Author: Antonio Maquesuel Daltro Santos

Data Analysis and Security Policy.

Table of Contents

1. Initial Data Analysis

Based on my analysis of the data provided, showing an excerpt of network traffic. I listed the main or potential menaces. Let's break down the whole thing:

1.1 - Main clues of Footprinting/Scanning

Type	Description
SQL Injection	Several strange entries: • **/reset-password?email=%27%20OR%202=2** • **/index.php?id = ' OR '2' = '2'**

	• **/login?username = admin&password=‘ OR ‘1’ = ‘1’**
Escape characters and attempts of bypassing	The attacker made some attempts of access using ‘/’ and ‘..’ in order of getting access to sensitive files and executables: • **/../../../../../../../../../../etc/shadow** • **/../../../../windows/system32/cmd.exe** • **/login?username = admin&password=‘ OR ‘1’ = ‘1’**
Cross-Site Scripting (XSS) Attack	An attack executed from a website or web-based application (e.g. a cross-site scripting attack used to steal credentials or a redirect to a site that exploits a browser vulnerability and installs malware). Those parts appear to be XSS attempts • **<script>alert('XSS')</script>** • **favicon.ico?search=<svg onload=alert(2)>** • **<iframe src='javascript:alert(2)'></iframe>**
Scans	A lot requests targeting **/view/require** and **/fish** probably comes from web scans or others tools. It’s a signal that they are advancing from Reconnaissance/Footprinting to another phase like Enumeration or even worse: Fingerprint, discover the OS and its version or web server version and some vulnerability to compromise the system.
Running scripts to detect vulnerabilities or even exploit one.	Many requests are coming from old sources/machines using **“Windows 98”** or trying to explore some known/old vulnerability.

2. Risk Identification and Policy Development

2.1 – Applying security policy

Considering that experienced hackers can disguise some unusual network traffic, or probes using NMAP, Nikito, Nessus and so many tools, just to be brief, we must be paranoid as much as we can. Some attacks have a great impact, like XSS and its variants.

All the data coming to our network or sent to the Internet must be considered neutral or malicious, but never take for granted or considered since the beginning as normal or common.

That's why I'd apply some of the following measures:

1) **All the Intranet access should be made using VPN for all the Company members.**
2) **All the workers and collaborators have to use 2FA auth and strong passwords.**
3) **Have a list of all devices and relate each one to just one worker (Notebooks, Stations, desktops and etc.).**
4) **Any attempt to access the Intranet coming from an IP outside of the VPN must be blocked.**
5) **Use Sniffers to detect some suspicious traffic. Or some customized solution/tool to analyse and detect traffic that it's not common in the network.**
6) **I really would avoid all the use of Windows, Chat GPT, Copilot, Whatsapp, Google Chrome, Microsoft Edge and so on and so forth. And I'd recommend the use of Signal, Brave browser, Ubuntu or another OS based on Linux/Unix, Docker and containerized applications. And for the last, customized AI Tool made by some Software Startup / IT Company or built by the IT Team from the Company itself. It could be annoying and very hard to implement. But we know for a several facts(like the Snowden leaked docs) that those Big Techs do not respect or protect our data. Expose the data of the company and its personnel using those service I listed above, it's very dangerous.**
7) **Red Team, Purple and Blue Team and all personnel working together and even if it's possible, buying or have information about new Zero Day Vulnerabilities. Maybe build some innovative partnership with Bugcrowd or HackerOne to be more prepare for the new cyber threats.**
8) **Use Honeypots to attract invaders and discover information about them. I will explain more later.**

3. Implementation

3.1. Counter Measures and Tools to Increase Security

As part of my plan to improve the security, I created a script to block IPs after a certain quantity of attempts or uncommon requests. Here is the DigitalShield.sh:

```
#!/bin/bash
if [ -z "$1" ]; then
    echo "Usage: $0 <SUSPICIOUS_IP_ADDRESS>"
    exit 1
fi
SUSPICIOUS_IP_ADDRESS=$1
sudo iptables -A INPUT -s $ SUSPICIOUS_IP_ADDRESS -j DROP
sudo iptables-save > /etc/iptables/rules.v4
echo "Blocked IP address: $ SUSPICIOUS_IP_ADDRESS"
```

After this, save and prepare for execution:

a) **chmod +x Digital-Shield.sh**
b) **./digital-shield.sh 200.220.***.*** (some suspicious IP)**

Beyond the script, we can use UFW interface for managing Iptables:

$ **sudo ufw deny from 200.220.***.***

Script for UFW:

```
#!/bin/bash

if [ -z "$1" ]; then
   echo "Usage: $0 200.220.***.*** "#IP ADDRESS
```

```
   exit 1
fi

200.220.***.*** =$1
sudo ufw deny from $200.220.***.***

echo "Blocked IP address: $200.220.***.*** "
```

4. Explanation and Documentation

4.1. Counter Measures and Tools to Increase Security

Not only the execution and pentests with conventional tools must be applied. I used my script as an example. I wrote with Nano and tested in my Kali Linux and my Ubuntu.

But we can made surprise attacks hiring a secret Red Team in order to see how the official defenders will react and perform to protect the company resources.

The second part i mentioned before, is about traps and honeypots to harvest the maximum of information about our attackers. Of course, i'd ask my superiors to get permission for such thing. It must be made in an environment secure and isolated from the
Private network of the enterprise. We could use several ways to allure and fool our eavesdroppers.

We could put some false private keys for crypto wallets or with little amount of money/cents.

Or put fake databases, API keys, authentication passwords, files in those honeypots.

It's serious and bit dangerous, but it would give us advantage in a possible investigation for the Police or a trial in a Court. Just because in this situation we can provide a lot evidence and information about our invaders. If they are doing those probes from another invaded network, we could contact the admins of those nets to discover who are those crackers and avoid future problems.

5. Innovation

5.1. AI and other technologies to add to our policy

Implement virtualization and containerization are really good approach and essentials today. EDRs and WAFs are “layers” to difficult incidents, but we should never trust 100%. The human “resource” is the most important. We can choose decentralized apps and blockchain solutions and others innovations to stay less dependent from Microsoft, Playstore, Appstore and others centralized service providers.

As I said earlier, it worth to produce a customized AI to catch and analysed traffic, PIDs, process and etc. If we really treasure security, those expenses are worth it. In a case like this, we can improve more and more and make our AI to grow in the direction we want. We wouldn’t waste our time creating fictional data to hide info about our company and throw them in Chat GPT, or worse, use the real assets and our real info to resolve and analysed data in Copilot or Chat GPT.

I am sure we are ***NOT*** secure with those Big Brothers out there, invading our privacy, collection so many things and creating a profile for each human being with all the things we do and consume. The same way happened in the last 8 or 10 years, that the enterprises realized how important it’s to worry about cybersecurity and not only take some actions after been invaded, i think that the protection of our private life, jobs and private documents will enter in the “radar” too.