



Digital Forensics Technology and Practices:

Project 1 - A Network Intrusion

CST 640 Section
9042

Ryan Steggerda
1/28/2024

Project 1 - Introduction

- The purpose of Project 1 is to play the role of a digital forensic analyst for a company that recently hired a small firm to manage one of several websites owned by the company
- A network intrusion is any illegal activity carried out on a digital network. Network incursions frequently entail the theft of valuable network resources and virtually always compromise a network security and/or data security(Gou et al., 2023)
- A critical vector from the security incident is how the hidden folder was discovered by using a directory discovery tool as well as how the base64 was decoded.



MARS Linux System

- The Linux system being used has an IP address of 10.138.16.136
- Netmask: 255.255.240.0
- Broadcast: 10.138.31.255

```
root@kali: / January 28, 2024, 11:59:14 AM
File Edit View Search Terminal Help
(root@kali) - [/]
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 9001
    inet 10.138.16.136 netmask 255.255.240.0 broadcast 10.138.31.255
    inet6 fe80::c0:4bff:fe48:880b prefixlen 64 scopeid 0x20<link>
    ether 02:c0:4b:48:88:0b txqueuelen 1000 (Ethernet)
    RX packets 1537 bytes 103084 (100.6 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1397 bytes 1247000 (1.1 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

MARS Windows System

- IP address: 10.138.1.44
- Subnet Mask: 255.255.240.0
- Default Gateway: 10.138.0.1

Windows IP Configuration

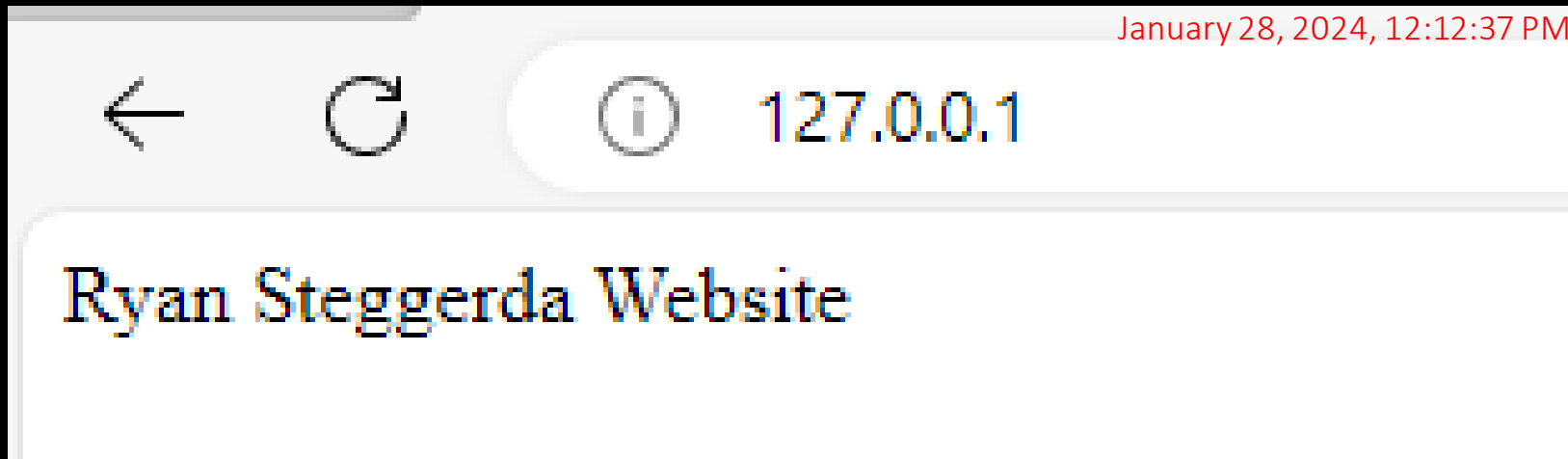
January 28, 2024, 12:07:33 PM

Ethernet adapter Ethernet 4:

