UNIVERSIDADE DE AVEIRO

universidade de aveiro

DNS Tunneling

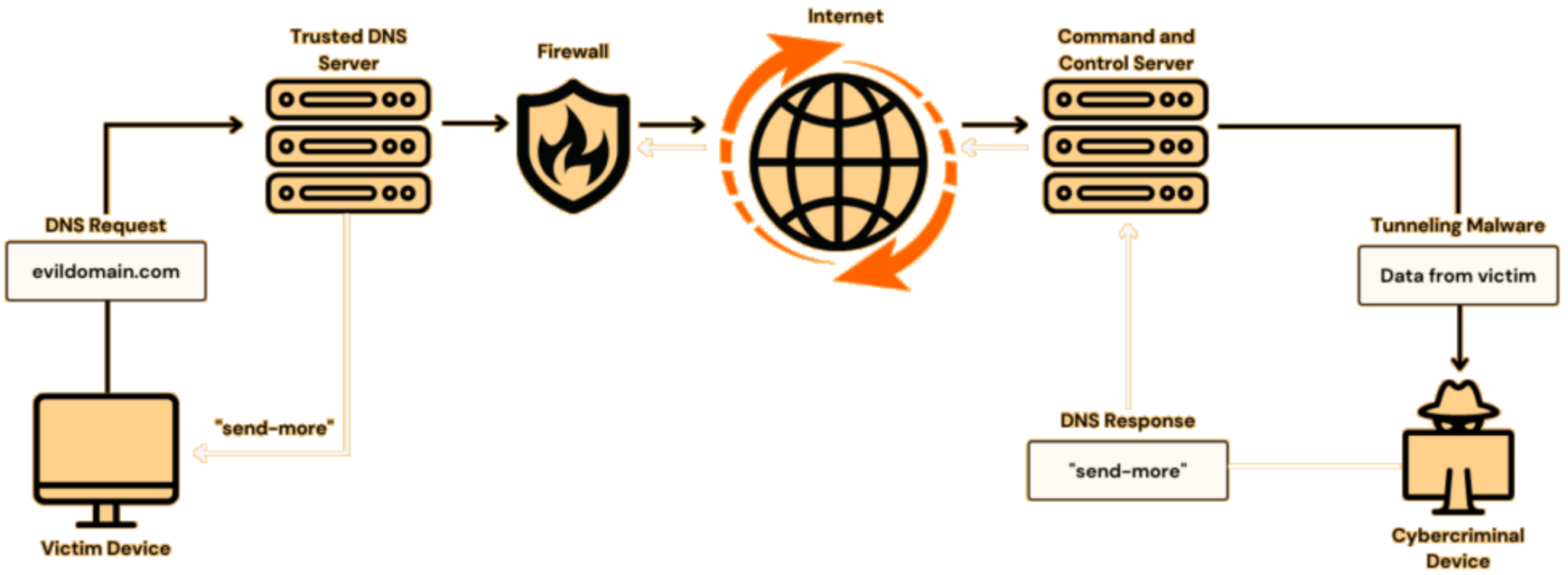
Técnicas de Percepção de Redes

Marta Oliveira 97613
Bruno Silva 97931

INDEX

Security problem

DNS tunneling is a technique used by attackers to bypass security measures and exfiltrate data or establish communication channels by encapsulating non-DNS traffic within DNS packets.



Importance of the security issue/solution

DNS tunneling is a significant security issue that can have far-reaching consequences.
Because DNS is not intended for general data transfer, often has less attention in terms of security monitoring. If DNS tunneling goes undetected, it represents a significant risk to an organization like:

Data Exfiltration

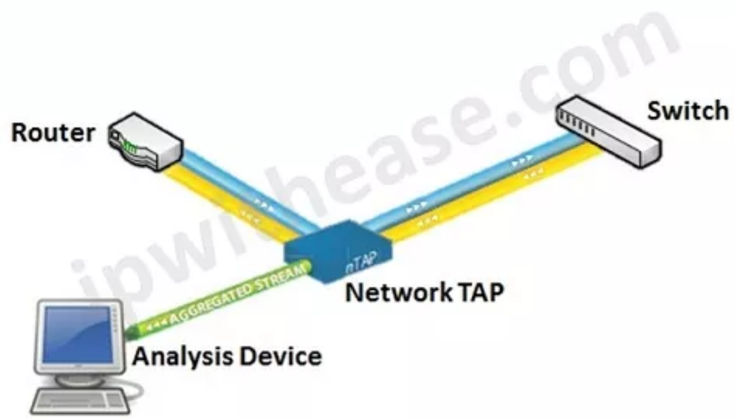
Malware Propagation

Command and control

DDoS Attacks

Data Accquisition (Real World Scenario)

- Between the client and the DNS server place a TAP interface that ‘listens’ to all the traffic.
- Capture the packets (on the TAP interface) with Wireshark.
- Perform operations on the client that send DNS queries to the server.
  - Web browsing.



