**DNS Tunneling and Exfiltration**

DNS data exfiltration is a way to exchange data between two computers without any direct connection. The data is exchanged through DNS protocol on intermediate DNS servers. During the exfiltration phase, the client makes a DNS resolution request to an external DNS server address. Instead of responding with an A record in response, the attacker's name server will respond back with a CNAME, MX or TXT record, which allows a large amount of unstructured data to be sent between attacker and victim.

The purpose of the project is to develop detection algorithms that will detect when an infected machine within the protected network is exfiltrating data to an external server, using such techniques.

[Some] References:

- https://www.akamai.com/blog/news/introduction-to-dns-data-exfiltration
- https://www.giac.org/paper/gcia/1116/detecting-dns-tunneling/108367

**Weblogs to Detect attacks**

In any security scenario – even though we try to ensure that we do as best as we can to protect the systems — we need to consider the possibility that we could do better. We need to learn from day-to-day traffic, from ways by which hackers attack our system, and use that to improve our WAF rules.

Usually, before a hacker is successfully able to breach the website, he/she would probably have made a few unsuccessful attempts. These attempts if not blocked by WAF would be available as unusual entries in the web server logs. Also, in the normal operation of the web apps, regular users would be using certain URLs, making a certain type of requests, etc. This normal behavior would result in certain log entries in the web server access logs. Security admins operating the website should be intimately familiar with normal web server logs corresponding to the normal use of their web apps. Thus, when unusual entries arise in the web server access logs, they represent anomalies. In some cases, if a LFI vulnerability is available, the attack can be performed through the logs itself.

The purpose of this project is to detect in progress or previous attacks based solely on weblogs.

[Some] References:

- https://medium.com/@p.matkovski/detection-of-php-web-shells-with-access-log-waf-and-audit-deamon-e798d4c95ec
- https://www.acunetix.com/blog/articles/using-logs-to-investigate-a-web-application-attack/

**Attack Detection with Web Proxy Logs**

Web proxy logs provide valuable information. The purpose of a web proxy is to relay URL requests from clients to a server, receive the responses from the server and send them back to the appropriate clients. The web proxy acts as a gateway between the Internet and browsers on a local network.

Web Proxies generate a common set of information that can be used for threat hunting and detection. This information contains Duration, HTTP Status, Bytes In, Bytes Out, Protocol, HTTP Method, HTTP Version, URL Category, URL Hostname, URL Path, URL Query, Mime Type, File Name, User-Agent.

The purpose of this project is to detect in progress or previous attacks based solely on proxy weblogs.

[Some] References:

- https://link.springer.com/content/pdf/10.1007/0-387-36891-4_20.pdf
- https://posts.bluraven.io/threat-hunting-and-detection-with-web-proxy-logs-58094cae3537

**Data Exfiltration Detection from Netflow**

By definition, data exfiltration is the unauthorized copying, transfer, or retrieval of data from a computer or server. It is a malicious activity performed through various different techniques, typically by cybercriminals over the internet or other network.

One of the many benefits of NetFlow and metadata is that you have quick access to the most valuable information on your network. You have details on the source and destination IPs, ports used, application details (depending on your exports), latency, etc., which gives you a good representation of what is taking place on your network. By leveraging this information, you can identify problems quickly, and you can determine root-cause without needing full packet capture to understand what's taken place.

The purpose of this project is to determine whether a data exfiltration attack is has happened during a week's netflow capture, detection based solely on netflow.

[Some] References:

- https://repository.tudelft.nl/islandora/object/uuid%3A19aa873d-b38d-4133-bcf8-7c6c625af739
- https://pberba.github.io/security/2019/10/08/data-exfiltration/

**Detect network scans from Netflow**

Tracking network scanning activities can help researchers understand which services are being targeted. By monitoring the origins of the scanners, researchers can also identify compromised endpoints. If a host suddenly starts to scan a part of the organization, looking for open ports and services, it is a strong indicator that the host is compromised and an attacker is already inside the organization, trying to perform lateral movement.

The purpose of this project is to determine whether an attacker has already compromised the organization and is performing networks scans to laterally move inside the organization.

[Some] References:


- https://pure.tue.nl/ws/portalfiles/portal/52024831/20170321_Schneider_2016_bb844319.pdf
- https://blogs.gartner.com/anton-chuvakin/2016/07/21/can-i-detect-advanced-threats-with-just-flowsipfix/