```
Connection-specific DNS Suffix . :  
Link-local IPv6 Address . . . . . : fe80::77ec:d95d:a8a2:f6df%10  
IPv4 Address. . . . . : 10.138.1.44  
Subnet Mask . . . . . : 255.255.240.0  
Default Gateway . . . . . : 10.138.0.1
```


IIS Setup

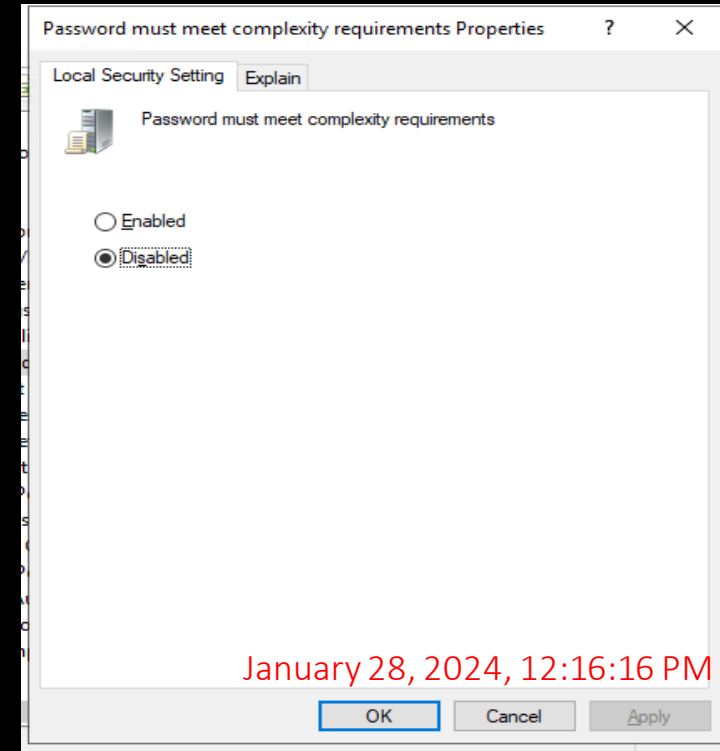
- The Internet Information Service is an extensible web server created by Microsoft for use with the Windows NT family. IIS supports HTTP, HTTP/2, HTTPS, FTP, FTPS, SMTP and NNTP. It has been an integral part of the Windows NT family since Windows NT 4.0, though it may be absent from some editions (e.g. Windows XP Home edition), and is not active by default(Rosencrance & Bigelow, 2019).



Security Policy Changes

-Secure Password Policy Benefits-

- Mitigating the risk of weak passwords.
- Bringing consistency in password creation, use, and management.
- Establishing accountability for each activity performed on the organization's systems.
- Adding an extra layer/s of security to password-based authentication.
- Preventing data breaches and safeguarding your business' data and customer details.
- Maintaining order and building trust. Cultivating cybersecurity culture(Touil et al., 2024).



Adding an Administrative Account

-Net User Command-

The Net User tool is a command-line tool that is available in Windows 10 as well as Windows 11 and is used by administrator accounts mainly to add, delete or modify user accounts. This tool can be used to display user account information as well. But the endless possibilities of this tool are not limited to the above said usages only.

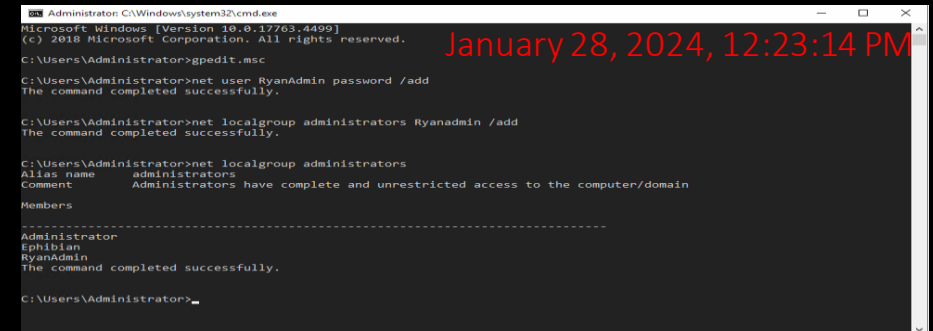
```
C:\Users\Administrator>net user RyanAdmin password /add  
The command completed successfully.
```

