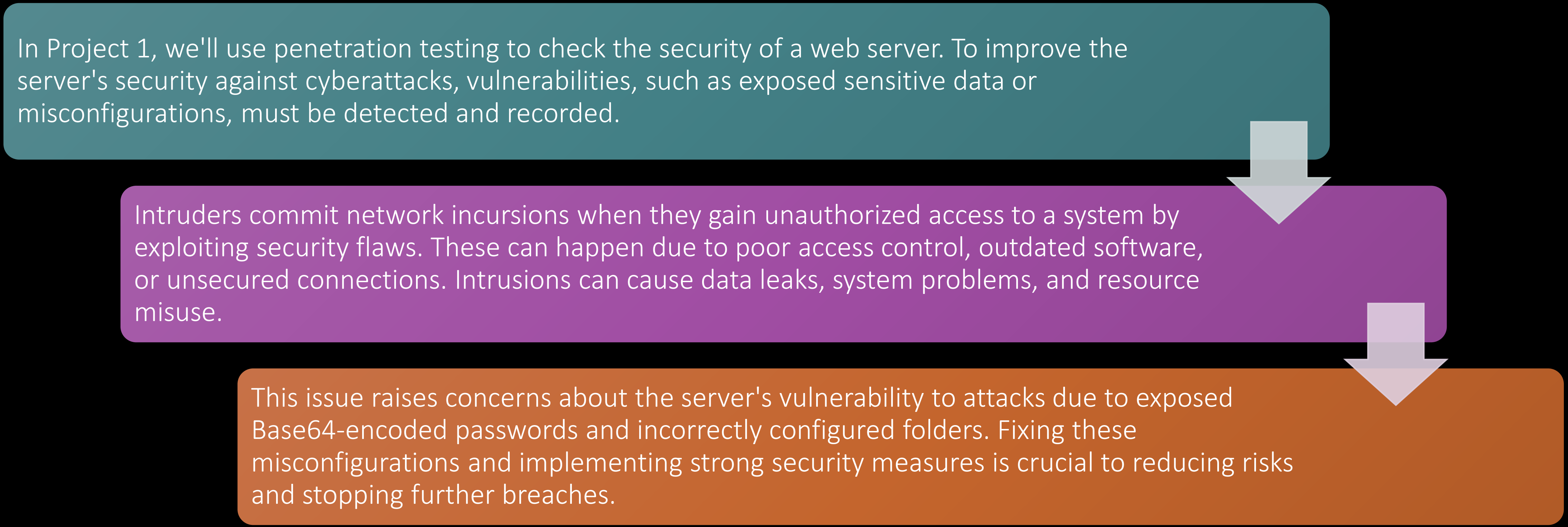
#define ASM_VMX_VMREAD_RDX_RAX
static __always_inline unsigned long
unsigned long va
asm volatile

Digital Forensics Technology and Practices:

Project 1 - A Network Intrusion

<CST 640 9040 Digital Forensics Technology and Practices (2251)>
<Niknaz Sadehvandi>
<1/30/2025>

Project 1 - Introduction



In Project 1, we'll use penetration testing to check the security of a web server. To improve the server's security against cyberattacks, vulnerabilities, such as exposed sensitive data or misconfigurations, must be detected and recorded.

Intruders commit network incursions when they gain unauthorized access to a system by exploiting security flaws. These can happen due to poor access control, outdated software, or unsecured connections. Intrusions can cause data leaks, system problems, and resource misuse.

This issue raises concerns about the server's vulnerability to attacks due to exposed Base64-encoded passwords and incorrectly configured folders. Fixing these misconfigurations and implementing strong security measures is crucial to reducing risks and stopping further breaches.

MARS Linux System

- Based on Kali Linux, a specialized version for security testing and digital analysis.

- Comes with built-in tools for analyzing networks, checking security weaknesses, and handling hacking jobs.

- Operates with root rights for unlimited management functions.

The networking setup is approved with the IP address 10.11.3.52 for smooth contact.

- Preinstalled dirb, Nmap, and Nikto tools for reconnaissance and vulnerability evaluations.

- Reachable with TurboVNC from a Windows machine.