Data Sources

Normal behaviour

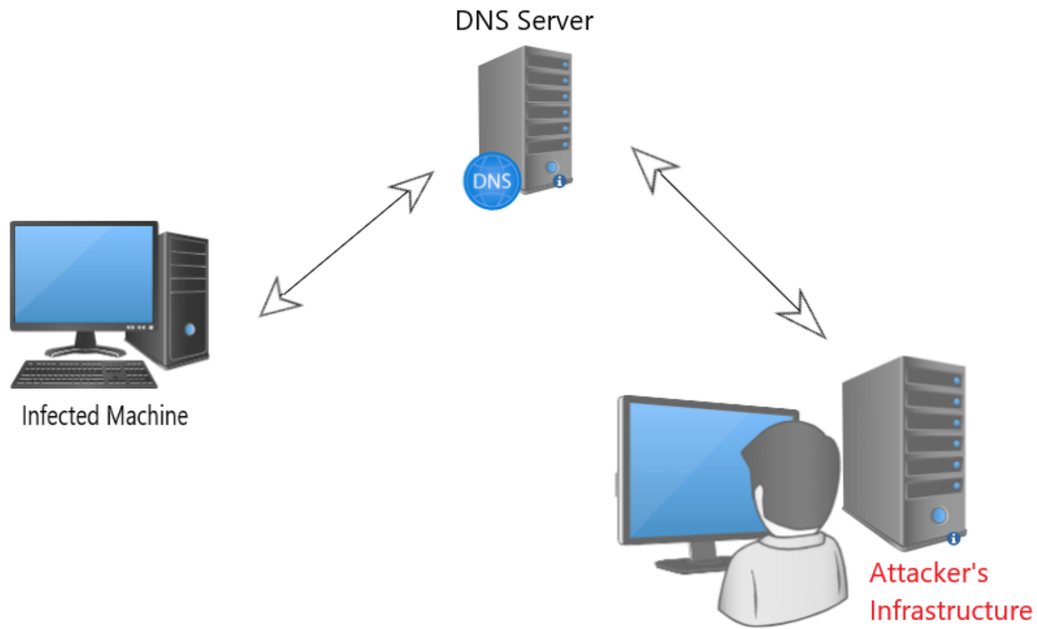
Capture traffic (DNS packets) between a computer and a DNS server in order to define the normal network behavior.

Malicious Behaviour

Capturing packets on the same computer where a DNS tunnel will be established between a client and a server (attacker).

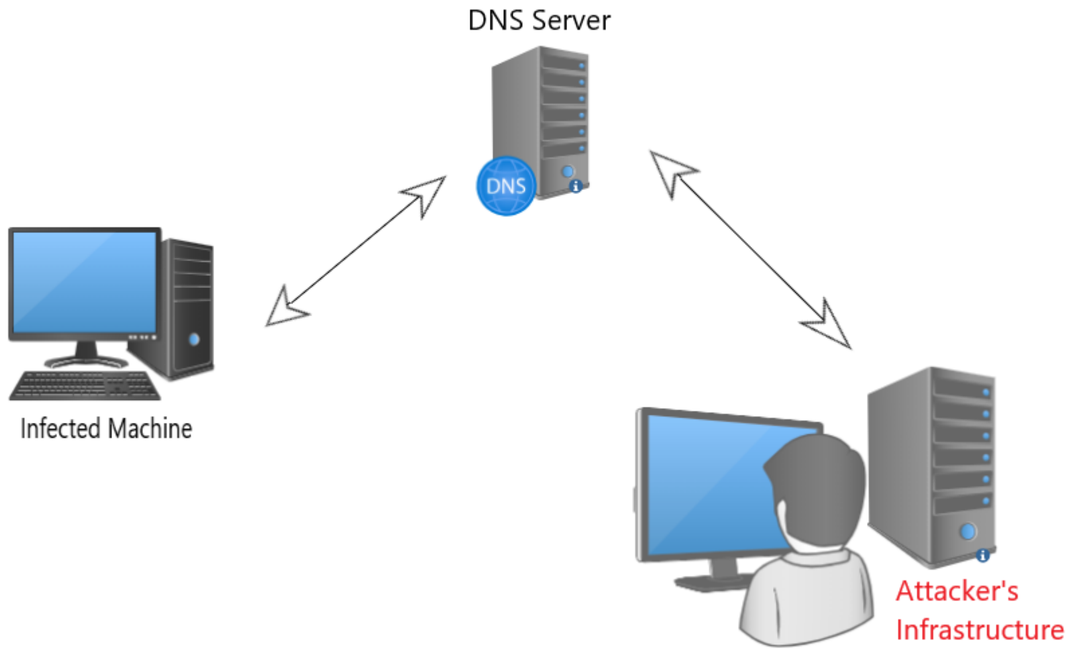
Test Scenario

- Creation of a Virtual Machine that will act as a client
- Connect the virtual machine to a virtual router or switch in your simulated network.
- Set up a DNS Server
  - Add a Virtual Machine
  - install package bind9
  - configure the DNS server to act as a master server (zone) for the domain
- Implement Iodine tunnel
  - On the server, run: *./iodined -f ip_network test.com*
  - Enter a password.
  - On the client, run: ./iodine -f -r server_ip test.com
  - Enter the same password.



Test Scenario

- The client side component initiates a DNS request.
- The client is connected to a DNS Server that will redirect the traffic to the attacker’s machine.
- Extract data through the established tunnel



Data Processing

- **Anomaly Detection:** our goal is to identify unusual events or patterns in the data
  - Comparing the malicious dataset with the normal behaviour dataset

- **Data filtering:** DNS packets (traffic UDP) on port 53.

- **Data sampling/aggregation:**
  - Volume of DNS traffic (packet count)
    - per IP address
    - per domain
  - Time interval between communications

- **Observation process:**
  - Sliding Window
    - Sliding value: 1 minute
    - Width: 5 minutes

Features

- **Volume of DNS traffic per IP address**
  - Maximum
  - Mean, median, variance
  - Percentiles (98%, 95%)
  - Periods of Silence
    - Mean, median, variance
- **Volume of DNS traffic per domain**
  - Maximum
  - Mean, median, variance
  - Percentiles (98%, 95%)
  - Periods of Silence
    - Mean, median, variance
- **Time interval between communications**
  - Mean, median, variance
  - Percentiles (98%, 95%)

Webgraphy

https://www.prosec-networks.com/en/blog/dns-tunneling-erkennen/

https://www.giac.org/paper/gcia/1116/detecting-dns-tunneling/108367

https://github.com/yarrick/iodine