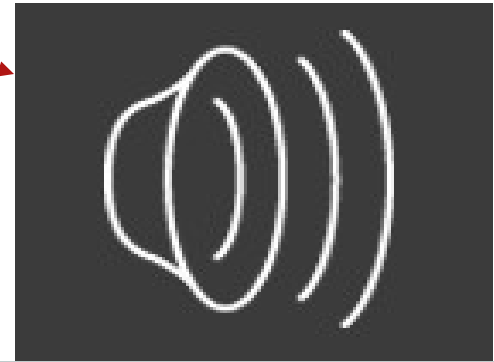
Digital Forensics Technology and Practices:

Project 2 – The Hacker Attacks

<Stephanie coffie>

<22/02/2023>

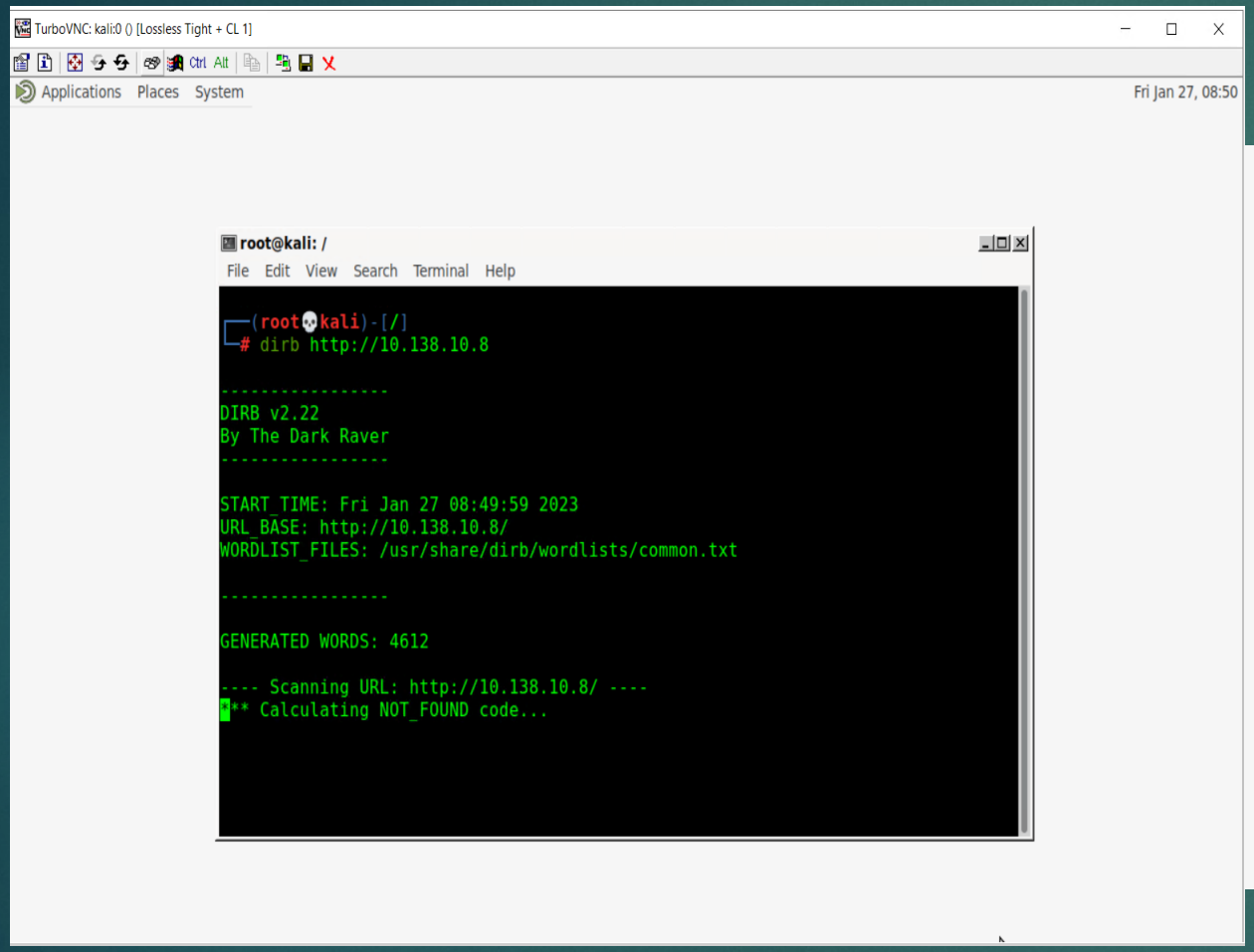
Example narration

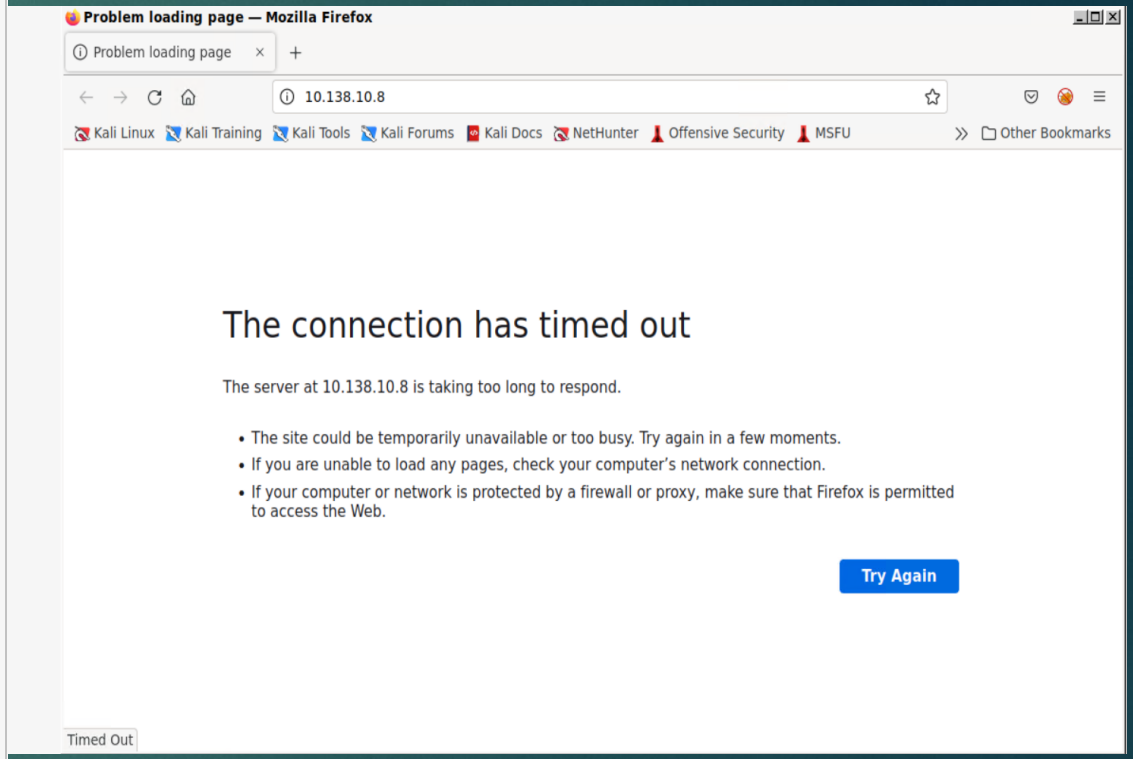


Project 2 - Introduction

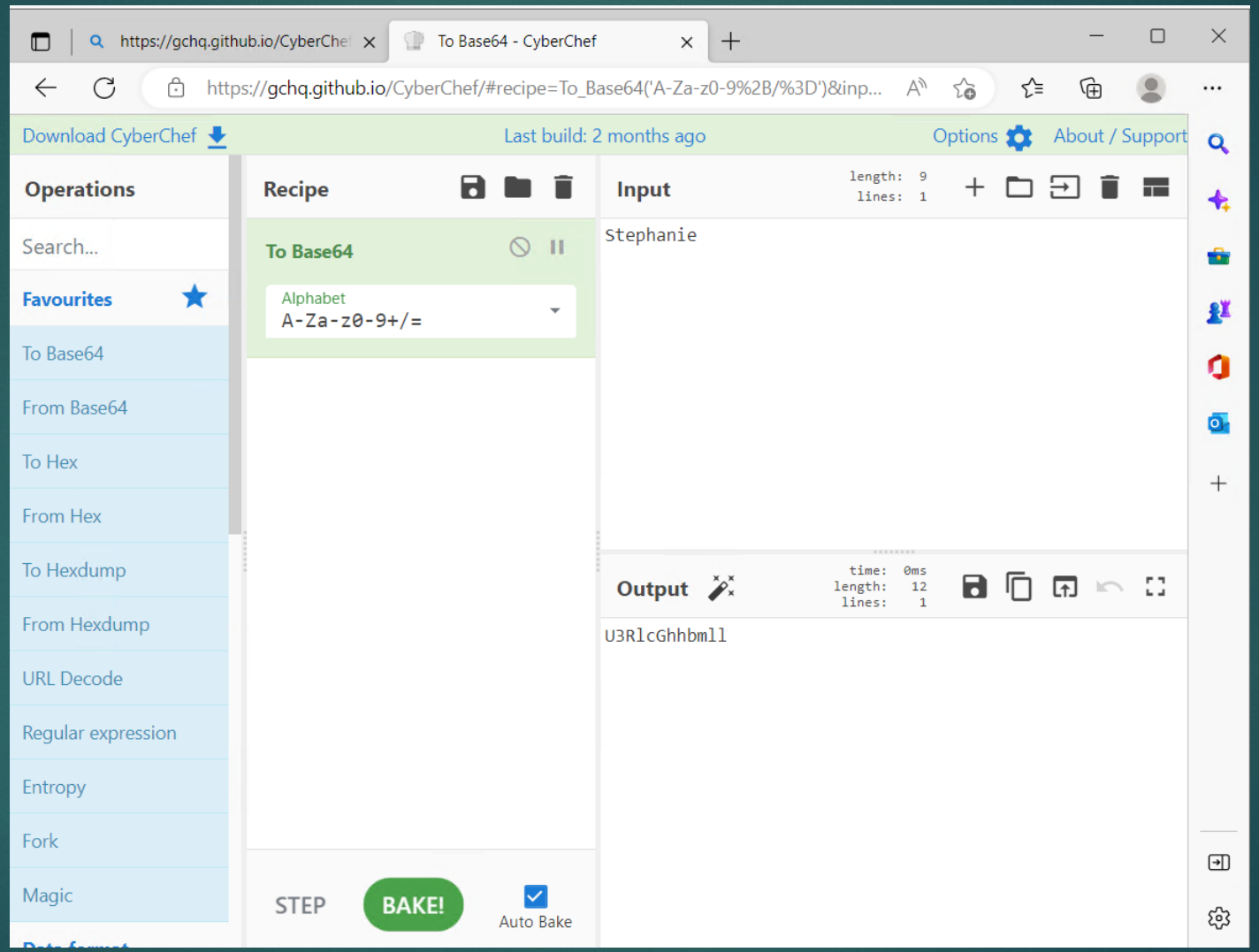
- Include Voice Narration in Your Slides
- A person who hacks into a computer system is a hacker. There are numerous reasons for hacking: malware installation, data theft or destruction, service disruption, and other activities Ethical hacking can also be carried out for the purpose of locating software flaws that need to be fixed.
- Bait and Switch: Hackers use Bait and Switch to purchase ad space on any website and then create a standout ad on the website's page. When a user visits that website, the majority of the time, they are persuaded to click on the advertisement because of how it looks to them, and when they do, they are taken to a malicious web page. Hackers can steal user data and install malicious code on the victim's system in this manner.
- What exactly is a cyber security artifact? Tracks are left behind by artifacts. They might be related to the footprints of the hacker or end user. However, the existence of artifacts is frequently unknown to end users. They are hard to manipulate, just like permanent footprints. Consequently, artifacts assist cyber security consultants in identifying the threat actors and the underlying causes of a data breach.
- Erase all of the directions provided in this text box when you submit the project

Conti’’


TurboVNC: kali:0 () [Lossless Tight + CL 1]
Ctrl Alt
Applications Places System
Fri Jan 27, 08:50
root@kali: /
File Edit View Search Terminal Help
(root kali)-[/]
dirb http://10.138.10.8
DIRB v2.22
By The Dark Raver
START_TIME: Fri Jan 27 08:49:59 2023
URL_BASE: http://10.138.10.8/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
GENERATED WORDS: 4612
---- Scanning URL: http://10.138.10.8/ ----
** Calculating NOT_FOUND code...