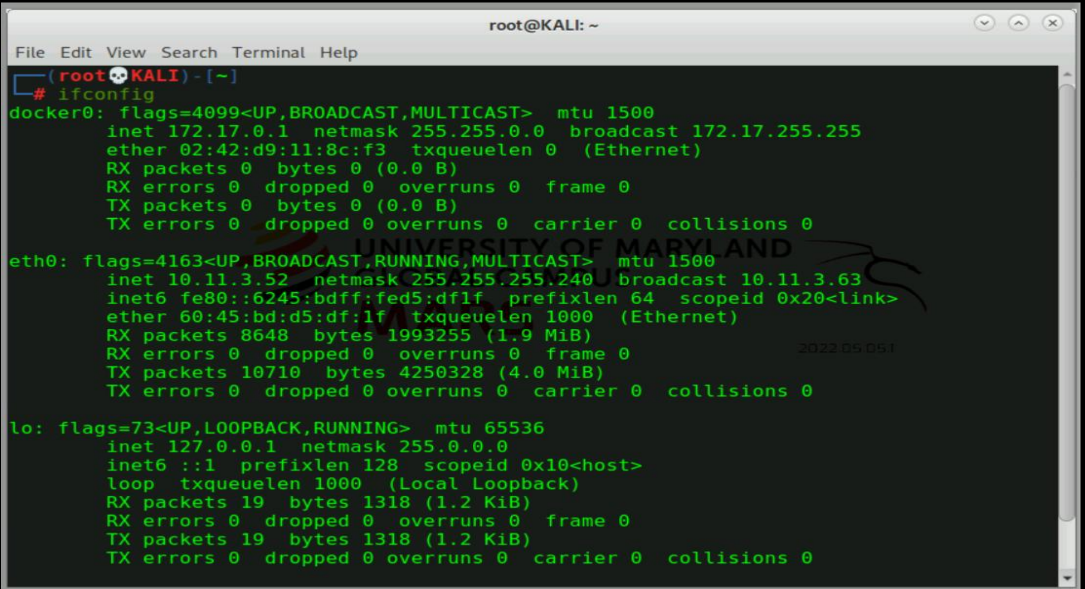
Linux Desktop

IP Address:

10.11.3.52

Connection Info:

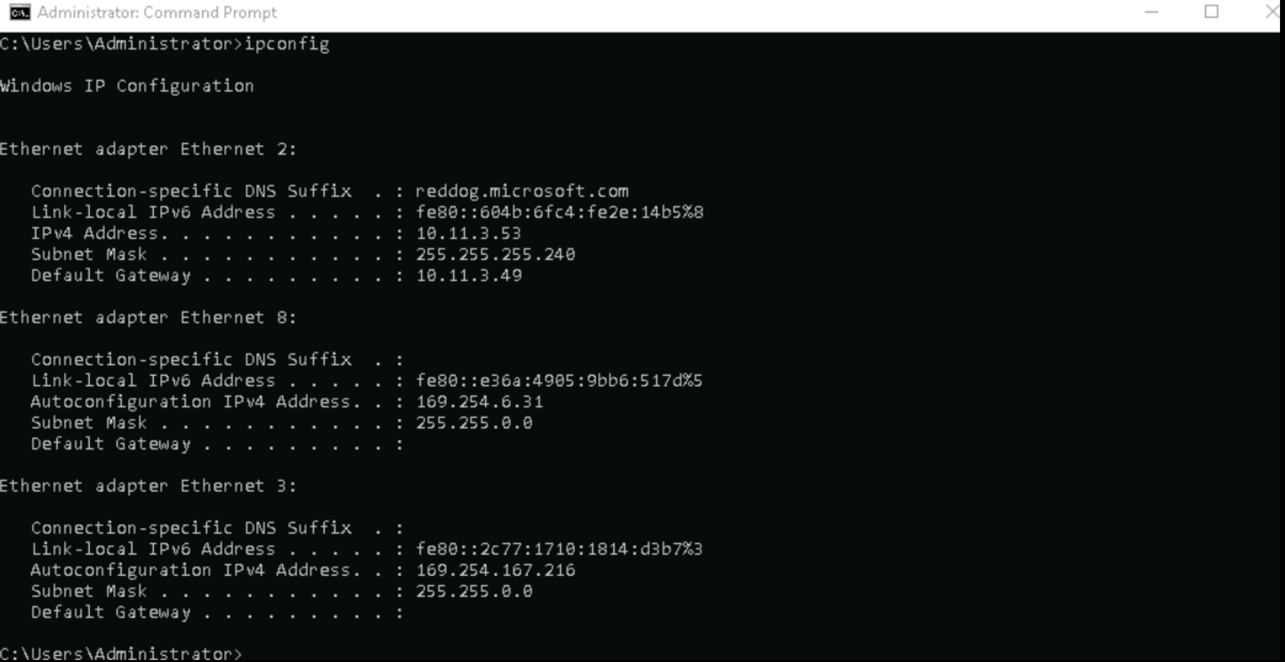
Use the TurboVNC shortcut on the desktop of your Windows Desktop to connect to your Linux Desktop.



```
┌──(root💀KALI)-[~]
└─# ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 02:42:d9:11:8c:f3  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.11.3.52  netmask 255.255.255.240  broadcast 10.11.3.63
        inet6 fe80::6245:bdff:fed5:df1f  prefixlen 64  scopeid 0x20<link>
        ether 60:45:bd:d5:df:1f  txqueuelen 1000  (Ethernet)
        RX packets 8648  bytes 1993255 (1.9 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 10710  bytes 4250328 (4.0 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 19  bytes 1318 (1.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 19  bytes 1318 (1.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

MARS Windows System

- The Windows system in MARS is set up to work well with the virtual lab and is used for testing and analyzing hacking.
- Its IP address is 10.11.3.53, which shows it is connected to the virtual lab.
- The system has tools to help manage security settings and support checking for vulnerabilities.
- It enables working with the Linux system in the lab to check networks for weaknesses and gather information.
- The setup ensures seamless communication between systems in the lab for comprehensive testing and learning purposes.



