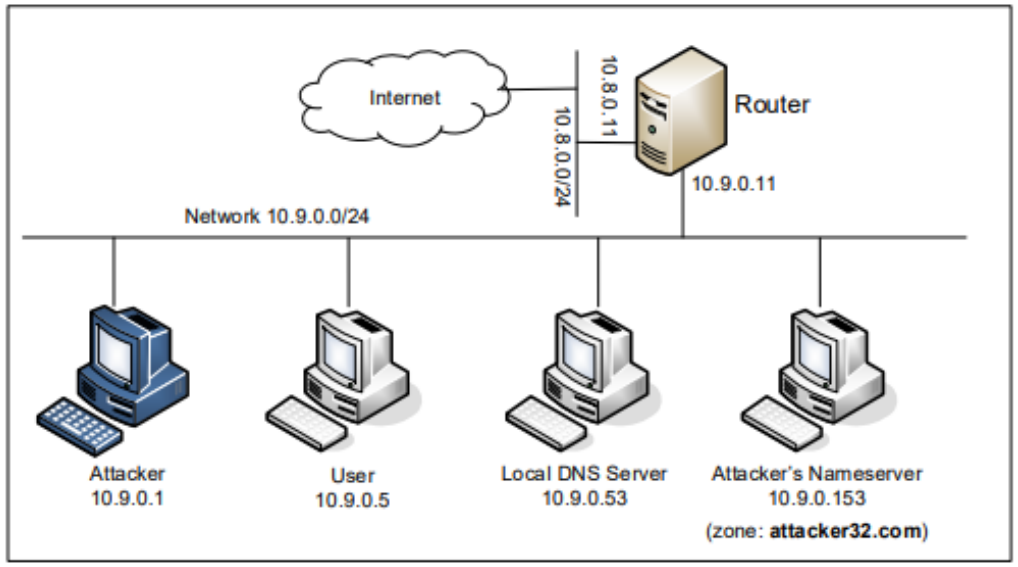
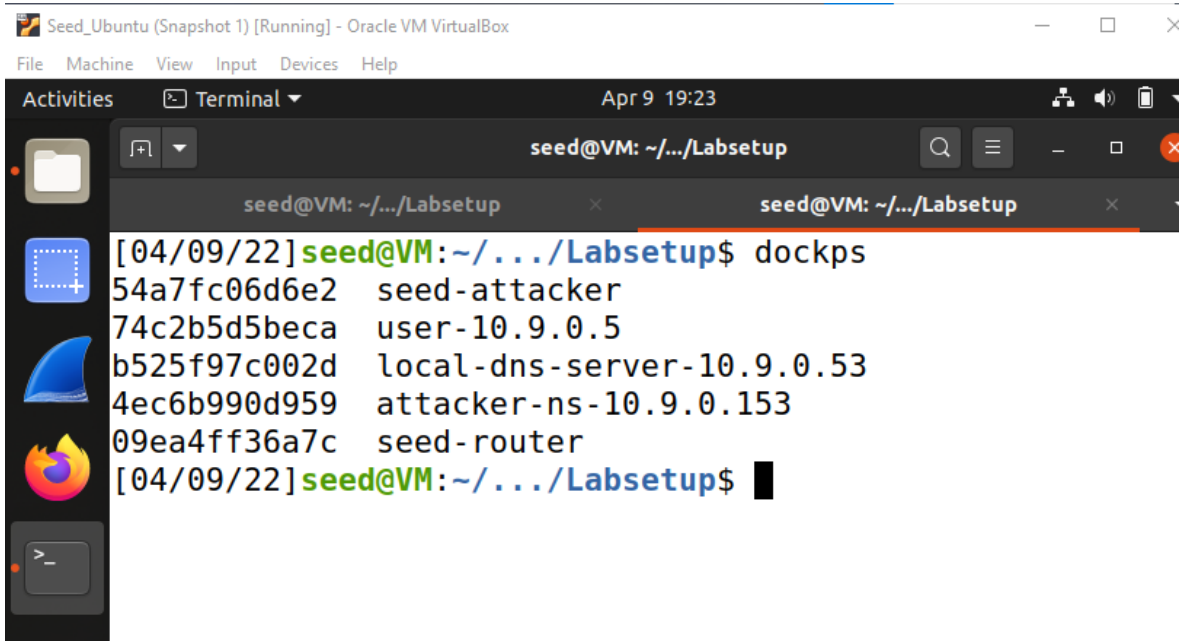
