

Detecting Exfiltration (DNS)

Attackers employ **DNS-based exfiltration** due to its reliability, stealthiness, and the fact that DNS traffic is often allowed by default in network firewall rules. By embedding data within DNS queries and responses, attackers can bypass security controls and exfiltrate data covertly. Below is a detailed explanation of this technique and detection methods:

How DNS Exfiltration Works:

- **Initial Compromise:** The attacker gains access to the victim's network, typically through malware, phishing, or exploiting vulnerabilities.
- **Data Identification and Preparation:** The attacker locates the data they want to exfiltrate and prepares it for transmission. This usually involves encoding or encrypting the data and splitting it into small chunks.
- **Exfiltration via DNS:** The attacker sends the data in the subdomains of DNS queries, utilizing techniques such as DNS tunneling or fast flux. They typically use a domain under their control or a compromised domain for this purpose. The attacker's DNS server receives the queries, extracts the data, and reassembles it.
- **Data Retrieval and Analysis:** After exfiltration, the attacker decodes or decrypts the data and analyzes it.

How DNS Exfiltration Traffic Looks Like

8967 196.451321	192.168.38.102	192.168.38.104	DNS	138 Standard query response 0x4e2b A www.111edd479a7512c9c.7c9a5671.456c54f2.blue.letsghunt.online A 0.0.0.0
8968 196.452214	192.168.38.104	192.168.38.102	DNS	122 Standard query 0x8f5a A www.11483ec878e733131.8c9a5671.456c54f2.blue.letsghunt.online
8971 196.592143	192.168.38.102	192.168.38.104	DNS	138 Standard query response 0x8f5a A www.11483ec878e733131.8c9a5671.456c54f2.blue.letsghunt.online A 0.0.0.0
8972 196.593084	192.168.38.104	192.168.38.102	DNS	122 Standard query 0x0805 A www.1f5e9474847b08157.9c9a5671.456c54f2.blue.letsghunt.online
8983 196.749783	192.168.38.104	192.168.38.102	DNS	122 Standard query 0x0805 A www.1f5e9474847b08157.9c9a5671.456c54f2.blue.letsghunt.online
8984 196.765666	192.168.38.102	192.168.38.104	DNS	138 Standard query response 0x0805 A www.1f5e9474847b08157.9c9a5671.456c54f2.blue.letsghunt.online A 0.0.0.0
8985 196.766564	192.168.38.104	192.168.38.102	DNS	122 Standard query 0x9942 A www.114cbea090a81874a.ac9a5671.456c54f2.blue.letsghunt.online
8986 196.907655	192.168.38.102	192.168.38.104	DNS	138 Standard query response 0x9942 A www.114cbea090a81874a.ac9a5671.456c54f2.blue.letsghunt.online A 0.0.0.0
8987 196.908569	192.168.38.104	192.168.38.102	DNS	122 Standard query 0x2d8c A www.10db7634eade0b736.bc9a5671.456c54f2.blue.letsghunt.online
9015 197.004357	192.168.38.102	192.168.38.104	DNS	138 Standard query response 0x2d8c A www.10db7634eade0b736.bc9a5671.456c54f2.blue.letsghunt.online A 0.0.0.0
9016 197.004148	192.168.38.104	192.168.38.102	DNS	122 Standard query 0x59bd A www.1d5aee37e1c25ba02.cc9a5671.456c54f2.blue.letsghunt.online
9017 197.199001	192.168.38.102	192.168.38.104	DNS	138 Standard query response 0x59bd A www.1d5aee37e1c25ba02.cc9a5671.456c54f2.blue.letsghunt.online A 0.0.0.0
9018 197.200130	192.168.38.104	192.168.38.102	DNS	122 Standard query 0x7809 A www.1d4f517cdcfc8807c2.dc9a5671.456c54f2.blue.letsghunt.online
9019 197.339166	192.168.38.102	192.168.38.104	DNS	138 Standard query response 0x7809 A www.1d4f517cdcfc8807c2.dc9a5671.456c54f2.blue.letsghunt.online A 0.0.0.0
9020 197.340009	192.168.38.104	192.168.38.102	DNS	122 Standard query 0xd1f9 A www.14d71a77201813b75.ec9a5671.456c54f2.blue.letsghunt.online
9022 197.480990	192.168.38.102	192.168.38.104	DNS	138 Standard query response 0xd1f9 A www.14d71a77201813b75.ec9a5671.456c54f2.blue.letsghunt.online A 0.0.0.0
9023 197.482195	192.168.38.104	192.168.38.102	DNS	122 Standard query 0xf371 A www.1e3723505f4eb0d07.fc9a5671.456c54f2.blue.letsghunt.online
9026 197.619489	192.168.38.102	192.168.38.104	DNS	138 Standard query response 0xf371 A www.1e3723505f4eb0d07.fc9a5671.456c54f2.blue.letsghunt.online A 0.0.0.0
9027 197.628375	192.168.38.104	192.168.38.102	DNS	115 Standard query 0x56c0 A www.1aa649b2d.1b9a5671.456c54f2.blue.letsghunt.online
9043 197.757677	192.168.38.102	192.168.38.104	DNS	131 Standard query response 0x56c0 A www.1aa649b2d.1b9a5671.456c54f2.blue.letsghunt.online A 0.0.0.0

Let's now navigate to the bottom of this section and click on "Click here to spawn the target system!". Then, access the Splunk interface at [https://\[Target IP\]:8000](https://[Target IP]:8000) and launch the Search & Reporting Splunk application. The vast majority of searches covered from this point up to end of this section can be replicated inside the target, offering a more comprehensive grasp of the topics presented.