```
C:\Users\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . : reddog.microsoft.com
   Link-local IPv6 Address . . . . . : fe80::604b:6fc4:fe2e:14b5%8
   IPv4 Address. . . . . . . . . . . : 10.11.3.53
   Subnet Mask . . . . . . . . . . . : 255.255.255.240
   Default Gateway . . . . . . . . . : 10.11.3.49

Ethernet adapter Ethernet 8:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::e36a:4905:9bb6:517d%5
   Autoconfiguration IPv4 Address. . : 169.254.6.31
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . :

Ethernet adapter Ethernet 3:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::2c77:1710:1814:d3b7%3
   Autoconfiguration IPv4 Address. . : 169.254.167.216
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . :

C:\Users\Administrator>
```

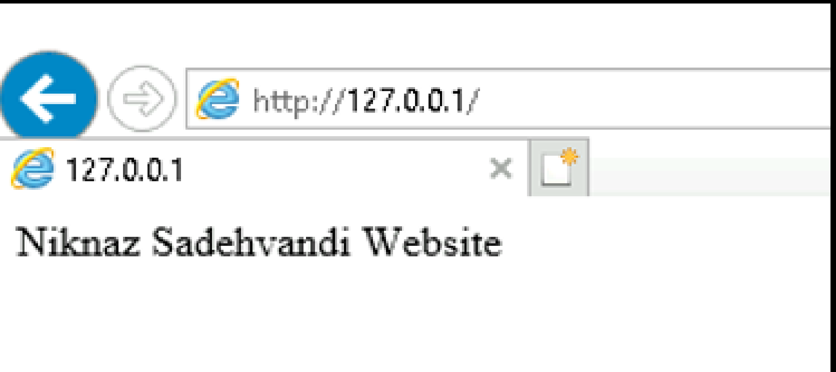
IIS Setup

IIS is a Microsoft web server made for Windows computers.

Provides a place to store and send the HTML pages or files you request.

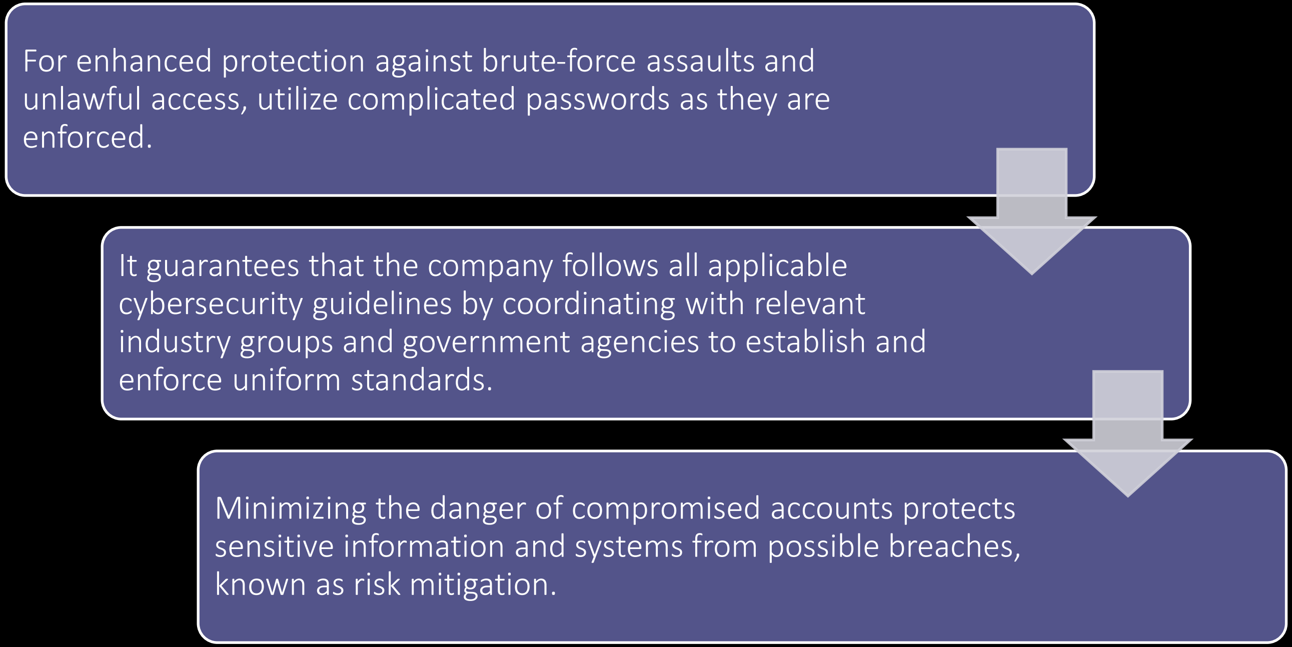
Handles calls from client computers and gives answers back, making it easy to share information over networks.

The purposes include handling websites and pages, responding to requests, running server programs, and keeping things safe.



Niknaz Sadehvandi Website

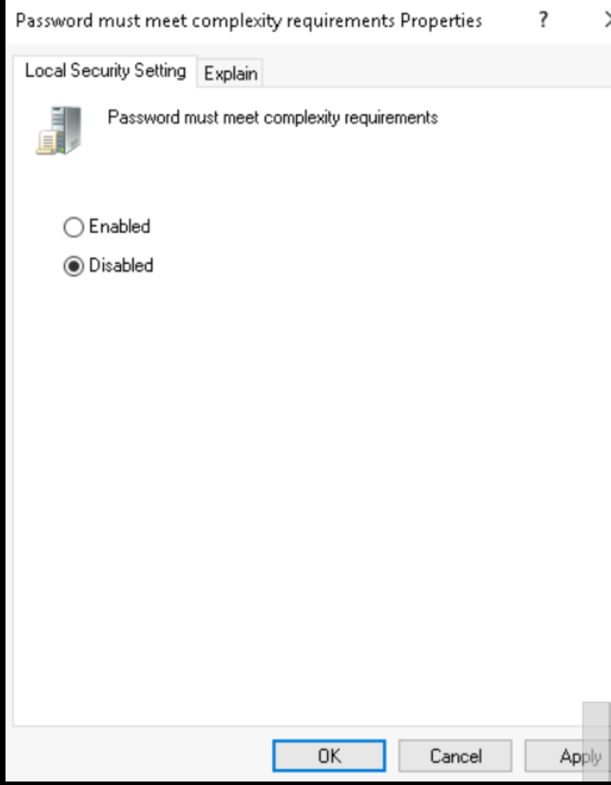
Security Policy Changes



