

Operation Clear Water

May 15, 2024

Overview

An anonymous tip was sent to our agency, referring to a potential conversation between **Alex Zane**, head IT admin for **Waterworks Solutions**, and a yet unidentified person. These two messages were sent to us:

INTERCEPTED MESSAGE CFU-24-3246

I... Suppose you're right... Thales definitely seems to know what he's doing...!

Sent on 13:22 on 11/05/24 from cell phone
Owner/Alex Zane

INTERCEPTED MESSAGE CFU-24-3247

Exactly! Trust in the process and soon we'll be richer than you could ever imagine! Might even finally get that car I always wanted!

Sent on 13:26 on 11/05/24 from cell phone
Owner/Unidentified

Under normal circumstances this would be disregarded, but suspiciously, a few hours later, Waterworks Solutions **registered a new domain** under their company name. Moreover, codename '**Thales**' is already a quite well known criminal in the cyber space and a highly wanted one at that. As such, we request your immediate assistance.

All intrusion operations must be conducted exclusively under the Stinger OS Penetration and Cyber Attack Platform.

Goal 1: Assess Alex Zane's role in Thales's plan

As the **IT admin** for the company, Zane would absolutely be pivotal to the plan's success. **Investigate the possible threat** by accessing Waterworks Solutions' network. Use your **Information Gathering** modules to locate a vulnerability and then proceed to infiltrate their network via the use of your **Network Intrusion** modules. Their newly registered domain and the one you should investigate is "**knowthyself.hvm**". Once you gain access, try **digging** around for information on their IT department, and proceed from there.

Goal 2: Uncover Thales's identity and find evidence connecting him to the group's activities

We don't quite know what to expect, but we'll make sure to keep track of your progress as you search deeper and deeper. This is our chance to finally **take down Thales**. Their plan hasn't been finalized yet, but considering the tone of the message between Zane and Thales, they're definitely progressing at a good pace.

Your mission will end by finding the **HVM:Trading** service and **infiltrating it**. It's very possible that it's **hidden in plain sight**, but you'll need a **username** and a **password**, so I doubt they'll make it easy for you. Chances are that you will need to **use** your **Password Attack** module to **crack the password** needed. You should also have **found 5 variables** that you can use against him for the **password cracker**. **Good luck agent.**

Brief introduction of your available modules and tools

Overview

The **modules** available to you and the ones **you will need to use** are the ones **listed below**. **Real life resources** will also be provided **if you wish to learn more** about their **real life applications**.

You are also expected to make use of your **real life internet browser** while navigating through the network, as you will need to **obtain information** both **inside and outside** of the platform provided to you.

Information gathering:

DNS & Host Mapping:

Allows you to find the **subdomains of a domain** (website).

<https://www.kali.org/tools/dnsrecon/>

<https://medium.com/@0xbharath/a-penetration-testers-guide-to-sub-domain-enumeration-7d842d5570f6>

Host Fingerprint:

Identifies the **technologies** and **ports** used for a specific **subdomain**.

<https://www.avast.com/en-us/business/resources/what-is-port-scanning#pc>

<https://pentest-tools.com/website-vulnerability-scanning/website-scanner>

Exploit Database:

Used to find information on how to **exploit vulnerabilities** in a specific **technology/service**.

https://en.wikipedia.org/wiki/Common_Vulnerabilities_and_Exposures

https://cve.mitre.org/cve/search_cve_list.html

WMI Scanner:

Can either **scan** the internal network or **dig** into a network path to identify ports and **technologies/services** used. **Works only when connected to a network**.

<https://pentestlab.blog/2017/11/20/command-and-control-wmi/>

Air Crack:

Is able to both **scan the network** for **WiFi hotspots** as well as **download the log files** of said hotspots.

<https://developer.android.com/develop/connectivity/wifi/wifi-scan>

All intrusion operations must be conducted exclusively under the Stinger OS Penetration and Cyber Attack Platform.

Active Directory:

Used to access the **active directory**, providing you with **information** on the **company personnel** as well as potentially their policies or equipment. Just enter the **active directory path** and you will be **connected** to the corresponding active directory

<https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview>

Network Intrusion:

Foxacid Server:

Used to **exploit the vulnerabilities** found via the use of the **Exploit Database** module. There are three possible rootkits.

- **Assassin**: Used exclusively to **acquire information** from **internal paths**.
- **AfterMidnight**: Used to **gain access** to a **network**.
- **HVM:Mount**: Used for **infiltrating a network path** utilizing the **HVM:Trading** service.

Phone CID Backdoor:

Used to either **infiltrate a mobile device** or to **navigate** an already **exposed one**.

Password Attack:

Used to **make a password attack**. There are two possible types of attacks.

- **Basic**: Requires a **target url** (often an **internal path**) and a **username**. For this assignment, you'll need to use the **John the Ripper** password cracker with the **Rock You** password list. You can speed up the cracking process substantially by **inputting the correct information** about the **victim** to the right side of the module.
- **Hash**: Requires the use of a **password hash**. As with the basic attack, you will need the **John the Ripper** password cracker but instead of the **Rock You** password list, you'll need to select a **Rainbow Table**, which you should determine the **correct one** via your **in-platform investigation**.

<https://www.openwall.com/john/>

<https://www.kaspersky.com/resource-center/definitions/what-is-a-dictionary-attack>

Data forensic:

Xkeyscore Forensics:

Since this is a fairly complicated module, a **more extended overview** will be provided.

After you **acquire entities** to be used in **XKeyscore** (they can be either **people** or **organizations** and will be **highlighted**), you may then **search for any connection** between **up to 3 entities** via the module. **Select the entities** you wish to examine on the **left side**, and choose what kind of **information** you wish to find that **connects said entities** on the **right side**.

<https://en.wikipedia.org/wiki/XKeyscore>

All intrusion operations must be conducted exclusively under the Stinger OS Penetration and Cyber Attack Platform.

File Browser:

Similar to the **Active Directory** module, but for **standard network paths instead**. Used to **read** their **contents**.

Note Pad:

While **not required**, the Note Pad module is highly **recommended** to **keep and organize your notes** as you find more and more information.

Commands cheatsheet

In case you're feeling overwhelmed with some of the commands or if you're feeling lost in general, this section can guide you through specific actions.

Hacking and entering a system

Usually you will wanna **start** by using your **DNS & VHOST Mapping** tool, under Information Gathering. By using the **sfuzzer** command as explained in the module itself, you can **find** the corresponding **subdomains** for the site.

Then, you can **scan** said **subdomains** for **vulnerabilities** with your **Host Fingerprint** module, also under Information Gathering.

After you successfully identify a vulnerability, you can use your **Exploit Database** in the same category to **identify the methods** used to **exploit** the vulnerability.

Finally, you can use the **Foxacid Server** tool to **execute your attack**, providing the correct variables.

Once you successfully enter the network, you can use your **WMI Scanner** module to perform a **network scan** and proceed accordingly.