Test Project for CYBER SECURITY

*Infrastructure Hardening & Incident Response*

**Regionals (West)**

Ahmedabad

# Module

## Introduction

The competition has a fixed start and finish time. You must decide how to best divide your time.

Please **carefully** **read** the following instructions!

When the competition time ends, please leave your station in a running state. The assessment will be done in the state as it is. *No reboot will be initiated as well as powered off machines will not be powered on!*

The provided tasks can be completed in any order. Just ensure that all goals are achieved

## Challenge Server (Individual for EACH Team)

A windows server, running on 2 vCPU and 4GB RAM will be provisioned for Security Hardening.

All traffic to the servers would be logged

Administrator credentials to the server would be provided on site

## Challenge Server (Individual for EACH Team)

The webserver is an Ubuntu 20.04 machine running on 2 vCPU and 4GB RAM

All traffic to the servers would be logged

Root credentials to the server would be provided on site

## File Server (COMMON for EACH Team)

All teams will have access to a common file server to download files relevant to the challenge (Private key, etc..) as well as other files which deemed relevant for the competition to not provide unfair advantage to any team

## TIE-Breaker

Teams are encouraged to improve the security of the provided servers by whatever means they deem fit without compromising the accessibility of the website. Mention these steps in the excel sheet. If the additional steps are security relevant steps, these steps would be considered for tie-breaker.

# Tasks

**Part 1: Infrastructure Hardening**

In Part 1 you will be responsible for hardening the infrastructure provided to you

1. **Windows Server Hardening**
   1. Enforce password policy with below configuration

|  |  |  |
| --- | --- | --- |
| **S. No** | **Policy Options** | **Configuration** |
| 1 | Enforce Password History | 5 passwords remembered |
| 2 | Maximum Password Age | 45 days ( maxium is 90) |
| 3 | Minimum Password Age | 3 days ( minimum is 1 |
| 4 | Minimum Password Length | 12 characters |

LOACL SERVER-> TOOLS-> ACTIVE Directory Users and Computers-> user ( all default settings are listed there

LOACL SERVER-> TOOLS-> Group Policy Management -> Forest ->

Domains -> Dafault Domain Policy or

-> Group Policy Objects -> Default Domain Policy -> edit( right Click)

Compute Configuration -> Polices ->windows Settings -> Security Settings -> Account Policy -> Password Policy

* 1. Enforce password complexity

( IF DISABLE THEN ENABLE -> PASSWORD MUST MEET COMPLEXITY REQUIREMENTS)

* 1. Implement the best practice for password storage

A knowledgeable attacker who is able to break this encryption can then sign in to network resources by using the compromised account. For this reason, never enable Store password using reversible encryption for all users in the domain unless application requirements outweigh the need to protect password information

( IF DISABLE THEN LEAVE IT -> STORE PASSWORD USING REVERSIBLE ENCRYPTION)

* 1. Implement the account lockout policy for not to get unlocked automatically

Compute Configuration -> Polices ->windows Settings -> Security Settings -> Account Policy ->Account Lockout Policy

Account Lookout Threshold Properties

3 is threshold

Account LookOut Duration

30 min

Reset account lookout counter after

30 min

* 1. Enable all events to be logged for:
     1. Audit Credential Validation
     2. Audit Kerberos Authentication Services
     3. Audit Kerberos Service Ticket Operations
     4. Audit other account login events
* Launch **Server Manager** in your Windows Server instance.
* Under Manage, select **Group Policy Management** and launch the **Group Policy Management console**.
* Navigate to **Forest ➔ Domain ➔ Your domain ➔ Domain Controllers**.
* Create a new GPO and link it to the domain containing the file to be monitored, or edit any existing GPO that is linked to the domain to open the **Group Policy Management Editor**.
* Navigate to **Computer Configuration ➔ Windows Settings ➔ Security Settings ➔ Advanced Audit Policy Configuration ➔ System Audit Policies - Local Group Policy ➔ Account Logon**.
* The Account Logon lists all of its sub-policies in the right panel, as shown in the figure below.
* Select the **Audit Credential Validation** and enable audit for **Success** and **Failure** events.
* Select the Audit Kerberos Authentication Services and enable audit for **Success** and **Failure** events.
* Select the Audit Kerberos Service Ticket Operation and enable audit for **Success** and **Failure** events.
* Select the Audit other account login events and enable audit for **Success** and **Failure** events.
* Click **Apply** and **OK** to close **Properties** window.
  1. Implement the appropriate rights assignment to the provided user / group.
     1. Ensure only Administrators and Authenticated Users group are authorized to logon to the computer in the network