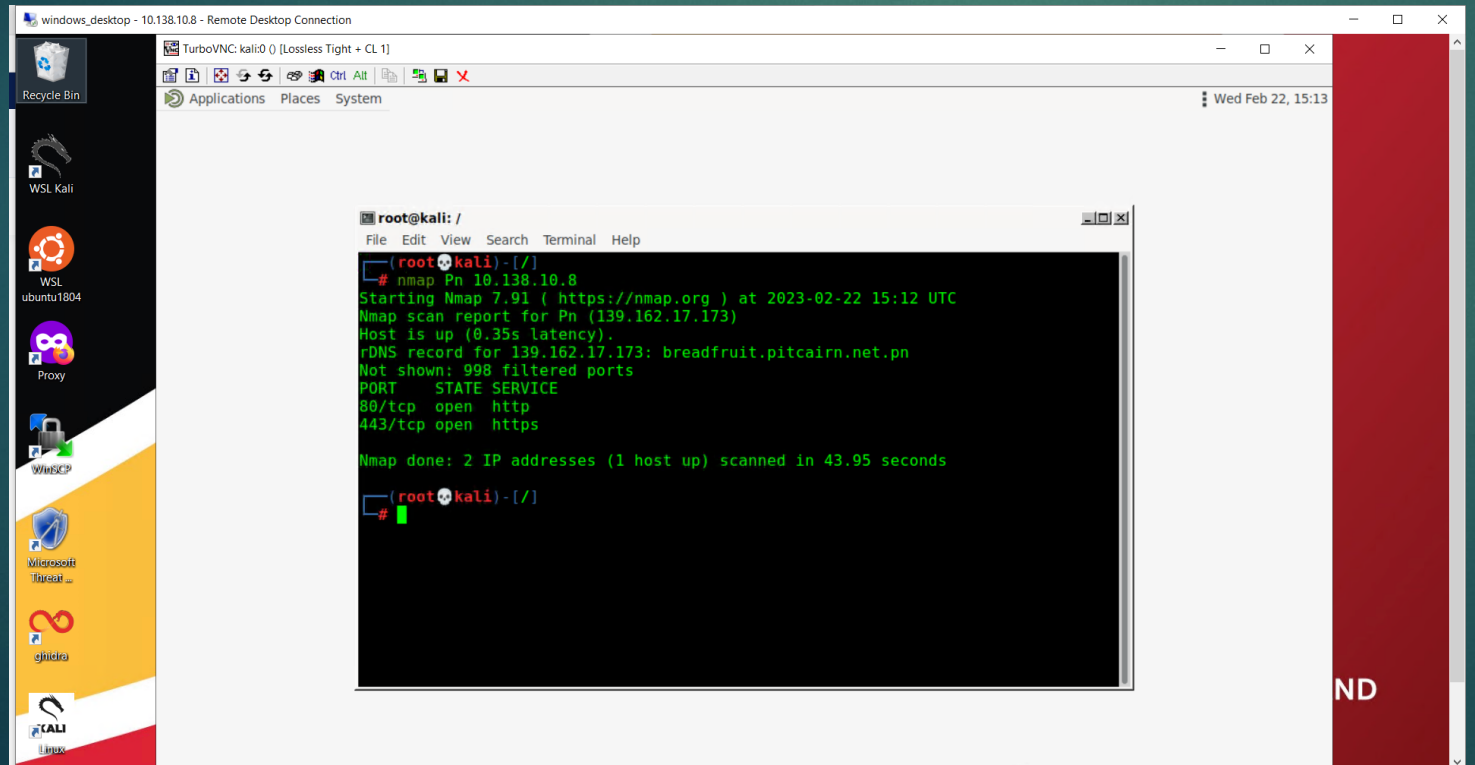

Problem loading page — Mozilla Firefox
Problem loading page
10.138.10.8
Kali Linux Kali Training Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Other Bookmarks
The connection has timed out
The server at 10.138.10.8 is taking too long to respond.
• The site could be temporarily unavailable or too busy. Try again in a few moments.
• If you are unable to load any pages, check your computer’s network connection.
• If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.
Try Again
Timed Out

