worldskills India

Skill India
कौशल भारत - कुशल भारत

N·S·D·C
National Skill Development Corporation
Transforming the skill landscape

Module A

IndiaSkills National Competition

Cyber Security

NASSCOM®

Description

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
- Marking for each section has been provided in brackets

Report Submission Link: https://forms.gle/b94vTvv5HQ2ZTYEfA

Credentials

```
splunk -> splunk:splunk123
ubuntu(sudo user) -> ubuntu:ubuntu
```

Part 1: Hardening (21.75)

1. Windows Hardening (15.5)

a. Enforce password policy with below configuration

S. No	Policy Options	Configuration
1	Enforce Password History	5 passwords remembered
2	Maximum Password Age	45 days
3	Minimum Password Age	3 days
4	Minimum Password Length	12 characters

b. Enforce password complexity

c. Implement the best practice for password storage

d. Implement the account lockout policy
   - i. User account not to get unlocked automatically
   - ii. User account should get locked out after 5 invalid password attempts
   - iii. Account lockout reset counter to be set to 1 day

e. Enable all events to be logged for:
   - i. Audit Credential Validation
   - ii. Audit Kerberos Authentication Services
   - iii. Audit Kerberos Service Ticket Operations
   - iv. Audit other account login events

f. Implement the appropriate rights assignment to the provided user / group.
   - i. Ensure only Administrators and Authenticated Users group are authorized to logon to the computer in the network
   - ii. Restrict the system time and time zone change privilege only to the Administrators group & Local Service
   - iii. Guests user account should not be allowed to login to the system
   - iv. Allow only Administrators and Remote Desktop Users to logon remotely (interactive logon)
   - v. Allow Administrators and Power Users to force shutdown remotely

vi. Enable auditing and security log management for Administrators and Power Users

vii. Administrators alone should have the privilege for taking ownership of the files or other objects

viii. There should not be any user / group to log on as a service

ix. Administrators and Power Users should have the privilege for Loading and Unloading Device Drivers

x. Administrators alone to perform volume maintenance tasks

g. Implement Security Options for:

i. Disabling USB Storage Devices access

ii. Not to display logged on user information either when locked

iii. Not to display logged on user information either when logged off

iv. Display the below text as title whenever any user logs in

“Welcome to IndiaSkills!!!”

v. Display the below text as content whenever any user logs in

“This system is restricted to authorized users only!”

vi. Printer drivers shall be installed by Everyone

vii. Enable Interactive Logon: Machine inactivity limit to 10 minutes

viii. Enable Microsoft network server: Digitally sign communication (always)

ix. Disable Network access: Allow anonymous SID/Name translation

x. Ensure to prompt for credentials for User Account control: Behaviour of the elevation prompt for standard users.

h. Disable “NetBIOS over TCP/IP”

i. Disable POSIX subsystem

j. Disable SMB v1 support

k. 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

l. Define the below settings for Event Logging

S. No	Event Log Policy Attributes	Settings
1	Maximum application log size*	1048576 kilobytes
2	Maximum security log size*	1048576 kilobytes
3	Maximum system log size*	1048576 kilobytes
4	Prevent local guest group from accessing application log**	DWORD (1)
5	Prevent local guest group from accessing security log**	DWORD (1)
6	Prevent local guest group from accessing system log**	DWORD (1)

* - to be defined on Group Policy Editor

** - to be defined in Windows Registry

m. Enable logging for Print auditing

n. Implement the below security configuration settings on Windows Defender Firewall

i. Create an inbound rule for the below condition

1. Create a FTP inbound rule (Port 21) for allowing connections only if it is secure
2. Allow connections only for Administrators group
3. No Exception users / groups
4. Implement the rule for Private networks only
5. Rule Name to be provided as “FTP Rule for Indiaskills”

o. Configure the system to open .reg file with notepad.exe

p. Disable below services in the Computer Policy settings

i. Cortana

ii. Location

iii. Sensors

iv. Windows Mail

v. Force automatic setup for all users (under Work folder)