LOACL SERVER-> TOOLS-> ACTIVE Directory Users and Computers-> Techforall Users -> IT Department -> select a user

Right clisk -> properties -> Account -> Log on -> ( there will be all computer by default change it to specific computer which you want to give acess.-> add -> apply -> ok -> apply

* + 1. Restrict the system time and time zone change privilege only to the Administrators group & Local Service

Cmd-> secpol.msc -> Local Security Policy -> Secuity settings -> local Policies -> User Rights Assignment -> Change the time Zone Policy -> ( you can add or delete )

* + 1. Guests user account should not be allowed to login to the system

Terminal Method:  
Run the following command to disable the guest account:  
  
$ /usr/bin/sudo /usr/bin/defaults write /Library/Preferences/com.apple.loginwindow GuestEnabled -bool false

1. Graphical Method: ...
2. Open System Settings.
3. Select Users & Groups.
4. Select the i next to the Guest User.
5. Set Allow guests to log in to this computer to disabled.
   1. Implement Security Options for:
      1. Disabling USB Storage Devices access

LOACL SERVER-> TOOLS-> Group Policy Management -> Forest ->

Domains ->mylab.local -> create a gpo in this domain ( removable Driver Access Deny GPO ) -> ok

Right click edit -> computer Configuration -> Polices -> Administrative Templates -> System -> Removable Storage Access -> All Removable Storage Classes -> Enabled

* + 1. Not to display logged on user information either when locked

Tools -> Group Policy Management -> Forest -> domain -> (name ) -> Default Domain Policy -> right click edit ->

Default Domain Policy -> Computer Configuration -> Polices -> Windows Settings -> Security Settings -> local Polices -> Security Options -> slect the the task and edit it according to the command and then apply .-> and then enable it

gpupdate /force

* + 1. Not to display logged on user information either when logged off

Tools -> Group Policy Management -> Forest -> domain -> (name ) -> Default Domain Policy -> right click edit ->

Default Domain Policy -> Computer Configuration -> Polices -> Windows Settings -> Security Settings -> local Polices -> Security Options -> select the the task and edit it according to the command and then apply .-> and then enable it

gpupdate /force

* + 1. Display the below text as title whenever any user logs in

**“Welcome to IndiaSkills Regionals (West)!!!”**

Tools -> Group Policy Management -> Forest -> domain -> (name ) -> Default Domain Policy -> right click edit ->

Default Domain Policy -> Computer Configuration -> Polices -> Windows Settings -> Security Settings -> local Polices -> Security Options -> select the task write what you need and then apply

* + 1. Display the below text as content whenever any user logs in

**“This system is restricted to authorized users only!”**

Tools -> Group Policy Management -> Forest -> domain -> (name ) -> Default Domain Policy -> right click edit ->

Default Domain Policy -> Computer Configuration -> Polices -> Windows Settings -> Security Settings -> local Polices -> Security Options -> select the task write what you need and then apply

* 1. Disable “NetBIOS over TCP/IP”

Network and sharing center -> change adapter settings -> if ethernet is not working then select it or check of local -> right click on properties -> select internet protocol version 4 tcp/ipv4 -> click on properties and go to advance -> go to WINS -> now you can disable NetBIOS over TCP/IP

* 1. Disable POSIX subsystem
  2. Disable SMB v1 support
  3. Enforce the stronger encryption protocol (TLS 1.2 ) and disable legacy/weak protocol (SSL 2.0, SSL 3.0, TLS 1.0, TLS 1.1) support

Registory Editor -> HKEY\_LOCAL\_MACHINE -> SYSTEM -> CurrentControlSet -> Control -> Security Providers -> Schannel -> Protocols

Create new key and name them ssl 2.0, 3.0 and TLS 1.0, 1.1,

Create one server and client key in all

Create a DWORD ( 32 BIT VALUE ) AND NAME THEM

Enable 0

Disablebydefault 1

Create new key and name them TLS 1.2

Create one server and client key in all

Create a DWORD ( 32 BIT VALUE ) AND NAME THEM

Enable 1

Disablebydefault 0

1. **Linux Server SSH Policies**
   1. Setup SSH Policy on the server to only allow access through the provided private key

To avoid a password prompt from master computer to client

ssh-keygen ( by default it will generate rsa key for encryption )

( enter for location )

( enter for passphrase its like a password over password

( enter )

We got two files in that location public key and private key

Copy the file to master and paste the public key

ssh-copy-id -i /root/.ssh/id\_rsa.pub root@client-server

( frist time you need to enter password )

Ssh client-server

* 1. Setup SSH MOTD Banner “Unauthorized Access is prohibited!”