Base64 Decode



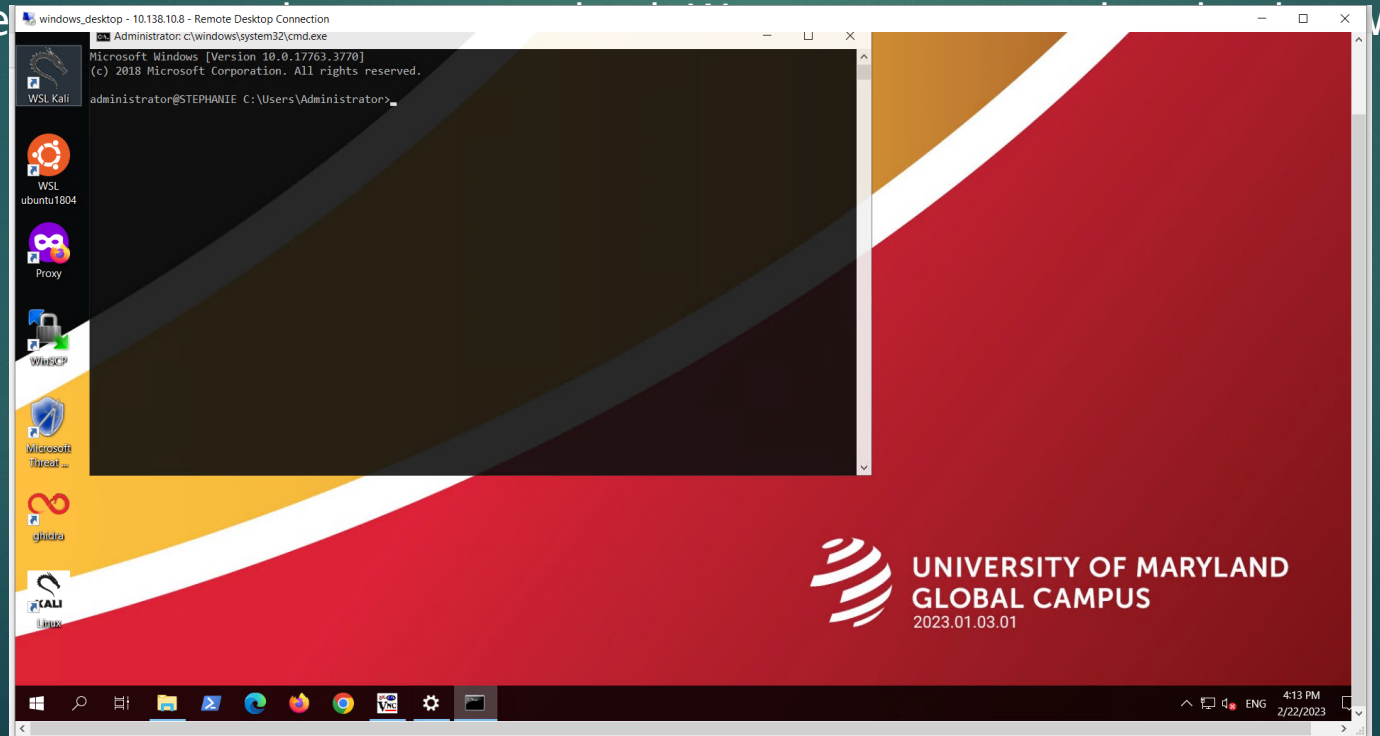
The attacker will map for more information

- To comprehend port configuration, some understanding of terminology is required. The following terms will assist you in comprehending the discussion:
- Port: a location on the network that can be addressed and used by the operating system to help differentiate traffic going to different applications or services.
- Sockets for the Web: a file descriptor that specifies the transfer protocol that will be used to handle the data, an associated port number, and an IP address.
- Binding: the process by which an application or service handles the data it inputs and outputs using an internet socket.
- Listening: When a service is bound to a port, protocol, or IP address in order to wait for requests from its clients, it is said to be "listening" on that port.



SSH into the Windows Victim

- The connection is not persistent, so if you stop typing, it will break. Tab does not work. You can't use vi, so you can't write files and must cat every file you want to read. There is no color (right, it's not a big deal, but still...) As a result, you can begin your investigation into the compromised instance with a clean slate.
- The SSH protocol supports a variety of authentication methods. The password-based authentication and the public key-based authentication are the most frequently used.
- We are not interested in the first one because we assume that we do not know the password of the user whose ...with keys. Let's check out this one.



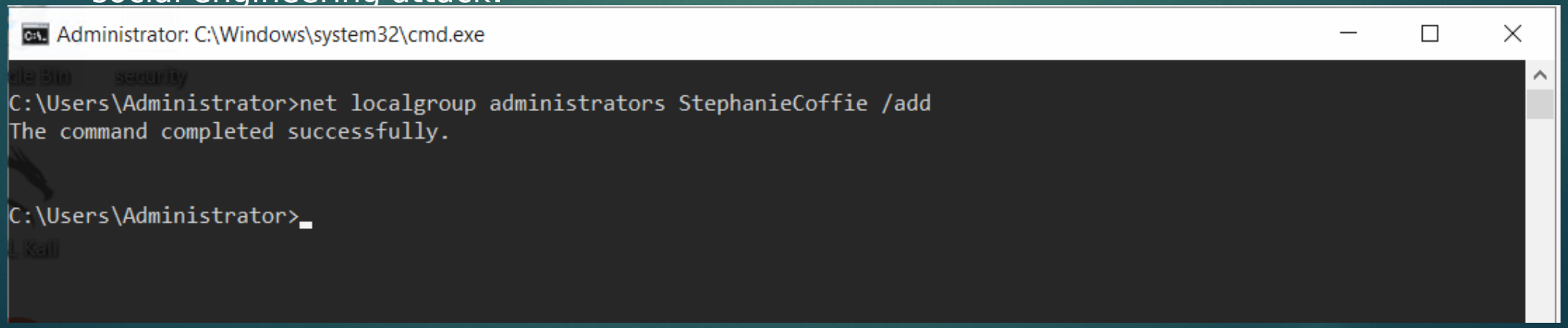
Add an Administrative Account

An attacker would add an administrator because of the following reasons:

Risk of getting in Malware Installation of unapproved software, downloading an attachment from an email, and visiting malicious websites are the most common ways for malware to spread. The majority of malicious software typically runs with the same rights as the logged-on user. The code can be executed on local machines with full admin rights without user notifications, putting the organization at risk of a wider attack. To gain access to computers, malware typically requires elevated privileges.