For enhanced protection against brute-force assaults and unlawful access, utilize complicated passwords as they are enforced.

It guarantees that the company follows all applicable cybersecurity guidelines by coordinating with relevant industry groups and government agencies to establish and enforce uniform standards.

Minimizing the danger of compromised accounts protects sensitive information and systems from possible breaches, known as risk mitigation.

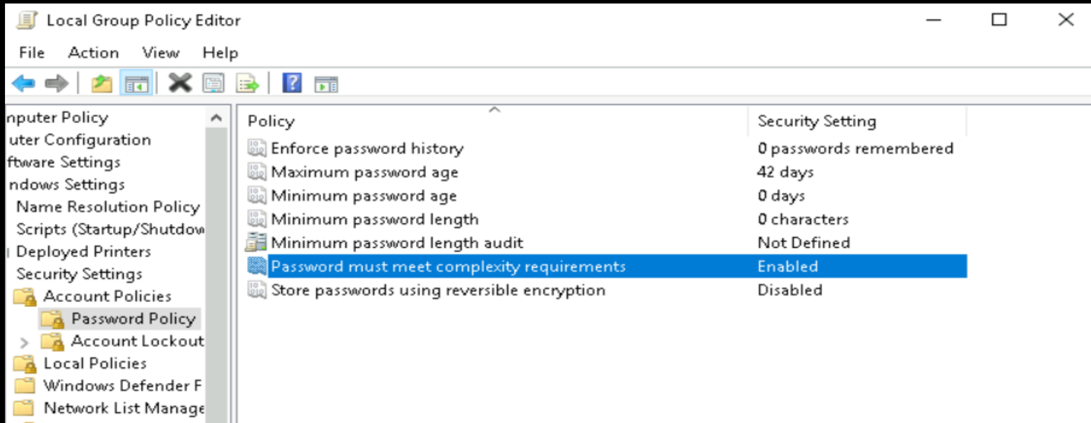


Password must meet complexity requirements Properties

Password must meet complexity requirements

○ Enabled

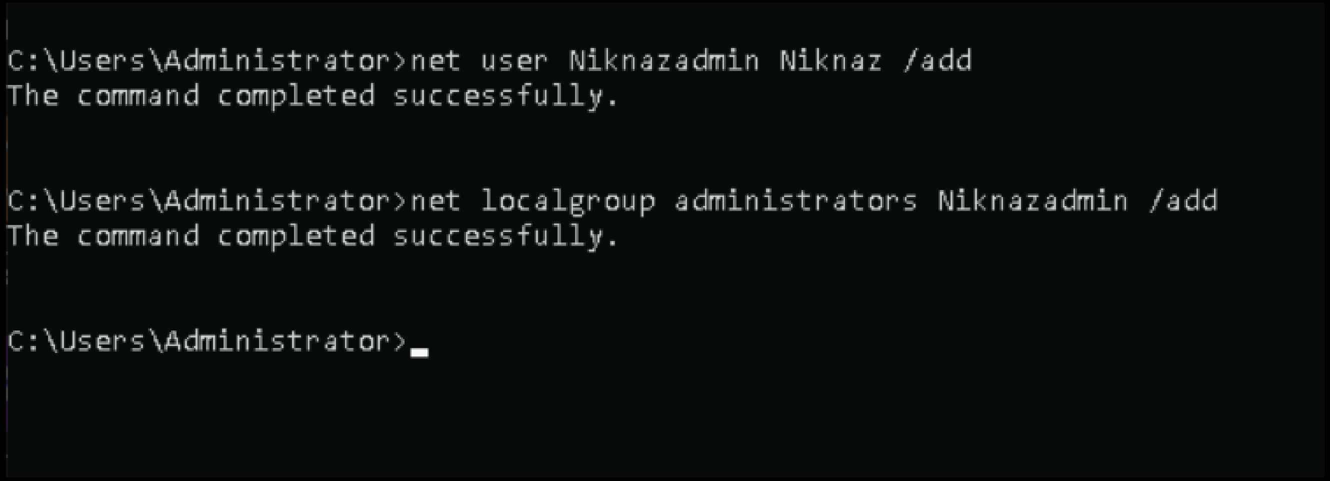
● Disabled



Local Group Policy Editor

nputer Policy
uter Configuration
ftware Settings
ndows Settings
Name Resolution Policy
Scripts (Startup/Shutdow
Deployed Printers
Security Settings
Account Policies
Password Policy
Account Lockout
Local Policies
Windows Defender F
Network List Manage

Policy	Security Setting
Enforce password history	0 passwords remembered
Maximum password age	42 days
Minimum password age	0 days
Minimum password length	0 characters
Minimum password length audit	Not Defined
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled



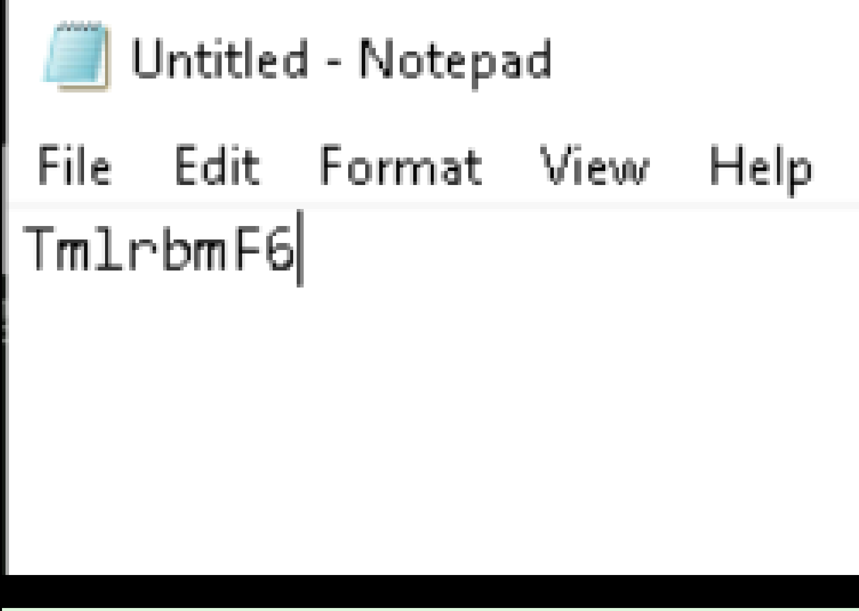
```
C:\Users\Administrator>net user Niknazadmin Niknaz /add
The command completed successfully.