Custom ssh warning banner

Sudo vim /etc/ssh/sshd\_config

Enter password

Un comment the Banner and get the banner location

Sudo vim banner location

Write save and exit

Systemctl restart sshd

Enter password

Ssh ip addresss

Warning banner before password

MOTD

Vl /etc/mo

Vl /etc/motd

Sudo /etc/motd

Write a text

Systemctl restart sshd

Password

Ssh ip address

Password

Warning banner after the password

1. **Snort**
   1. Write a Snort rule to alert and log for any ICMP traffic hitting on your sever

Cd /etc/snort/rules

Sudo nano icmp.rules

alert icmp any any => 192.168.1.77 (msg: “ICMP packet found”; std:10000001;)

sudo snort -A console -q -u snort -g snort -c /etc/snort/snort.conf -I ens33

1. **Certificate** 
   1. Setup a self-signed certificate for the provided IP and configure the website running on the server for HTTPS using nginx.

<https://www.humankode.com/ssl/create-a-selfsigned-certificate-for-nginx-in-5-minutes/>

1. **Misconfiguration**
   1. In your report mention all the misconfigurations you found in the server and how you fixed it. Ensure the website is functioning.

**Part 2: Security Monitoring**

In Part 2 you will be responsible for configuring Splunk (Security Information and Event Management) for security monitoring. Splunk is installed in Linux system. Splunk service and credentials will be provided separately.

1. **Integration of Windows**
   1. Integrate Windows system with Splunk to collect windows event logs (System, Application, Security)
   2. Ensure all logs are flowing to the Splunk platform
2. **Creation of Use Case and alerts**
   1. Write a correlation rule for detecting brute-force attempts with below criteria
      1. 3 consecutive failure attempts for the same user account in a span of 3 minutes
      2. Alert to be created for the investigation
   2. Write a correlation rule for detecting user account compromise
      1. instances of active session of a specific user account on multiple systems simultaneously
      2. Alert to be created for the investigation

**Part 3: Vulnerability Management**

List down 5 common protocols, its associated vulnerabilities and mitigation steps.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **S. No** | **Protocol** | **Port number** | **TCP / UDP?** | **Vulnerability** | **Remediation Step / Mitigation** |
|  | FTP | 21 | Tcp | Provides a way to transfer files between computers that operate on the simple get and put concepts to either receive or send files to a remote endpoint |  |
|  | Ssh | 22 | tcp | ability to connect to an endpoint over an unsecured network securely |  |
|  | Telnet | 23 | Tcp | allows interacting with a network endpoint from the command line |  |
|  | SMTP | 25 | Tcp | a protocol used to relay mail from email server to email server |  |
|  | Iamp | 145 | Tcp and udp | nternet Message Access Protocol synchronizes and displays emails without the need to download them |  |
|  | POP3 | 110 | TCP | Known as the Post Office Protocol, it is used by email clients to synchronize and download mail from remote mail servers |  |

What are the tips to ensure the ports security

1. **Conduct regular port scans –**Conducting regular port scans will help you find problems as they appear. Regular monitoring will also show you which ports are the most vulnerable to attack to create a better defense plan.
2. **Services monitoring** – It’s also important to focus on monitoring services, which allows gathering the details of running states of installed services and continuously tracking changes to service configuration settings. Services are vulnerable when they are unpatched or misconfigured. Using [Netwrix Change Tracker](https://www.netwrix.com/security_configuration_management_software.html), you can harden your systems by tracking unauthorized changes and other suspicious activities. In particular, it provides the following functionality:
   * Actionable alerting about configuration changes
   * Automatically recording, analyzing, validating and verifying every change
   * Real-time change monitoring
   * Constant application vulnerability monitoring
3. **Close all unused ports –**By disabling ports you’re not using, you’ll be able to protect your data from attackers.
4. **Continuously carry out port traffic filtering –**Port traffic filtering means blocking or allowing network packets into or out of your network based on their port number. It can protect you from cyber attacks associated with some ports. Most companies apply port traffic filtering to the most commonly vulnerable ports, such as port 20.
5. **Install firewalls on every host and patch firewalls regularly –**Firewalls will also block threat actors from accessing information through your ports. Remember to patch firewalls regularly for maximum efficacy.
6. **Monitor open port vulnerabilities –**Finally, you should monitor open port vulnerabilities. You can do this by:
   * **Using penetration testing to simulate attacks through open ports:**Penetration testing allows you to check for ports vulnerable to such attacks.
   * **Conducting vulnerability assessments:**Vulnerability assessment tools can protect your IT infrastructure by identifying which software or devices have opened ports and running tests for all known vulnerabilities.