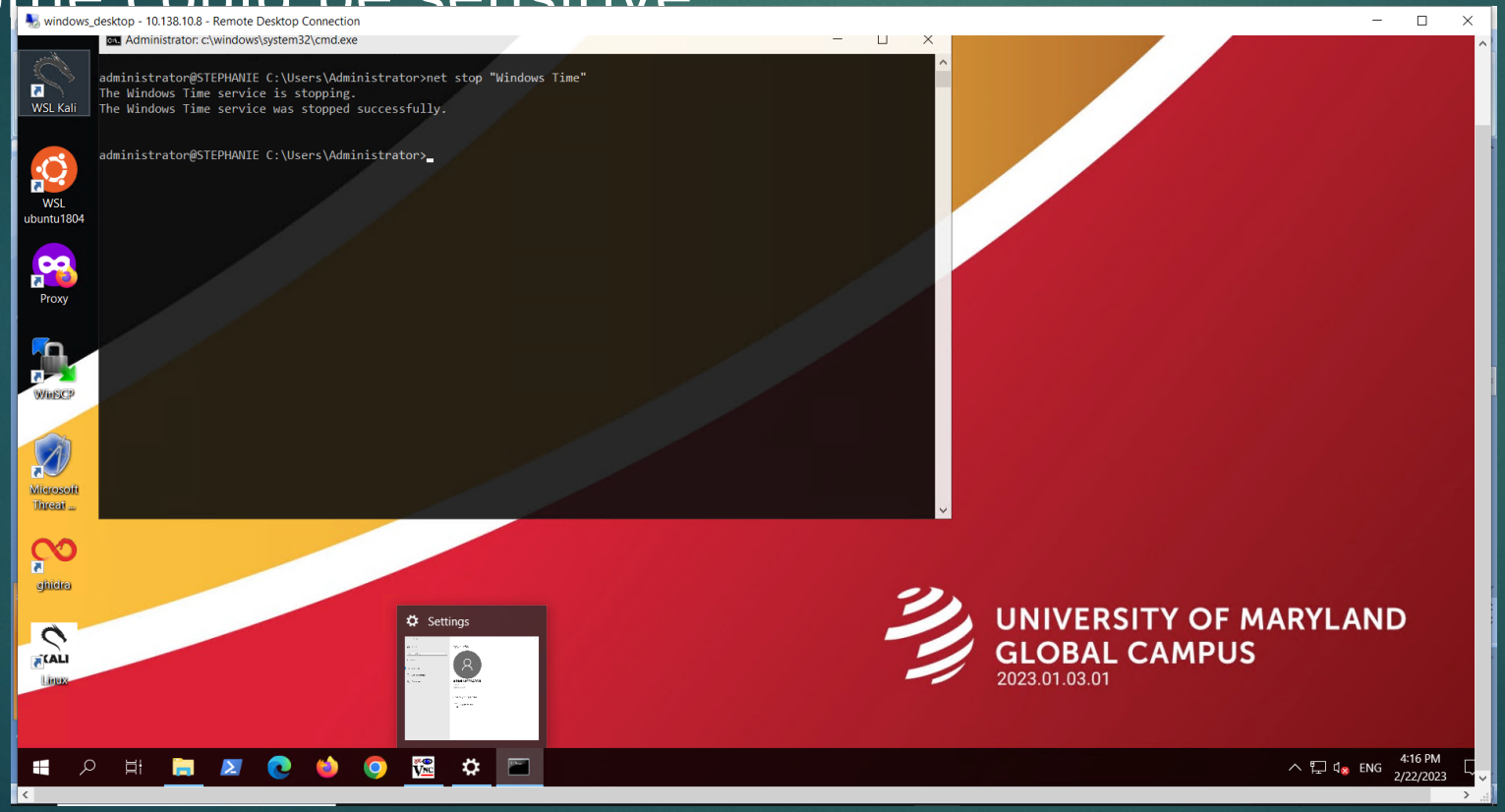
Hackers can use the all-powerful local admin access to bypass crucial security settings, run exploit code or tools, impersonate other logged-on accounts, delete system logs, and ultimately gain access to sensitive data.

- Windows caches the passwords as hashes to facilitate single-sign-on attacks and pass-the-hash attacks. Passing the hashes is all an attacker needs to gain access to a system, such as through a social engineering attack.