C:\Users\Administrator>net localgroup administrators Niknazadmin /add
The command completed successfully.


C:\Users\Administrator>_
```

Adding an Administrative Account

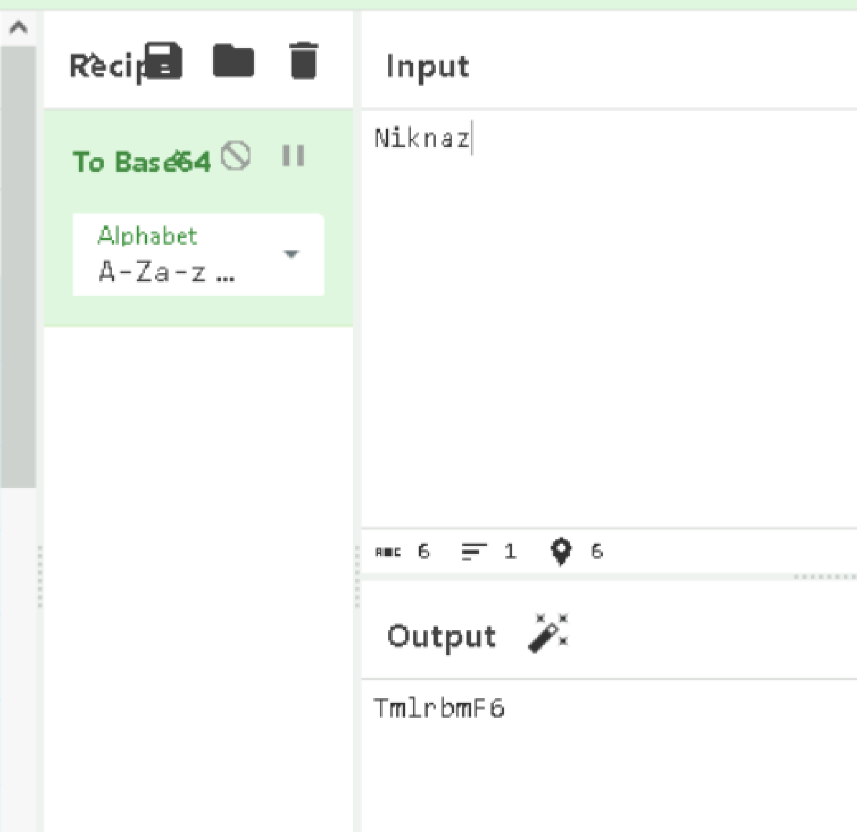
- The net user command is a Windows system utility for managing user accounts, including creating, editing, and deleting them; this is a must-have for Windows setups that deal with user accounts and access delegation.
- Adding or deleting people from specified groups is one of the many tasks that can be accomplished using the net localgroup Command. This is essential to keeping the system secure and providing role-based access.

Base64 Lesson

- With this flexible web-based solution, CyberChef can handle data encoding, decoding, encryption, and many other procedures. You can efficiently perform operations like Base64 encoding by dragging and dropping them into place; it's user-friendly.
- Base64 is an encoding strategy that uses a predefined set of 64 characters to transform binary data into a text format to ensure secure data transmission across text-based systems like email. Data encryption in cryptography applications, media file transmission, and web page embedding are some of its most prevalent uses.
- CyberChef is an excellent tool for cybersecurity experts since it makes Base64 encoding easy to do.



