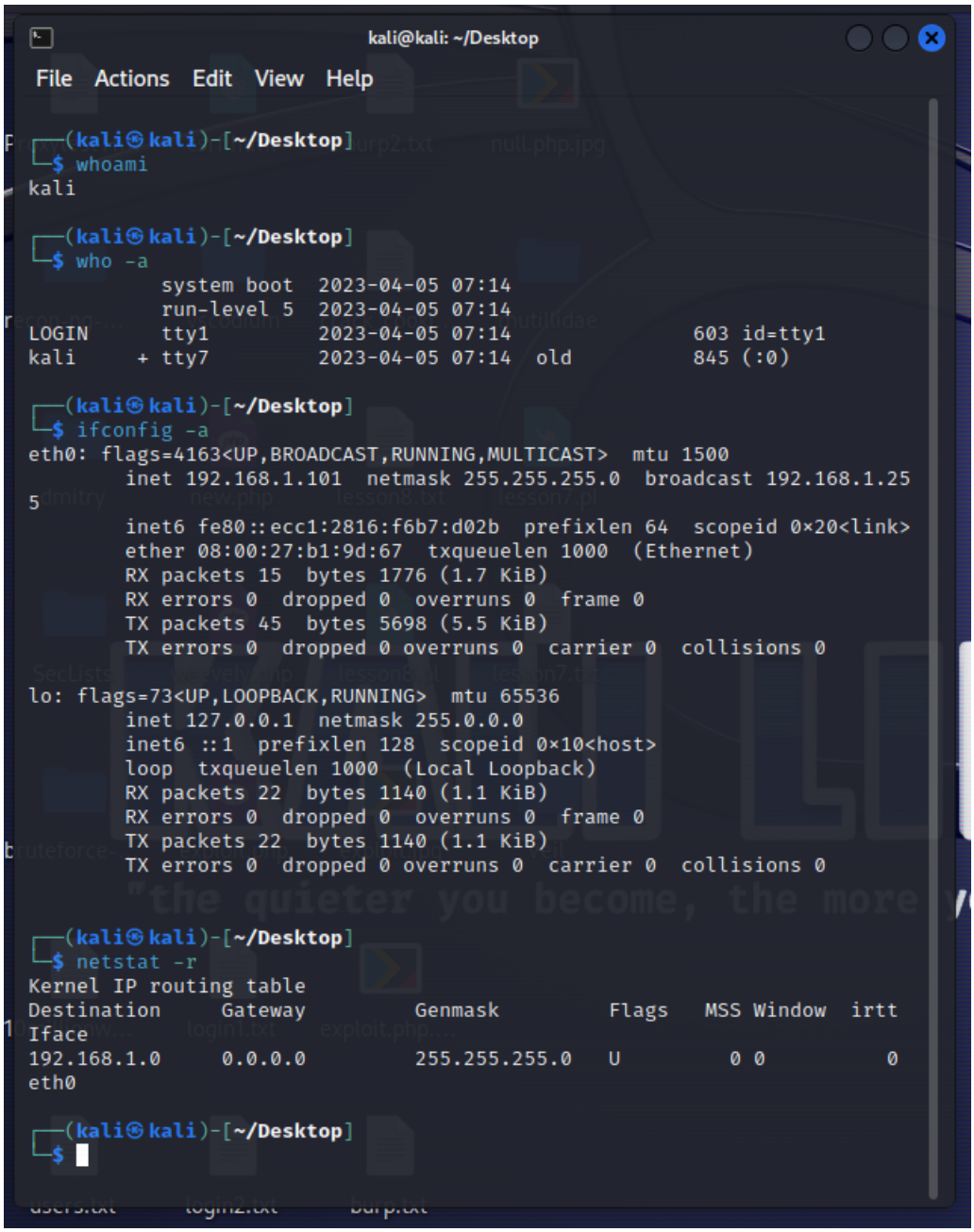
OLD DOMINION UNIVERSITY

CYSE 601 ADVANCED CYBERSECURITY TECHNIQUES AND OPERATIONS

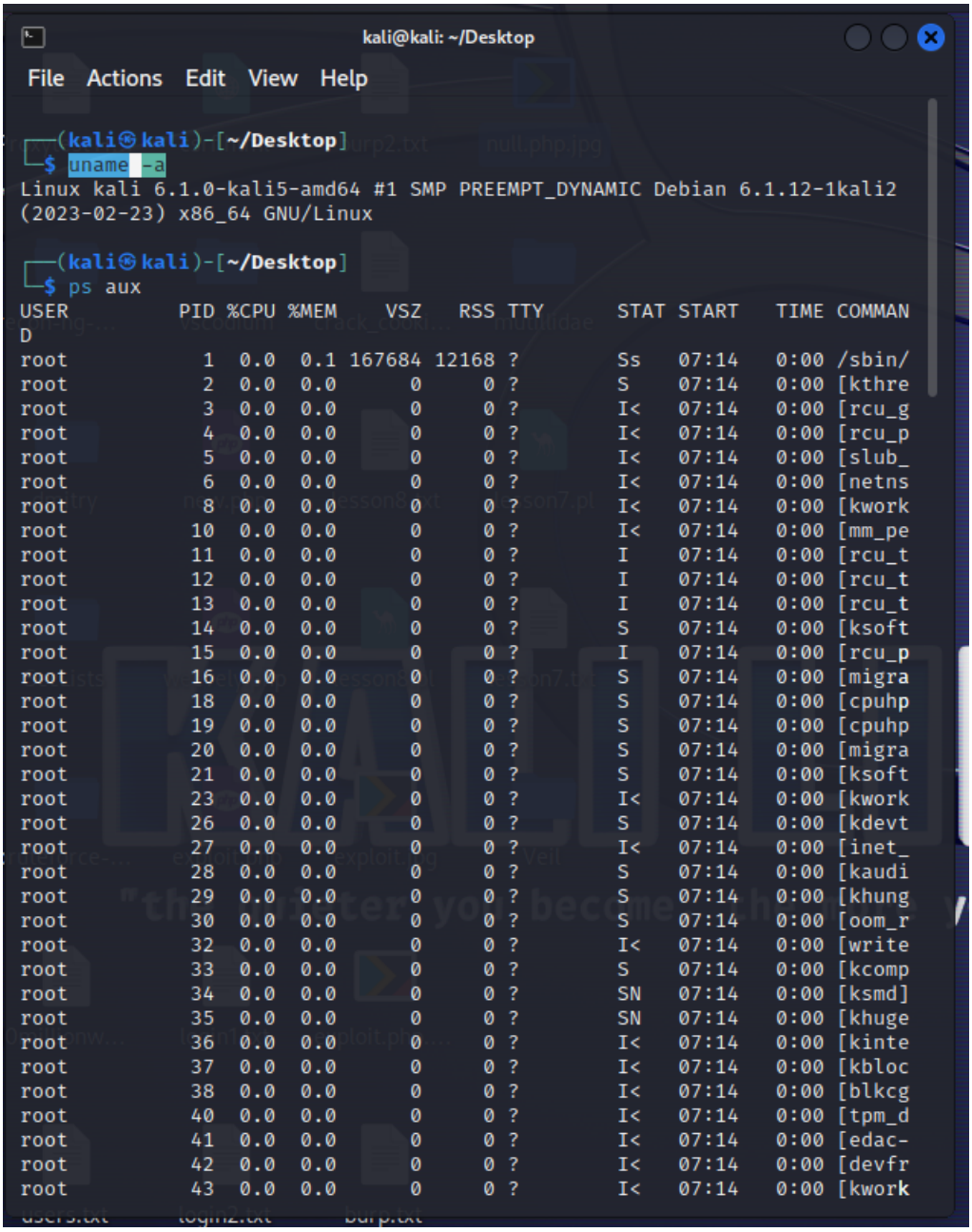
Assignment #10 Conducting rapid reconnaissance of a compromised system.

Nathaly Flores
Old Dominion University
00597869

Kali Linux



From the list of the section conducting rapid reconnaissance of a compromised system, I use the commands whoami < tells you who you are by displaying the user, who -a < who is logged in, ifconfig -a < displaying the current network interface configuration information like IP network address and netstat -r < nestat -r is used to show the network status, and those are the results of those commands in kali Linux and what they do.