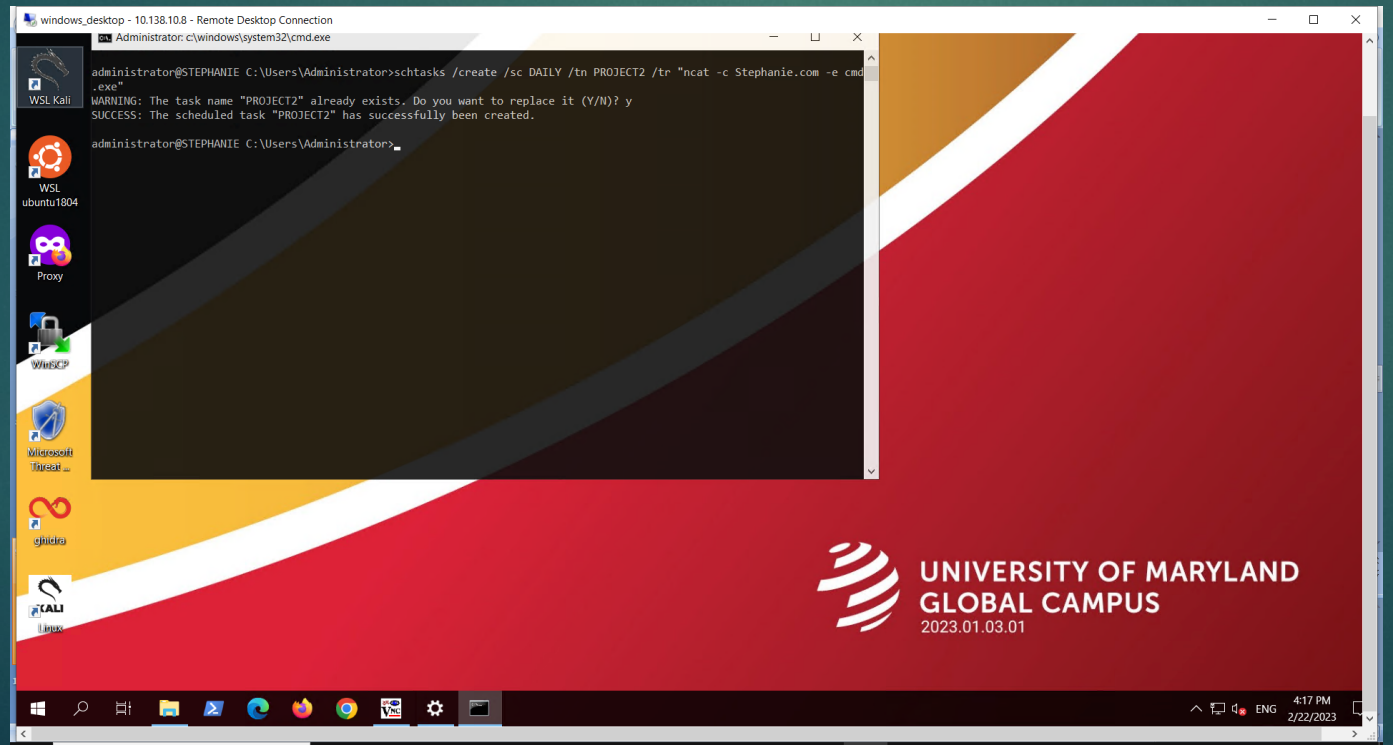
Stop A Service

- A hacker may want to stop a service like accounts-daemon service so as to stop the access of a user to his or her account and also to be the only one with the access to the files and folders of which some could be sensitive



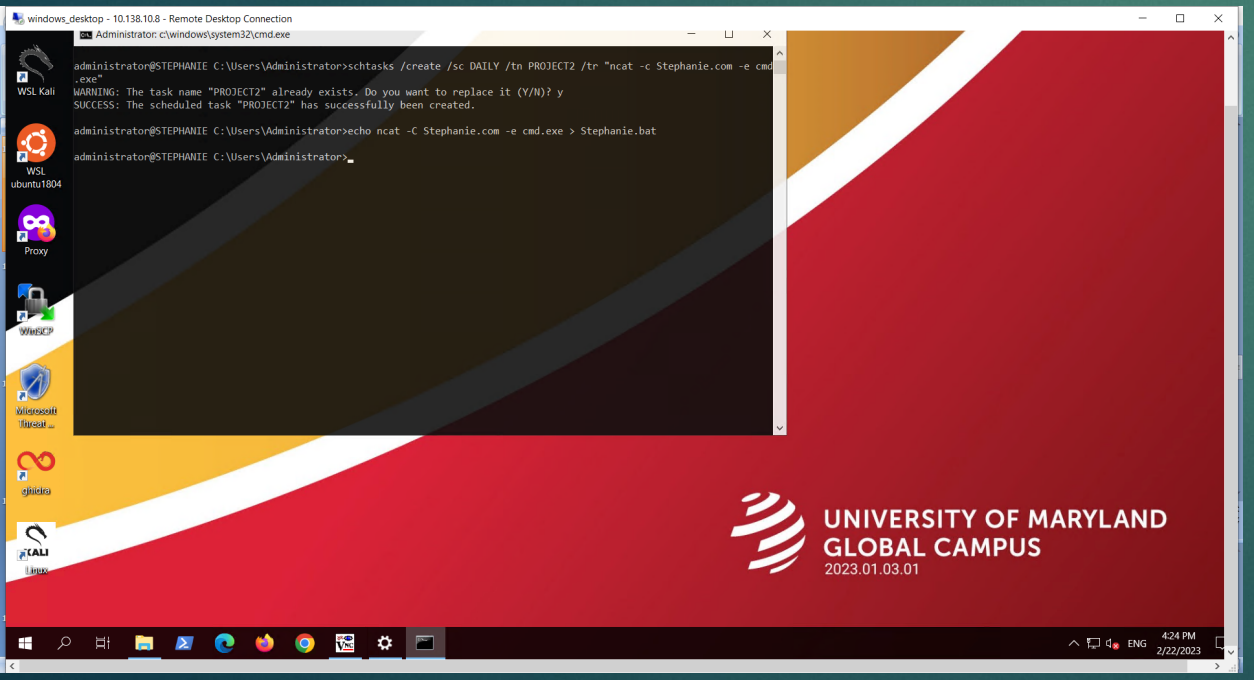
Creating a Scheduled Task (Backdoor)

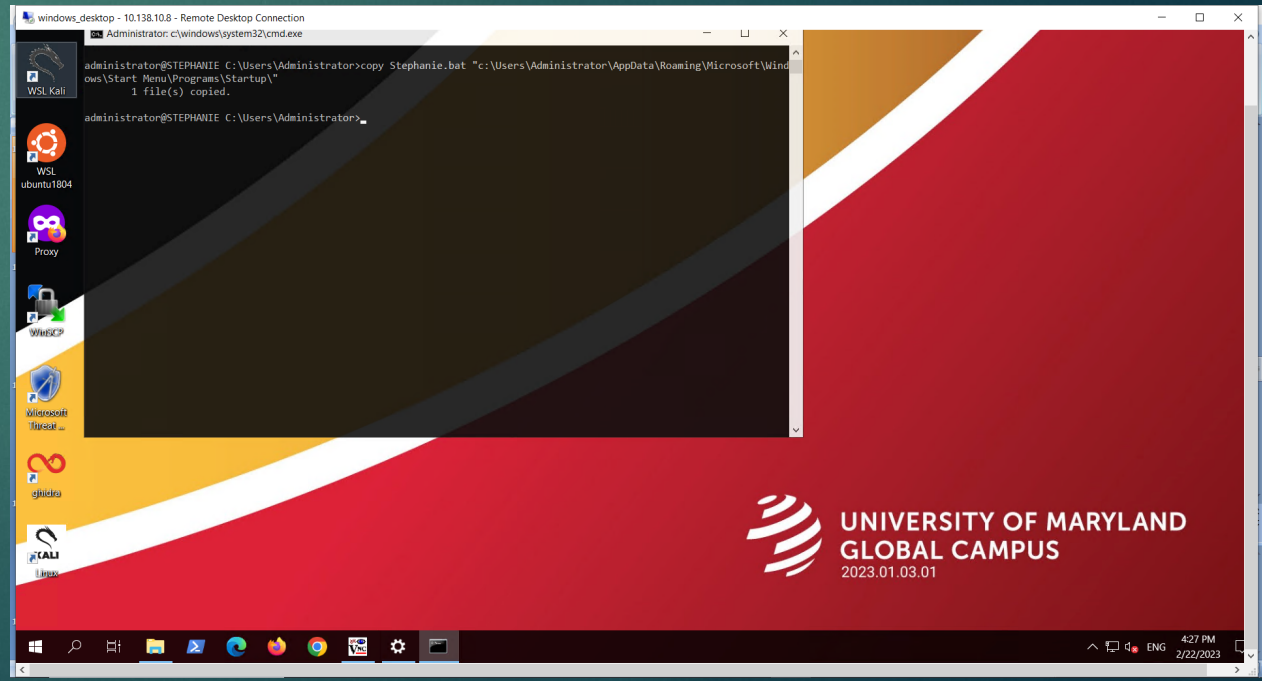
- schtasks command displays and alters scheduled tasks, adds and subtracts tasks from the schedule, starts and stops tasks on demand, and schedules commands and programs to run periodically or at a specific time.
- a hacker might want to schedule a task so as to start automatically sending files or emails to their designated work station and steal information from an organization