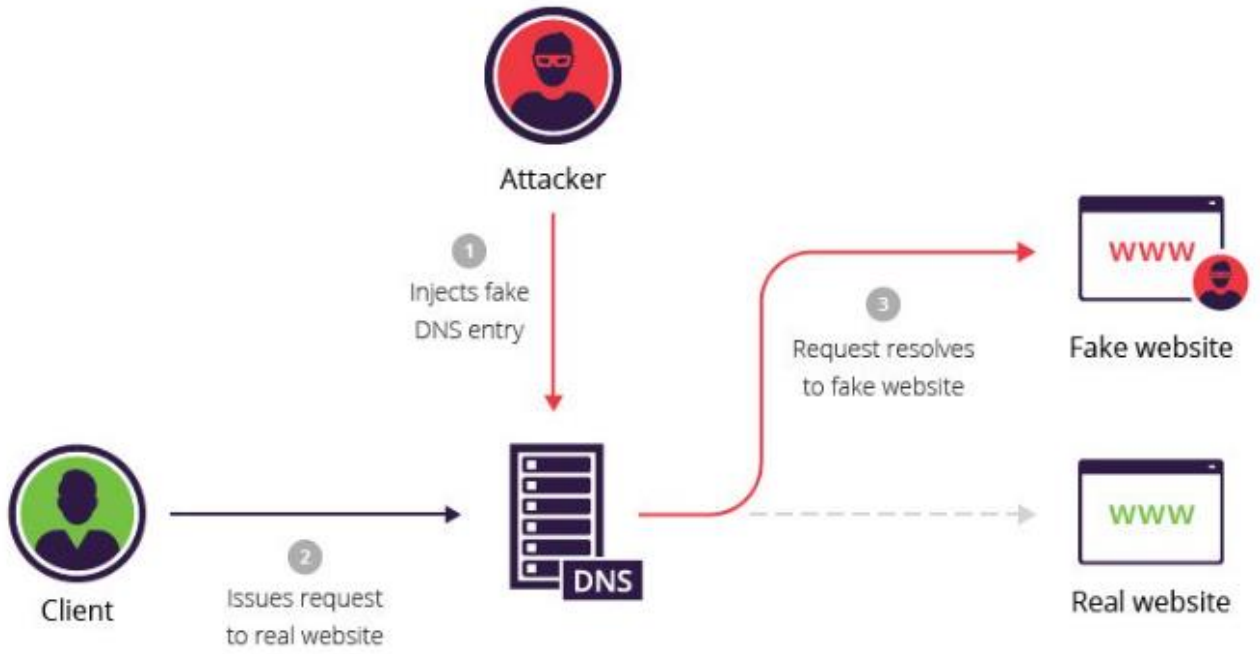