Additionally, we can access the spawned target via RDP as outlined below. All files, logs, and PCAP files related to the covered attacks can be found in the `/home/htb-student` and `/home/htb-student/module_files` directories.

```
● ● ● Detecting Exfiltration (DNS)
```

```
MisaelMacias@htb[/htb]$ xfreerdp /u:htb-student /p:'HTB@cademy_stdnt!' /v:[Target IP] /dynamic-res
```

Related Evidence

- Related Directory: `/home/htb-student/module_files/dns_exf`
- Related Splunk Index: `dns_exf`
- Related Splunk Sourcetype: `bro:dns:json`

[Resources](#)[Go to Questions](#)

Table of Contents

Leveraging Windows Event Logs

- 📁 Detecting Common User/Domain Recon ☒
- 📁 Detecting Password Spraying ☒
- 📁 Detecting Responder-like Attacks ☒
- 📁 Detecting Kerberoasting/AS-REProasting ☒
- 📁 Detecting Pass-the-Hash ☒
- 📁 Detecting Pass-the-Ticket ☒
- 📁 Detecting Overpass-the-Hash ☒
- 📁 Detecting Golden Tickets/Silver Tickets ☒
- 📁 Detecting Unconstrained Delegation/Constrained Delegation Attacks ☒
- 📁 Detecting DCSync/DCShadow ☒

Leveraging Splunk's Application Capabilities

- 📁 Creating Custom Splunk Applications ☒

Leveraging Zeek Logs

- 📁 Detecting RDP Brute Force Attacks ☒
- 📁 Detecting Beaconing Malware ☒
- 📁 Detecting Nmap Port Scanning ☒
- 📁 Detecting Kerberos Brute Force Attacks ☒
- 📁 Detecting Kerberoasting ☒
- 📁 Detecting Golden Tickets ☒
- 📁 Detecting Cobalt Strike's PSExec ☒
- 📁 Detecting Zerologon ☒
- 📁 Detecting Exfiltration (HTTP) ☒
- 📁 Detecting Exfiltration (DNS) ☒
- 📁 Detecting Ransomware ☒

Skills Assessment

Detecting DNS Exfiltration With Splunk & Zeek Logs

Now let's explore how we can identify DNS exfiltration, using Splunk and Zeek logs.

```
index=dns_exf sourcetype="bro:dns:json"
| eval len_query=len(query)
| search len_query>=40 AND query!="*.ip6.arpa*" AND query!="*amazonaws.com*" AND query!="*._googlelec
| bin _time span=24h
| stats count(query) as req_by_day by _time, id.orig_h, id.resp_h
| where req_by_day>60
| table _time, id.orig_h, id.resp_h, req_by_day
```

New Search

Save As Create Table View Close

1 index=dns_exf sourcetype="bro:dns:json"
2 | eval len_query=len(query)
3 | search len_query>=40 AND query!="*.ip6.arpa*" AND query!="*amazonaws.com*" AND query!="*._googlelec.*" AND query!="*_ldap.*"
4 | bin _time span=24h
5 | stats count(query) as req_by_day by _time, id.orig_h, id.resp_h
6 | where req_by_day>60
7 | table _time, id.orig_h, id.resp_h, req_by_day

All time

17116 events (before 8/20/23 3:36:31.000 AM) No Event Sampling

Job

Fast Mode

Events Patterns Statistics Visualization

20 Per Page Format Preview

_time	id.orig_h	id.resp_h	req_by_day
2021-08-26 17:00:00	192.168.38.104	192.168.38.102	17116

VPN Servers

Warning: Each time you "Switch", your connection keys are regenerated and you must re-download your VPN connection file.

All VM instances associated with the old VPN Server will be terminated when switching to a new VPN server.

Existing PwnBox instances will automatically switch to the new VPN server.

US Academy 3

Medium Load

PROTOCOL

UDP 1337 TCP 443

DOWNLOAD VPN CONNECTION FILE



Connect to Pwnbox

Your own web-based Parrot Linux instance to play our labs.

Pwnbox Location

UK

139ms

Terminate Pwnbox to switch location

Start Instance

1 / 1 spawns left

Waiting to start...

☐ Enable step-by-step solutions for all questions ⓘ ✨

Questions

Answer the question(s) below to complete this Section and earn cubes!



Download VPN
Connection File

Target(s): [Click here to spawn the target system!](#)

+ 0 📦 Use the "dns_exf" index and the "bro:dns:json" sourcetype. Enter the attacker-controlled domain as your answer. Answer format: __

letsgohunt.online

Submit

← Previous

Next →

✔ Mark Complete & Next

Powered by HACKTHEBOX