Adding a Batch File to Startup

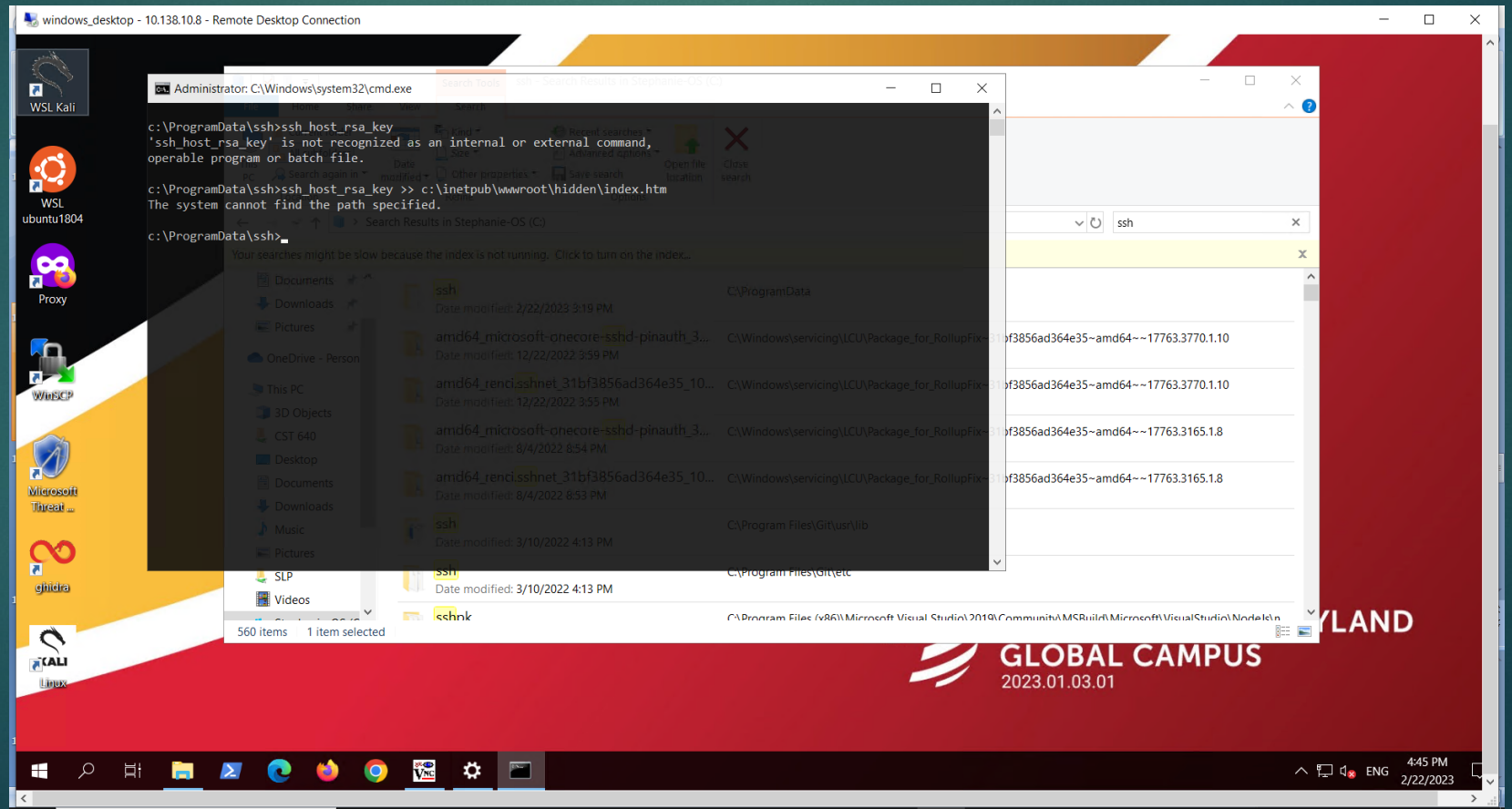
- By placing their malicious binary in the startup folders, adversaries can achieve persistence. The startup folder is looked up when the operating system starts, and the files in this folder are run. There are two kinds of startup folders that the Windows operating system keeps: a) client wide and (b) framework wide, as displayed in the accompanying code. A program that is in the user's startup folder is only run for that user; a program that is in the system folder is run every time a user logs in. Persistence with a system-wide startup folder requires administrator privileges.