Figure 1: Lab environment setup



1.
Direct Spoofing Response to user



Sample Source – Direct spoofing

```
#!/usr/bin/env python3
from scapy.all import *
import sys

NS_NAME = "example.com"

def spoof_dns(pkt):
  if (DNS in pkt and NS_NAME in pkt[DNS].qd.qname.decode('utf-8')):
    print(pkt.sprintf("{DNS: %IP.src% --> %IP.dst%: %DNS.id%}"))

    ip = IP(...)              # Create an IP object
    udp = UDP(...)            # Create a UPD object
    Anssec = DNSRR(...)       # Create an aswer record
    dns = DNS(...)            # Create a DNS object
    spoofpkt = ip/udp/dns     # Assemble the spoofed DNS packet
    send(spoofpkt)

myFilter = "..."     # Set the filter
pkt=sniff(iface='br-43d947d991eb', filter=myFilter, prn=spoof_dns)
```

2.
DNS Cache Poisoning

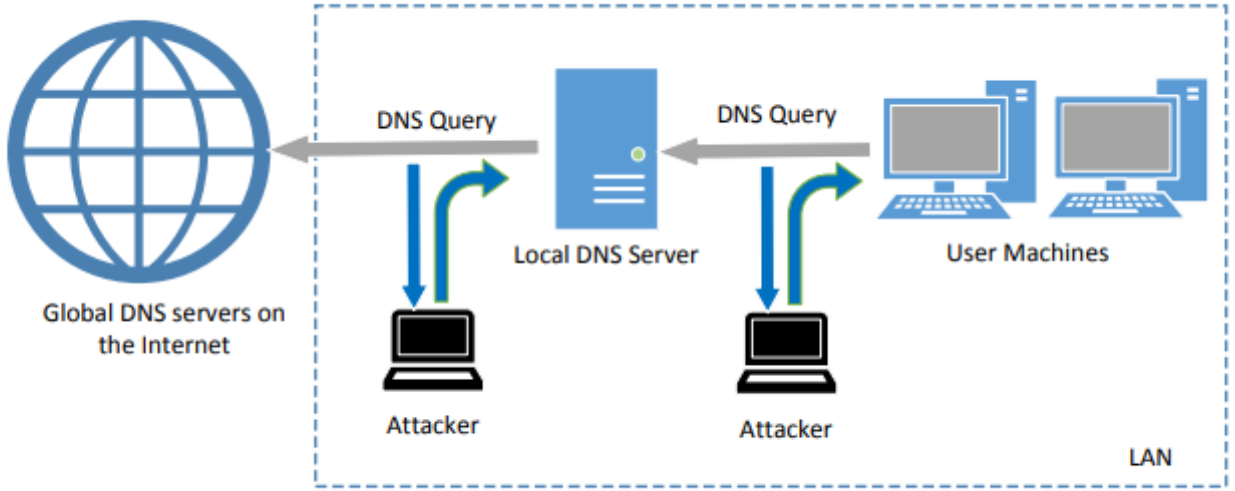
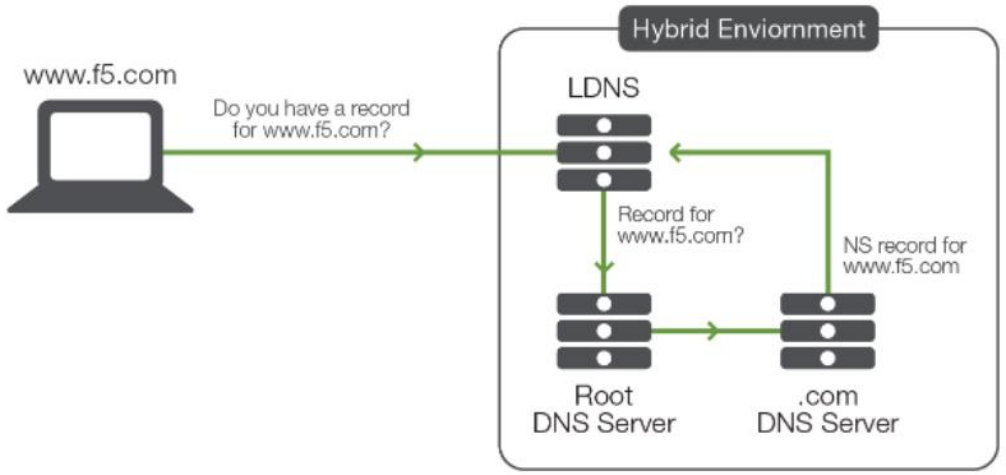


Figure 2: Local DNS Poisoning Attack

3. Spoof NS Records



- Command line tool to query Domain name systems
- Collects data about domain name servers
- Originally acronym "Domain Information Groper"

Roles and Responsibilities

- Sahil: Task 1
- Abhay: Task 2
- Rahul: Task 3

- Common: brainstorming and lab setup
- Common: python spoofing template

References

1) https://seedsecuritylabs.org/Labs_20.04/Files/DNS_Local/DNS_Local.pdf

2) https://www.youtube.com/watch?v=7Phz7s6XES0&t=1s

3) https://www.varonis.com/blog/dns-cache-poisoning