```
TmlrbmF6
```



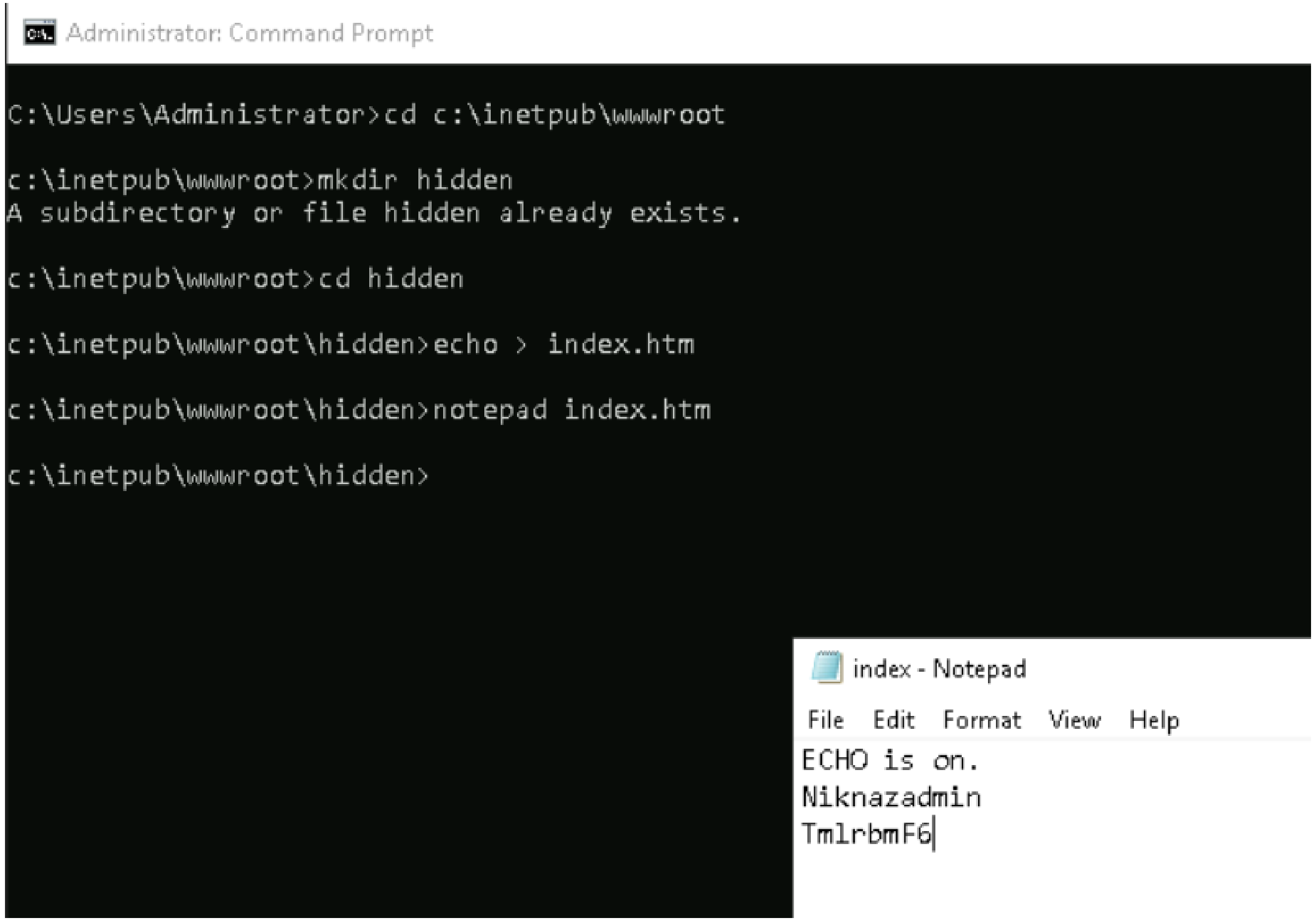
To Base64

Alphabet
A-Za-z ...