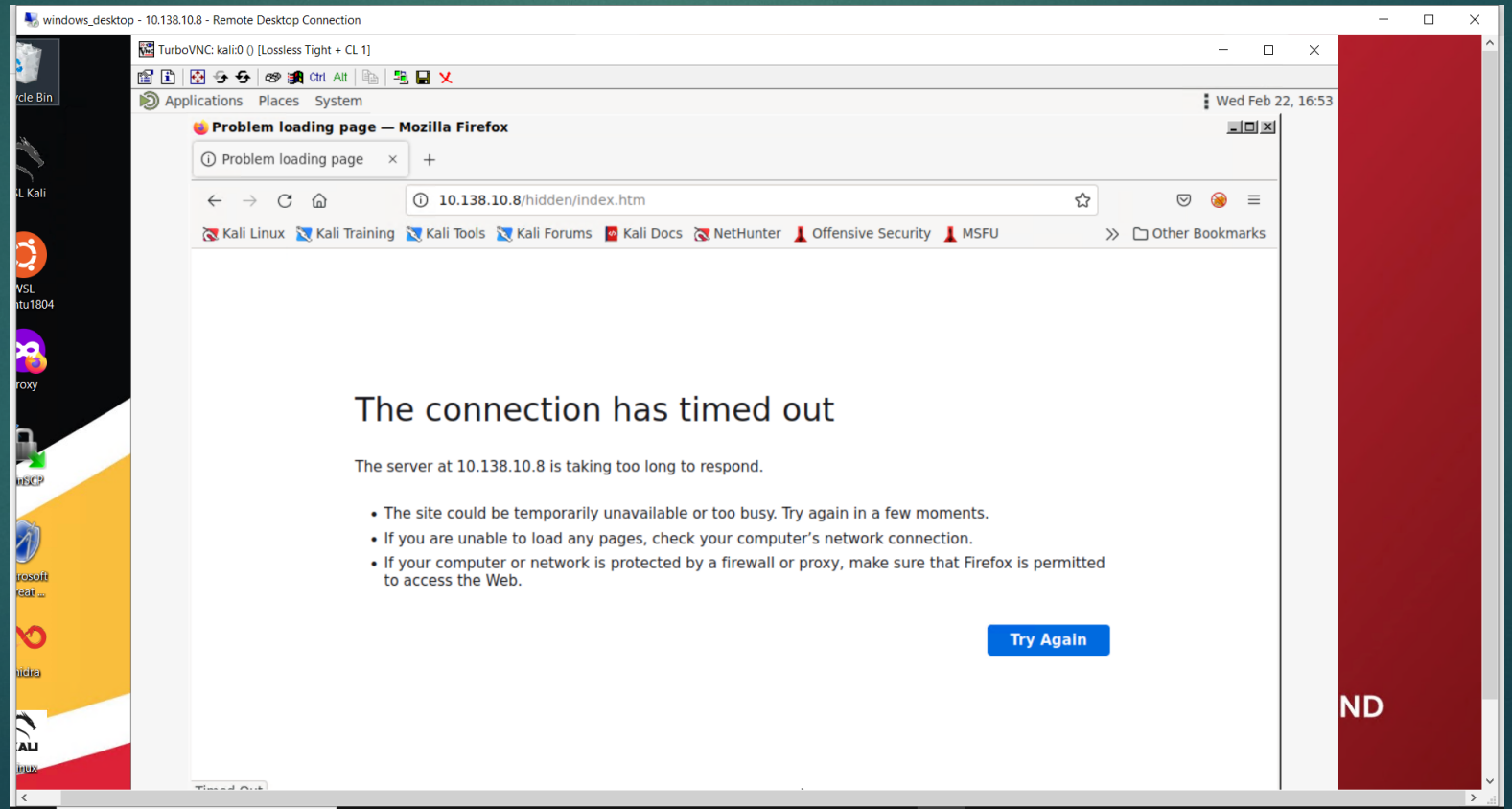
Stealing Data

You are able to spend or send the cryptocurrencies that are stored in your wallet because a private key for a cryptocurrency uniquely identifies, authenticates, and grants access to your account. As a result, if you lose your private key, you will lose all of your assets. Thankfully, there are ways to store your private keys, as we'll see in a moment.



Data Exfiltration

- Any unintentional movement of data is considered data exfiltration. Data exfil, data exportation, data extrusion, data leakage, and data theft are all possible names for it. Data exfil is a very real threat to businesses, whether it's done with a thumb drive or a printer.



Summary

- *Base64 is a group of binary-to-text encoding schemes in computer programming that use four 6-bit Base64 digits to represent binary data—specifically, a sequence of 8-bit bytes—in sequences of 24 bits.*
- *SSH, otherwise called Secure Shell or Secure Attachment Shell, is an organization convention that gives clients, especially framework executives, a safe method for getting to a PC over an unstable organization.*
- *Scheduled Maintenance is compatible with a variety of scheduling options. Choose the one that is best for the job. Without any dependencies, scheduled tasks execute according to a predetermined schedule. You could, for instance, schedule a task to run on the first Monday of January or every Tuesday at 4:00 a.m. When the task is dependent on changes in the Configuration Management application, demand-based tasks are executed. A trigger can be used to define this.*
- *The hacker will try to use these technologies to penetrate and manipulate the system using the methods that have been discussed in this presentation for malicious purposes.*
- *When the hacker penetrated the system he was able to schedule tasks such as send information from a system at a specific time to a system of his choosing, the hacker can also add himself as an administrator and access sensitive information from the machine.*

References

- hackers attack - Bing images
- www.cisco.com/c/en/us/products/security/what-is-a-hacker.html
- 5 Common Hacking Techniques Used by Hackers – GeeksforGeeks
- What is an Artifact in Cyber Security? | Systems Solution, Inc. (SSI) (ssi-net.com)
- How To Use Nmap to Scan for Open Ports | DigitalOcean
- SSH Backdoor: How to get a proper shell on the victim’s machine | by KSecurity | Medium
- Local Admin Accounts - Security Risks and Best Practices (Part 1) (securden.com)