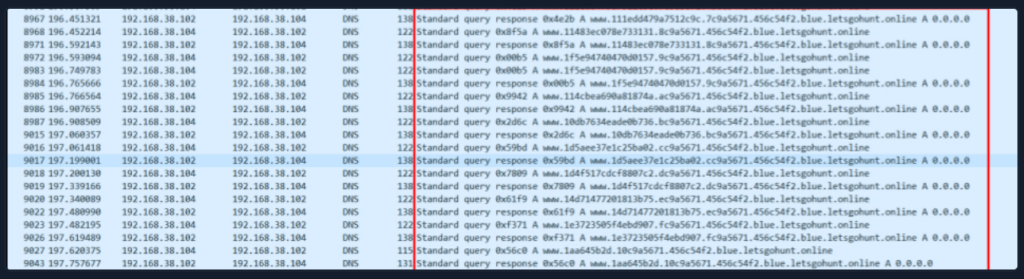
Detecting Exfiltration (DNS)

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



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 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.

Detecting Exfiltration (DNS)

```
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!="*._googlec
| 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
```

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 spawns left

Skills Assessment

My Workstation

OFFLINE

Start Instance

∞ / 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