```
Niknaz
```

```
TmlrbmF6
```

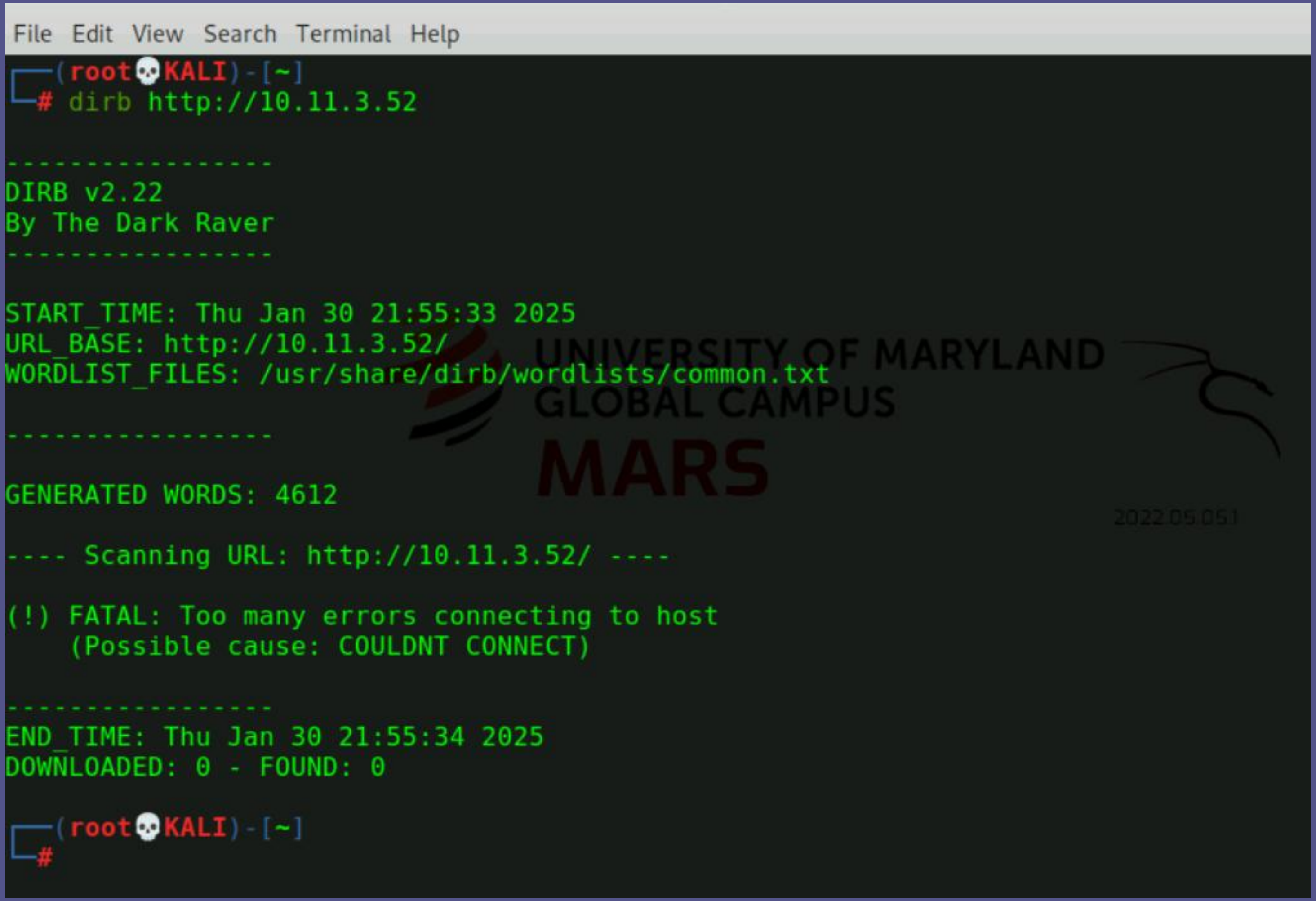
Website Misconfiguration



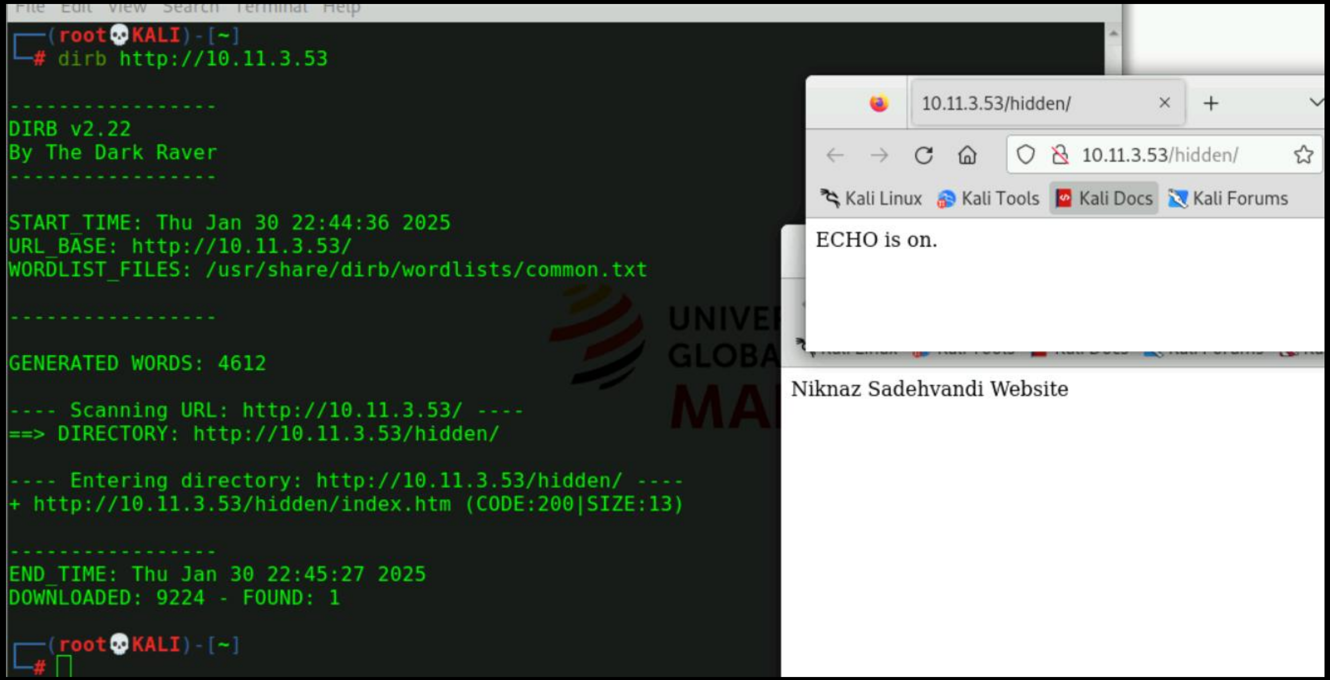
```
C:\Users\Administrator>cd c:\inetpub\wwwroot