```
C:\Users\Administrator>
```

January 28, 2024, 12:19:46 PM

-Net Local Group Command-

Net localgroup command is used to manage local user groups on a computer. Using this command, administrators can add local/domain users to groups, delete users from groups, create new groups and delete existing groups. Below you can find syntax for all these operations(*Net Localgroup*, n.d.).



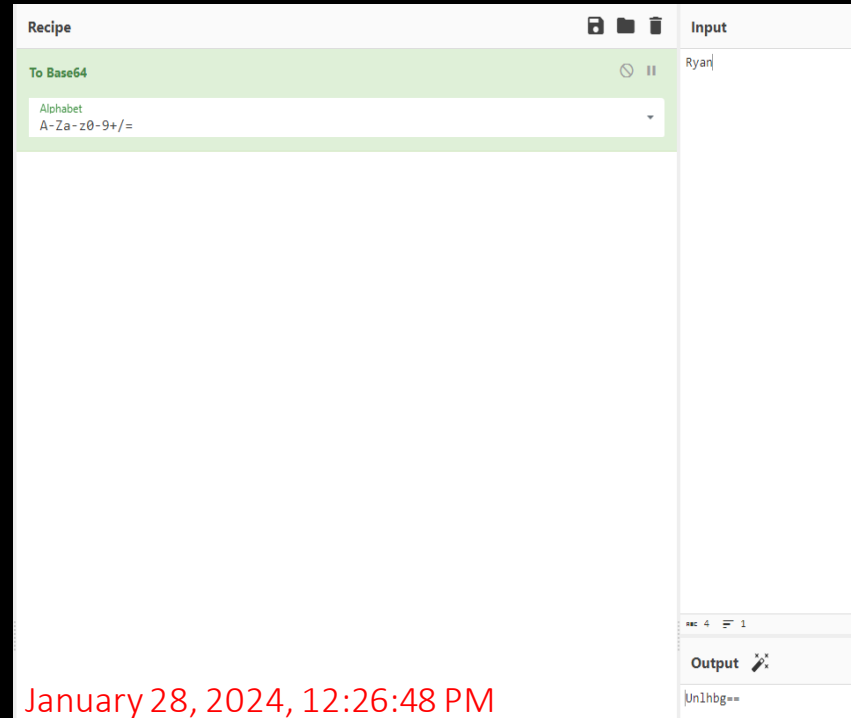
```
Administrator: C:\Windows\system32\cmd.exe  
Microsoft Windows [Version 10.0.17763.4499]  
(c) 2018 Microsoft Corporation. All rights reserved.  
C:\Users\Administrator>gpedit.msc  
C:\Users\Administrator>net user RyanAdmin password /add  
The command completed successfully.  
C:\Users\Administrator>net localgroup administrators RyanAdmin /add  
The command completed successfully.  
C:\Users\Administrator>net localgroup administrators  
Alias name     administrators  
Comment       Administrators have complete and unrestricted access to the computer/domain  