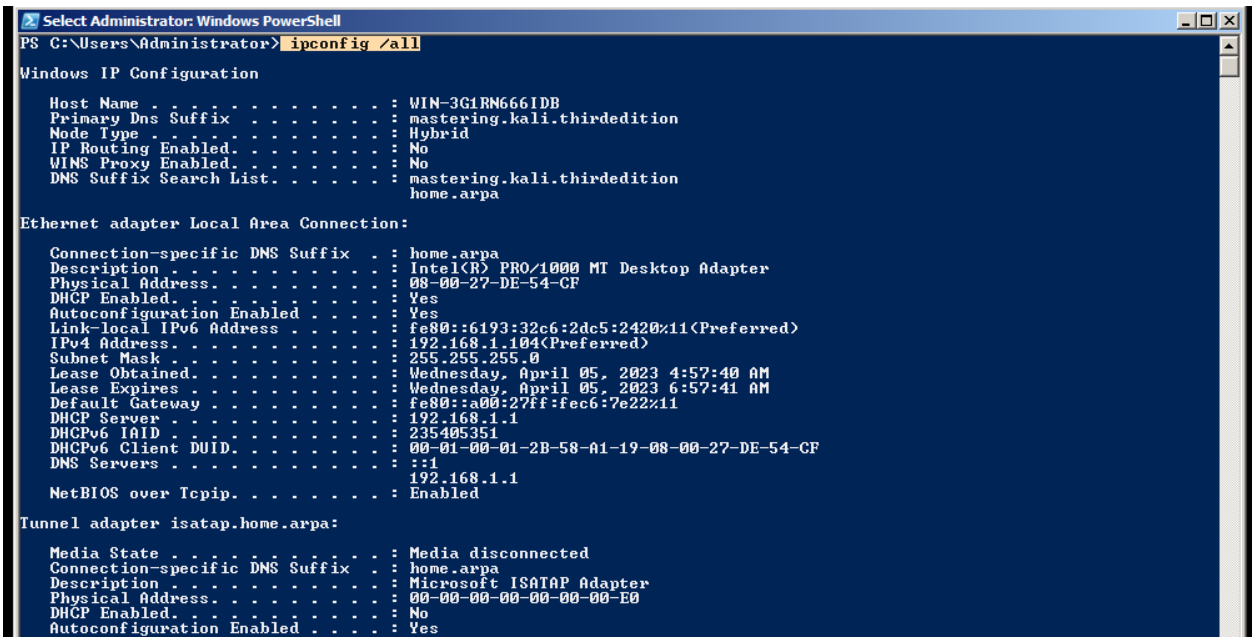


In the screenshot above, I also used the commands uname -a and ps aux. Ps aux gave out more results than uname -a . uname -a command you obtain the information about the system vs. ps aux that monitors the process running on the Linux system.

Windows

```
Select Administrator: Windows PowerShell
PS C:\Users\Administrator> whoami /all

USER INFORMATION
----------------

User Name                SID
======================== ==============================================
mastering\administrator S-1-5-21-1888473132-1320757285-3667122217-500


GROUP INFORMATION
-----------------

Group Name                                   Type             SID                                          Attribut
es
============================================ ================ ============================================ ========
=====================================================
Everyone                                     Well-known group S-1-1-0                                      Mandator
y group, Enabled by default, Enabled group
BUILTIN\Administrators                       Alias            S-1-5-32-544                                 Mandator
y group, Enabled by default, Enabled group, Group owner
BUILTIN\Users                                Alias            S-1-5-32-545                                 Mandator
y group, Enabled by default, Enabled group
BUILTIN\Pre-Windows 2000 Compatible Access   Alias            S-1-5-32-554                                 Mandator
y group, Enabled by default, Enabled group
NT AUTHORITY\INTERACTIVE                     Well-known group S-1-5-4                                      Mandator
y group, Enabled by default, Enabled group
CONSOLE LOGON                                Well-known group S-1-2-1                                      Mandator
y group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users             Well-known group S-1-5-11                                     Mandator
y group, Enabled by default, Enabled group
NT AUTHORITY\This Organization               Well-known group S-1-5-15                                     Mandator
y group, Enabled by default, Enabled group
LOCAL                                        Well-known group S-1-2-0                                      Mandator
y group, Enabled by default, Enabled group
MASTERING\Domain Admins                      Group            S-1-5-21-1888473132-1320757285-3667122217-512 Mandator
y group, Enabled by default, Enabled group
MASTERING\Group Policy Creator Owners        Group            S-1-5-21-1888473132-1320757285-3667122217-520 Mandator
y group, Enabled by default, Enabled group
MASTERING\Enterprise Admins                  Group            S-1-5-21-1888473132-1320757285-3667122217-519 Mandator
y group, Enabled by default, Enabled group
MASTERING\Schema Admins                      Group            S-1-5-21-1888473132-1320757285-3667122217-518 Mandator
y group, Enabled by default, Enabled group
MASTERING\Denied RODC Password Replication Group Alias        S-1-5-21-1888473132-1320757285-3667122217-572 Mandator
y group, Enabled by default, Enabled group
Mandatory Label\High Mandatory Level         Label            S-1-16-12288                                  Mandator
y group, Enabled by default, Enabled group, Local Group


PRIVILEGES INFORMATION
----------------------

Privilege Name                    Description                                                  State
================================= ============================================================ ========
SeIncreaseQuotaPrivilege          Adjust memory quotas for a process                           Disabled
SeMachineAccountPrivilege         Add workstations to domain                                   Disabled
SeSecurityPrivilege               Manage auditing and security log                             Disabled
SeTakeOwnershipPrivilege          Take ownership of files or other objects                     Disabled
SeLoadDriverPrivilege             Load and unload device drivers                               Disabled
SeSystemProfilePrivilege          Profile system performance                                   Disabled
SeSystemtimePrivilege             Change the system time                                       Disabled
SeProfileSingleProcessPrivilege   Profile single process                                       Disabled
SeIncreaseBasePriorityPrivilege   Increase scheduling priority                                 Disabled
SeCreatePagefilePrivilege         Create a pagefile                                            Disabled
SeBackupPrivilege                 Back up files and directories                                Disabled
SeRestorePrivilege                Restore files and directories                                Disabled
```

