Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

Network Security

Exercise Sheet 05:
Domain Name System Security & Network Firewalls Part 1

Prof. Dr. Mathias Fischer, August See, Finn Sell

Summer semester 2024

Goals and Objectives Solve this task sheet in groups as you organized yourselves beforehand. Your solution should be handed in as a pdf document that describes your results and how you got there. Submit your group solution to this task sheet in Moodle. You should reach at least 50%.

1 Domain Name System Security 50%

Preliminaries To solve this exercise, you are going to apply passive DNS analysis. For that, you can use the database from *CIRCL*[1] **or any other passive DNS source**. For *CIRCL*, we can provide the following credentials:

Username: `students.informatik.uni-hamburg.de`
Password: `DWW/ymamruvwjRfwo8g8SFaCw1H8zYj5GlxBS8JVWgM=`

You will issue several requests to query the respective data source. To automate this, you can simply use a Python module named `PyPDNS` specific to *CIRCL*. More convenient is the command line tool `dnsdbq`[2]. To use `dnsdbq`, insert your credentials into the `~/.dnsdb-query.conf`-file as follows:

CIRCL_AUTH="<username>:<password>"

You can install `dnsdbq` tool on your Linux VM manually or by executing:

```
$ cd ~/Desktop
$ wget https://svs.informatik.uni-hamburg.de/teaching/rn/exercise/04/dns_setup.sh
$ chmod +x ./dns_setup.sh && ./dns_setup.sh
```

[1] https://www.circl.lu/services/passive-dns/
[2] https://github.com/dnsdb/dnsdbq

By default, `dnsdbq` uses the *dnsdb*. Invoke with `dnsdbq -u circl -n <domain>` to use the CIRCL database for your queries. Remember to configure the file `~/.dnsdb-query.conf` accordingly.

Security Notice During this exercise, you are going to analyze potentially malicious websites. Visiting those websites might lead to malware infections or cause legal consequences. Thus, **DO NOT** visit any websites you discover while solving this exercise. However, analyzing the websites with the given tools is safe as this ensures you retrieve data about the websites in question from third-party sources.

1.1 Investigating legal Websites

In the first exercise part, you will analyze some well-known legal websites. This allows you to understand and make use of the passive DNS analysis.

1.1.1 Passive DNS

First, we recapitulate passive DNS in theory. Please answer the following questions:

1. What is passive DNS?
2. How can investigations in cybercrime benefit from passive DNS analysis?
3. Name two factors that the quality of passive DNS analysis, i.e., the number of returned results, depends on.

1.1.2 IT Security News

Please use passive DNS to analyze the legal website `www.heise.de` according to the following questions:

1. How many IPv4 addresses exist for this site? List all addresses (i.e., `A` records) you found.
2. Is this site using IPv6 as well? If yes, list all addresses (i.e., `AAAA` records) you found.
3. Search for other Fully-Qualified Domain Names (FQDNs) that are also hosted on the first IPv4 address of `www.heise.de`.
4. List all FQDNs that share a common IPv6 address with `www.heise.de`.

1.1.3 University Website

Please use passive DNS to analyze the legal website `www.uni-hamburg.de`.

1. Answer the same questions as in the previous task.
   Hint: For this task, you might not be able to find a directly referenced `A` record, but `CNAME` records instead that you have to follow. In this case, continue with the most recent alias name.

2. In addition, find more domain names that do not directly resolve to the IP address of `www.uni-hamburg.de` but also indirectly via the respective `CNAME`.

1.2 Investigating illegal Websites

Please use passive DNS to analyze the illegal streaming website `kinox.to`.
Hint: This website may not exist anymore, so you can also investigate other illegal websites. You presume that more streaming websites are hosted within the same address block 104.28.21.0/24.

1. Search for FQDNs that are hosted within this block. Describe your working steps.

2. You might have noticed that most of the returned results look meaningless. Therefore, you think of filtering all the FQDNs by meaningful search strings such as `stream`. Come up with at least four more appropriate search strings.

3. Apply your search strings to the full list of FQDNs and list the filtered names.

2 DNS and Firewall Evasion 50%

2.1 DNS Mechanisms and Evasion Techniques

- Why is DNS often used to bypass firewalls, and why is this a popular attack vector?

- Explain the process of how a DNS tunnel works from the client request through to the response.

- How would you further cloak traffic via DNS tunneling? While there are approaches known in the internet or ChatGpt, try to come up with your own solution as this is more a creative task and no points are deducted for inefficient solutions. Be creative, we want to bypass firewalls and IDS systems. Provide a detailed description and analyze the overhead involved. Give concrete numbers and percentages, e.g., for actual data transmission rate.

2.2 DoH, DoT Implementation and Analysis

- Implement a subset of DNS over HTTPS (DoH) and DNS over TLS (DoT) to query an A record. Demonstrate the implementation by querying a public DNS server.
- What are the drawbacks of DoH and DoT, and how could these drawbacks be addressed?