Members  
-----  
Administrator  
Ephibian  
RyanAdmin  
The command completed successfully.  
C:\Users\Administrator>
```

January 28, 2024, 12:23:14 PM

Base64 Lesson

-Base 64-

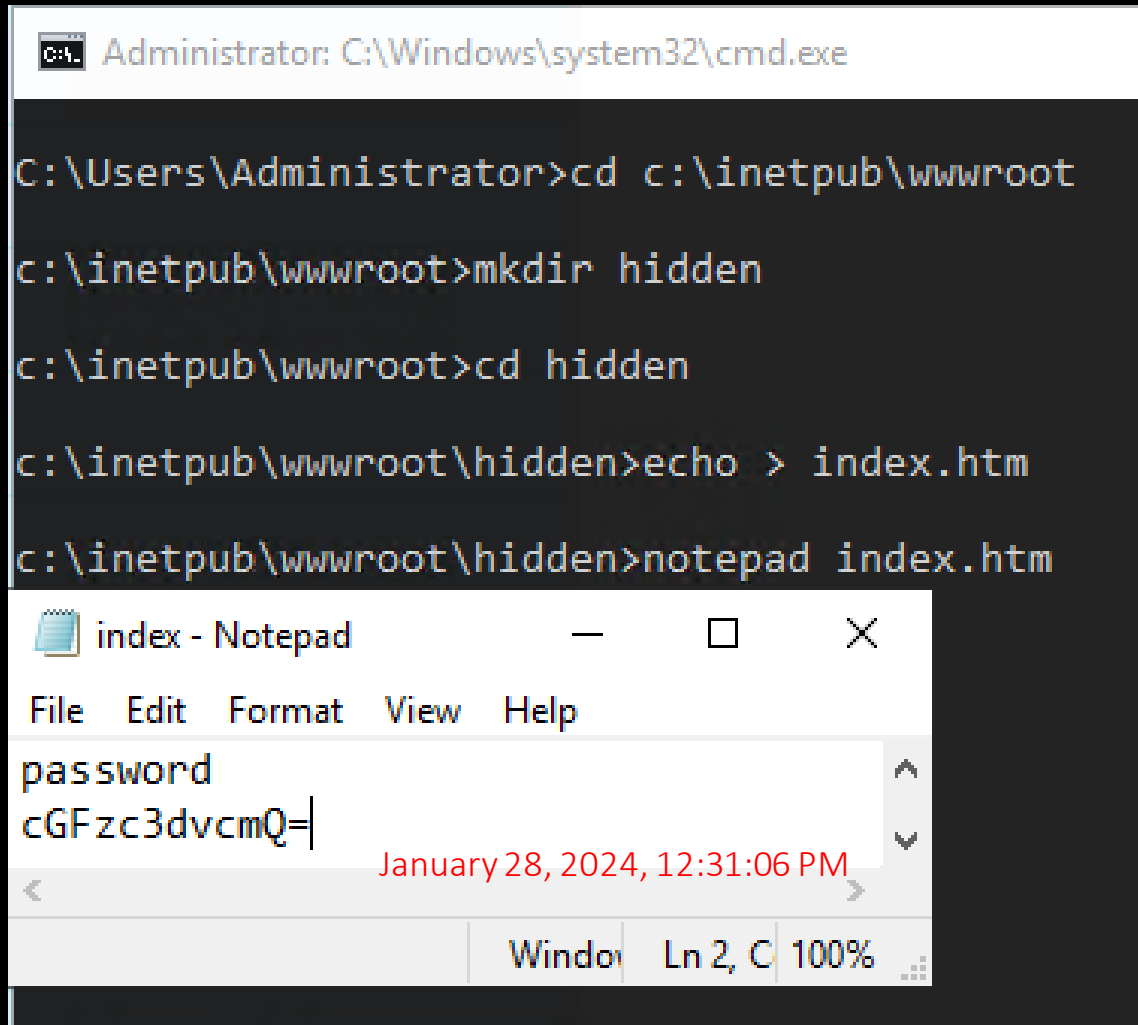
In computer programming, Base64 is a group of binary-to-text encoding schemes that transforms binary data into a sequence of printable characters, limited to a set of 64 unique characters. More specifically, the source binary data is taken 6 bits at a time (Shaamood, 2021).



-CyberChef-

CyberChef is a web app to carry out many cyber operations within a web browser. It has over 300 operations, including basic encoding with Base64, Advanced Encryption Standard (AES) decryption, or changing character encodings. The app can handle many operations at once, making it a quick way to experiment and translate data.

Website Misconfiguration



The image shows a Windows command prompt window titled "Administrator: C:\Windows\system32\cmd.exe" with the following commands and output:

```
C:\Users\Administrator>cd c:\inetpub\wwwroot
c:\inetpub\wwwroot>mkdir hidden
c:\inetpub\wwwroot>cd hidden
c:\inetpub\wwwroot\hidden>echo > index.htm
c:\inetpub\wwwroot\hidden>notepad index.htm
```

Below the command prompt, a Notepad window titled "index - Notepad" is open, showing the following text:

```
password
cGFzc3dvcmQ=
```

The Notepad window also displays a timestamp "January 28, 2024, 12:31:06 PM" and a status bar at the bottom indicating "Window Ln 2, C 100%".

dirb attack on the Windows Server

```
root@kali: / January 28, 2024, 12:34:08 PM
File Edit View Search Terminal Help
DIRB v2.22
By The Dark Raver
-----

START_TIME: Sun Jan 28 20:33:11 2024
URL_BASE: http://10.138.1.44/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----

GENERATED WORDS: 4612

---- Scanning URL: http://10.138.1.44/ ----
==> DIRECTORY: http://10.138.1.44/hidden/

---- Entering directory: http://10.138.1.44/hidden/ ----
+ http://10.138.1.44/hidden/index.htm (CODE:200|SIZE:24)

-----

END_TIME: Sun Jan 28 20:33:35 2024
DOWNLOADED: 9224 - FOUND: 1

(root@kali) - [/]
#
```

Credentials Extracted

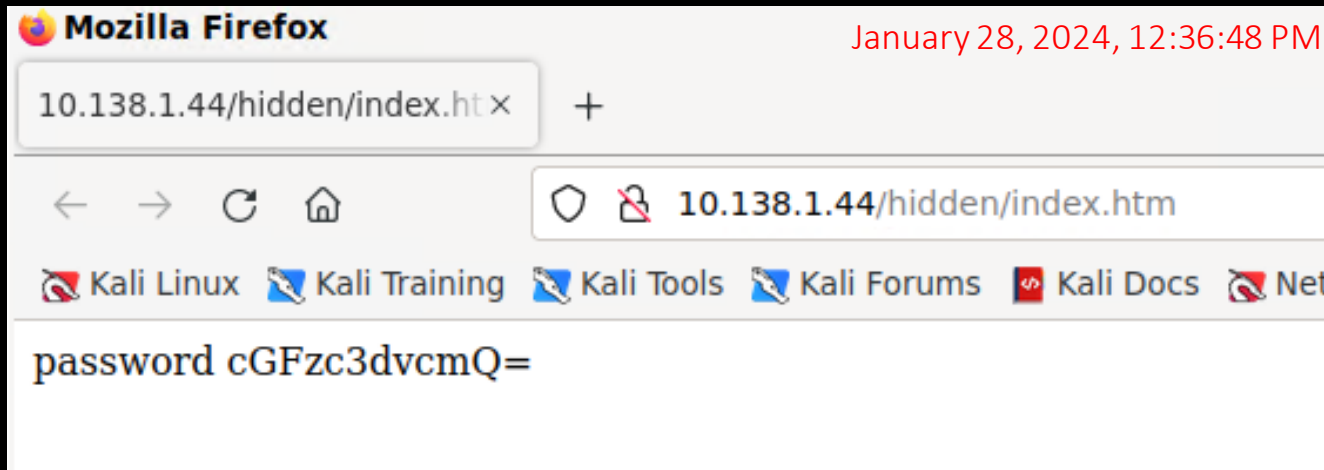
-Website Misconfiguration Examples-

Default settings: Default passwords, certificates, and installation settings are often left unchanged, making them vulnerable to attacks.

Deprecated protocols and encryption: Using outdated protocols and encryption methods can expose the system to vulnerabilities.

Open database instances: Leaving databases open to the public can allow attackers to access sensitive data.

Directory listing: Enabling directory listing can expose sensitive information to attackers(Dong et al., 2022).



Summary

- During the lab students were introduced to a myriad of tools including the net user, and netlocal group cmd tools for Windows.
- During the Lab the password policy rules were disabled and two new users were added, one being admin level. A hidden directory was also made containing the new Base64 encoded password.
- The attacker gained access to the site by performing a dirb attack on the IP address of the target system. After discovering the hidden path containing the Base64 password the attacker now has the users credentials.

References

- Dong, G., Liu, F., & Wu, G. (2022). A website's network attack analysis and security countermeasures. *Procedia Computer Science*, 208, 577–582.
<https://doi.org/10.1016/j.procs.2022.10.080>
- Gou, W., Zhang, H., & Zhang, R. (2023). Multi-Classification and Tree-Based ensemble network for the intrusion detection system in the internet of vehicles. *Sensors*, 23(21), 8788. <https://doi.org/10.3390/s23218788>
- Net Localgroup. (n.d.). <https://www.windows-commandline.com/net-localgroup/>
- Rosencrance, L., & Bigelow, S. J. (2019, September 5). Internet Information Services (IIS). *SearchWindowsServer*.
<https://www.techtarget.com/searchwindowsserver/definition/IIS>
- Shaamood, M. (2021). Encoding JSON by using Base64. *Al-mağallaṭ Al-ʿirāqiyyaṭ Al-handasaṭ Al-kahrabāʿiyyaṭ Wa-al-ilktrūniyyaṭ*, 17(1), 1–9.
<https://doi.org/10.37917/ijeee.17.1.4>
- Touil, H., Akkad, N. E., Satori, K., Soliman, N. F., & El-Shafai, W. (2024). Efficient braille transformation for secure password hashing. *IEEE Access*, 1.
<https://doi.org/10.1109/access.2024.3349487>