The command whoami /all shows the list of the current user and their privileges.



```
Select Administrator: Windows PowerShell
PS C:\Users\Administrator> ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : WIN-3G1RN666IDB
   Primary Dns Suffix  . . . . . . . : mastering.kali.thirdedition
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : mastering.kali.thirdedition
                                       home.arpa

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : home.arpa
   Description . . . . . . . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
   Physical Address. . . . . . . . . : 08-00-27-DE-54-CF
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::6193:32c6:2dc5:2420%11(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.104(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Wednesday, April 05, 2023 4:57:40 AM
   Lease Expires . . . . . . . . . . : Wednesday, April 05, 2023 6:57:41 AM
   Default Gateway . . . . . . . . . : fe80::a00:27ff:fec6:7e22%11
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 235405351
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2B-58-A1-19-08-00-27-DE-54-CF
   DNS Servers . . . . . . . . . . . : ::1
                                       192.168.1.1
   NetBIOS over Tcpip. . . . . . . . : Enabled

Tunnel adapter isatap.home.arpa:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : home.arpa
   Description . . . . . . . . . . . : Microsoft ISATAP Adapter
   Physical Address. . . . . . . . . : 00-00-00-00-00-00-00-E0
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
```

This screenshot I also did command ipconfig /all it list all the users and privileges; I can see where a hacker will try to benefit from these commands including the ones, I will being showing in a few.

```
PS C:\Users\Administrator> netstat -r
===========================================================================
Interface List
 11...08 00 27 de 54 cf ......Intel(R) PRO/1000 MT Desktop Adapter
  1...........................Software Loopback Interface 1
 12...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    306
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    306
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    306
      192.168.1.0    255.255.255.0         On-link     192.168.1.104    266
    192.168.1.104  255.255.255.255         On-link     192.168.1.104    266
    192.168.1.255  255.255.255.255         On-link     192.168.1.104    266
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    306
        224.0.0.0        240.0.0.0         On-link     192.168.1.104    266
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    306
  255.255.255.255  255.255.255.255         On-link     192.168.1.104    266
===========================================================================
Persistent Routes:
  None

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
 11    266 ::/0                     fe80::a00:27ff:fec6:7e22
  1    306 ::1/128                  On-link
 11    266 fe80::/64                On-link
 11    266 fe80::6193:32c6:2dc5:2420/128
                                    On-link
  1    306 ff00::/8                 On-link
 11    266 ff00::/8                 On-link
===========================================================================
Persistent Routes:
  None
PS C:\Users\Administrator>
```