c:\inetpub\wwwroot>mkdir hidden
A subdirectory or file hidden already exists.

c:\inetpub\wwwroot>cd hidden

c:\inetpub\wwwroot\hidden>echo > index.htm

c:\inetpub\wwwroot\hidden>notepad index.htm

c:\inetpub\wwwroot\hidden>
```

```
ECHO is on.
Niknazadmin
TmlrbmF6
```

dirb attack on the Windows Server



```
┌──(root💀KALI)-[~]
└─# dirb http://10.11.3.52

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Thu Jan 30 21:55:33 2025
URL_BASE: http://10.11.3.52/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.11.3.52/ ----

(!) FATAL: Too many errors connecting to host
    (Possible cause: COULDNT CONNECT)

-----------------
END_TIME: Thu Jan 30 21:55:34 2025
DOWNLOADED: 0 - FOUND: 0

┌──(root💀KALI)-[~]
└─#
```



```
┌──(root💀KALI)-[~]
└─# dirb http://10.11.3.53

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Thu Jan 30 22:44:36 2025
URL_BASE: http://10.11.3.53/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.11.3.53/ ----
==> DIRECTORY: http://10.11.3.53/hidden/

---- Entering directory: http://10.11.3.53/hidden/ ----
+ http://10.11.3.53/hidden/index.htm (CODE:200|SIZE:13)

-----------------
END_TIME: Thu Jan 30 22:45:27 2025
DOWNLOADED: 9224 - FOUND: 1

┌──(root💀KALI)-[~]
└─# 
```

ECHO is on.

Niknaz Sadehvandi Website

Credentials Extracted

- Improperly implemented access restrictions may reveal hidden or sensitive directories, as illustrated in this example where dirb was used to access a hidden directory. Attackers may exploit sensitive data, passwords, or other information in these folders.
- Enabling verbose warning messages or debugging modes on production servers might accidentally disclose server settings, database queries, and file structures, giving attackers essential information to exploit vulnerabilities.
- Websites using default passwords or unpatched software are easy targets for attackers. Automated attacks exploit such misconfigurations to obtain unauthorized access or impair services.
- Audits, least privilege, and OWASP recommendations may reduce these risks.

Summary

- *For this project, we searched a web server for hidden files and directories using the dirb program. The program uses a wordlist to brute-force URLs to find accessible sites. The scan can potentially reveal setup errors, such as credentials exposed in Base64 format. For testing purposes, a web service simulator was also built using IIS.*

- *During the scan, potential vulnerabilities caused by incorrect server setups were discovered. Exposed directories and encoded credentials showed the potential for data leakage due to improperly set web services. The scan proved that dirt and similar technologies might identify vulnerable endpoints that hackers might use.*

- *The attacker took advantage of website setup mistakes, like leaving private files and folders open. They took advantage of poorly protected Base64-encoded passwords to gain illegal entry; this shows the importance of having strict access rules and regular checks for security weaknesses.*

References

GeeksforGeeks. (2024, August 7). *Encoding and Decoding Base64 Strings in Python*. GeeksforGeeks. https://www.geeksforgeeks.org/encoding-and-decoding-base64-strings-in-python/

Stallings, W., Brown, L., University of New South Wales, Australian Defence Force Academy, Security Editor, Linux Journal, Dir. Of Value-Subtracted Svcs., Wiremonkeys.org, & Principle Security Program Manager, Microsoft Corporation. (2012). *Computer Security: Principles and Practice*. Pearson Education, Inc., publishing as Prentice Hall. https://unidel.edu.ng/focelibrary/books/Computer%20Security%20_%20Principles%20-%20WILLIAM%20STALLINGS_2089.pdf

National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0. In *NIST CSWP 29* [Report]. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

Cybersecurity Best Practices | Cybersecurity and Infrastructure Security Agency CISA. (n.d.). https://www.cisa.gov/topics/cybersecurity-best-practices

Decoding the DNA of Ransomware Attacks: Unveiling the Anatomy Behind the Threat. (n.d.). Trellix. https://www.trellix.com/blogs/research/decoding-the-dna-of-ransomware-attacks/