Command netstat -r shows the ports and connection the main purpose of netstat -r is to display network status and protocol statistics.

```
Select Administrator: Windows PowerShell
PS C:\Users\Administrator> net view and net view /domain
The syntax of this command is:

NET VIEW
[\\computername [/CACHE] | [/ALL] | /DOMAIN[:domainname]]

PS C:\Users\Administrator> net user %username%/domain
The syntax of this command is:

NET USER
[username [password | *] [options]] [/DOMAIN]
         username {password | *} /ADD [options] [/DOMAIN]
         username [/DELETE] [/DOMAIN]
         username [/TIMES:{times | ALL}]

PS C:\Users\Administrator> net accounts
Force user logoff how long after time expires?:       Never
Minimum password age (days):                          1
Maximum password age (days):                          42
Minimum password length:                              7
Length of password history maintained:                24
Lockout threshold:                                    Never
Lockout duration (minutes):                           30
Lockout observation window (minutes):                 30
Computer role:                                        PRIMARY
The command completed successfully.

PS C:\Users\Administrator> net localgroup administrators
Alias name     administrators
Comment        Administrators have complete and unrestricted access to the computer/domain

Members

-------------------------------------------------------------------------------
Administrator
Domain Admins
Enterprise Admins
The command completed successfully.

PS C:\Users\Administrator> net group "Domain Controllers" /domain
Group name     Domain Controllers
Comment        All domain controllers in the domain

Members

-------------------------------------------------------------------------------
WIN-3G1RN666IDB$
The command completed successfully.

PS C:\Users\Administrator> net share

Share name   Resource                        Remark

-------------------------------------------------------------------------------
C$           C:\                             Default share
IPC$                                         Remote IPC
ADMIN$       C:\Windows                      Remote Admin
NETLOGON     C:\Windows\SYSVOL\sysvol\mastering.kali.thirdedition\SCRIPTS
                                             Logon server share
SYSVOL       C:\Windows\SYSVOL\sysvol        Logon server share
The command completed successfully.

PS C:\Users\Administrator> _
```

In this screenshot, I tried various commands like net view and net view /domain <locates all current host, net user /domain <lists all users in the domain, net user %username% /domain< shows current user like local user and domains, net accounts < prints the password for the policy, netlocalgroup administrators <members of the local administrator group, the net group “Domain Controllers” /domain< gives domain controller list, net share < this displays the currently shared folders.

Real-world, Produce a game plan. You have been made aware that your hacking crew is going after Equifax; using information from reports of their last massive breach, put together a brief 1–2-page write-up on the steps you would take to gain access to systems using this week's tools and methods.

Equifax

One of the first steps in hacking would be reconnaissance to gather information about my target. In this reconnaissance, one of the main objectives will be researching information about the company's infrastructure and identifying possible vulnerabilities, and gathering information on employees or other workers that are part of the company.

Tools and methods:

1. Social engineering strategies like phishing emails or phone calls to the company. Winning the employee's trust to divulge sensitive information or credentials.
2. Do a network scan like utilizing Nmap or Nessus to pinpoint what open ports and services are being used in the network target.
3. Utilizing web application scanners like burp suite or OWAS Zap can show the vulnerabilities of web-based applications.
4. Utilizing open-source intelligence like using Maltego, Shodan, or recon-ng these tools can show further information about the target network and the services they are using, including their employees.
5. Conducting rapid reconnaissance of a compromised system, you can use Metasploit framework/meterpreter in Kali Linux using a password file that can be found to try to break into companies' employee accounts.

6. You can use the Empire project; this tool allows you to see the system vulnerabilities of the company you want to target. Mimikatz, you can use this tool without having to plant a backdoor.
7. Crack-Map-Exec will collect information to perform lateral movement and privileges attacks.

Once reconnaissance is done, the hacking team can access the target network or system. This could concern exploiting vulnerabilities identified during reconnaissance, employing stolen or weak credentials, or utilizing social engineering strategies to acquire access. Some of the tools and methods that could be used for gaining access might include:

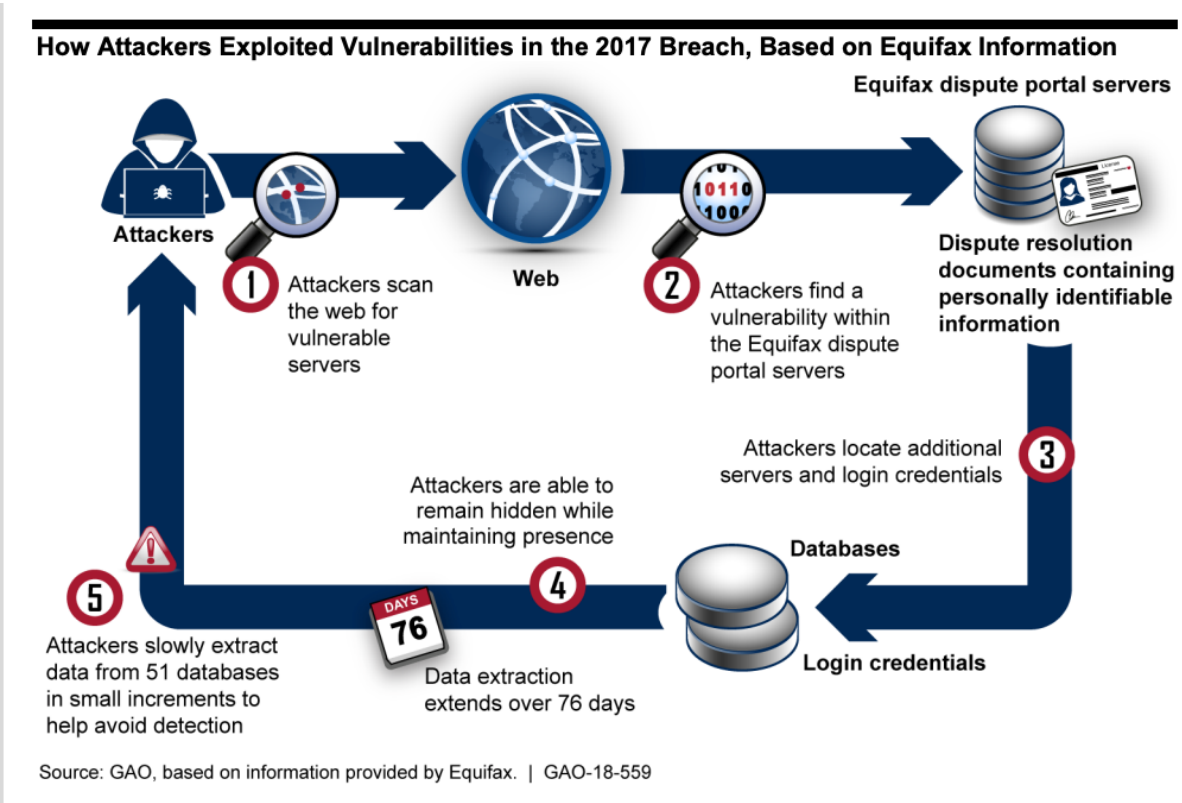
1. Exploitation frameworks, like Metasploit or Exploit DB, leverage known vulnerabilities in software or systems.
2. Password cracking tools like John, the Ripper, or Hash cat these tools are utilized to crack weak or stolen passwords.
3. Using social engineering methods like spear phishing or pretexting.
4. Brute force attacks against the target systems' weak passwords or default credentials.

Once the hacking team is in the target system and gained access, they can escalate the privileges and move laterally through the network by hacking and gaining access to other systems and sensitive information. At this point, covering your tricks to avoid being detected by the security teams is necessary. Tools and methods that can be used:

1. Privilege escalation tools, like PowerSploit or Psexec, to achieve administrative privileges on compromised systems.

2. Post-exploitation frameworks, like Cobalt Strike or Empire, preserve persistence on compromised systems and move laterally through the network.
3. Anti-forensic tools, like CCleaner or BleachBit, cover their tracks and avoid detection by security teams.

The final step is covering their tracks to avoid detection by security teams. This can be done using anti-forensic tools like CCleaner or BleachBit. These steps show in real scenarios what hackers can do to hide their tracks.



The above screenshot demonstrates how attackers exploited vulnerabilities.

Equifax, a major credit reporting company in the US, had a data breach in 2017 that exposed over 143 million customers' sensitive information, such as names, birth dates, and Social Security numbers. The breach was due to a vulnerability in Equifax's web application framework, Apache Struts, discovered and patched earlier but not applied by Equifax. The hackers exploited this vulnerability to access Equifax's systems and extract data. It is believed they used a combination of custom-made and publicly available software tools, such as Metasploit, to identify and exploit vulnerabilities and maintain their access. This breach highlights the importance of timely patching, vulnerability management, and robust cybersecurity measures to protect sensitive data.

Works Cited

Commission, F. T. (2022). Equifax Data Breach Settlement . *Federal Trade Commission* .

Commission, U. S. (2018). SEC Charges Ameriprise With Overcharging Retirement Account Customers for Mutual Fund Shares. *Sec Order*.

Office, U. S. (2018). Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach. *United States Government Accountability Office*.

Reform, U. H. (2018). The Equifax Data Breach. *Majority Staff Report 115th Congress*.

These references provide information on the breach itself, the aftermath and consequences, and the responses of both Equifax and government agencies.