q. Define below Windows Security – App and Browser control

Check Apps and files	Warn / On
SmartScreen for Microsoft Edge	Warn / On
SmartScreen for Windows Store apps	Warn / On
Exploit protection	Control flow guard: ON Data Execution Prevention: ON Force randomization for images: OFF Randomize Memory allocation: ON Validate exception chain: ON Validate heap integrity: ON

r. Disable Multicast Name resolution

s. Configure NETLOGON and SYSVOL shares as below

Value Name	Value
*\NETLOGON	RequireMutualAuthentication=1, RequireIntegrity=1
*\SYSVOL	RequireMutualAuthentication=1, RequireIntegrity=1

t. Configure below Remote Desktop session configuration

Setting	Recommendation	Value
Set time limit for disconnected sessions	Enabled	30 Minutes
Set time limit for active but idle Remote Desktop Service sessions	Enabled	1 hours
Set time limit for active Remote Desktop Services Session	Enabled	1 day

2. Linux Hardening (6.25)

a. Restrict root login to system console

b. Enable Login Banner with the message “Welcome to IndiaSkills!!!”

c. Enforce automatic logoff for user accounts after 600 seconds of no activity

d. Enforce password policy with below configuration

   i. Maximum Password age – 45 days

   ii. Minimum Password age – 3 days

   iii. Password expiry notification – 10 days

e. Define password rules as below

   i. Minimum password length – 8 characters

   ii. Minimum number of lower case letters – 1 letter

   iii. Minimum number of upper case letters – 1 letter

   iv. Minimum number of digits – 1 digit

   v. Minimum number of other (special) character – 1 character

f. Enable password history to remember past 5 passwords

g. Secure SSH services with following security configuration / policies

   i. Setup SSH Policy on the server to only allow access through the provided private key

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

   iii. Limit the SSH protocol to version 2 (disable SSH protocol version 1)

   iv. Enable logging of login and logout activity

   v. Restrict SSH X11 forwarding (X11 tunnelling)

   vi. Disable .rhosts file

   vii. Set SSH HostbasedAuthentication to NO

viii. Set SSH PermitEmptyPasswords to NO
ix. Do not allow users to set environment options
x. Set login grace time to 60 seconds
xi. Enable StrictModes
xii. Restrict SSH from setting up TCP Port forwarding
xiii. Enable Privilege separation

Part 2: Security Monitoring (3.25)

1. Integration of Windows & Linux

a. Integrate Windows system with Splunk to collect windows event logs (System, Application, Security)
b. Integrate Linux logs with Splunk to collect Linux host logs
c. Integrate Linux logs with Splunk to collect Linux SSH logs

Note: Ensure all logs are flowing to the Splunk platform

2. Creation of Use Case and alerts

a. Write a correlation rule for detecting brute-force attempts with below criteria
    i. 3 consecutive failure attempts for the same user account in a span of 3 minutes
    ii. Alert to be created for the investigation
b. Write a correlation rule for detecting user account compromise
    i. instances of active session of a specific user account on multiple systems simultaneously
    ii. Alert to be created for the investigation
c. Write a correlation rule for triggering alert when multiple failed logins are observed from the same IP (Windows)
d. Write a correlation rule for triggering alert when multiple failed logins are observed from the same IP (Linux)
e. Write a correlation rule for triggering alert when multiple failed logins are observed from the same IP (Linux-SSH)
f. Write a correlation rule to trigger alert whenever there is a creation of a user account with super user privileges (Linux)
g. Write a correlation rule to trigger alert whenever there is a creation of a user account with super user privileges (Windows)
h. Write a correlation rule to trigger alert whenever there is a search for password files using grep or find (Linux)
i. Write a correlation rule to trigger alert whenever there is a password change activity observed for any user account (Windows)

j. Write a correlation rule to trigger alert whenever there is a password change activity observed for any user account (Linux)

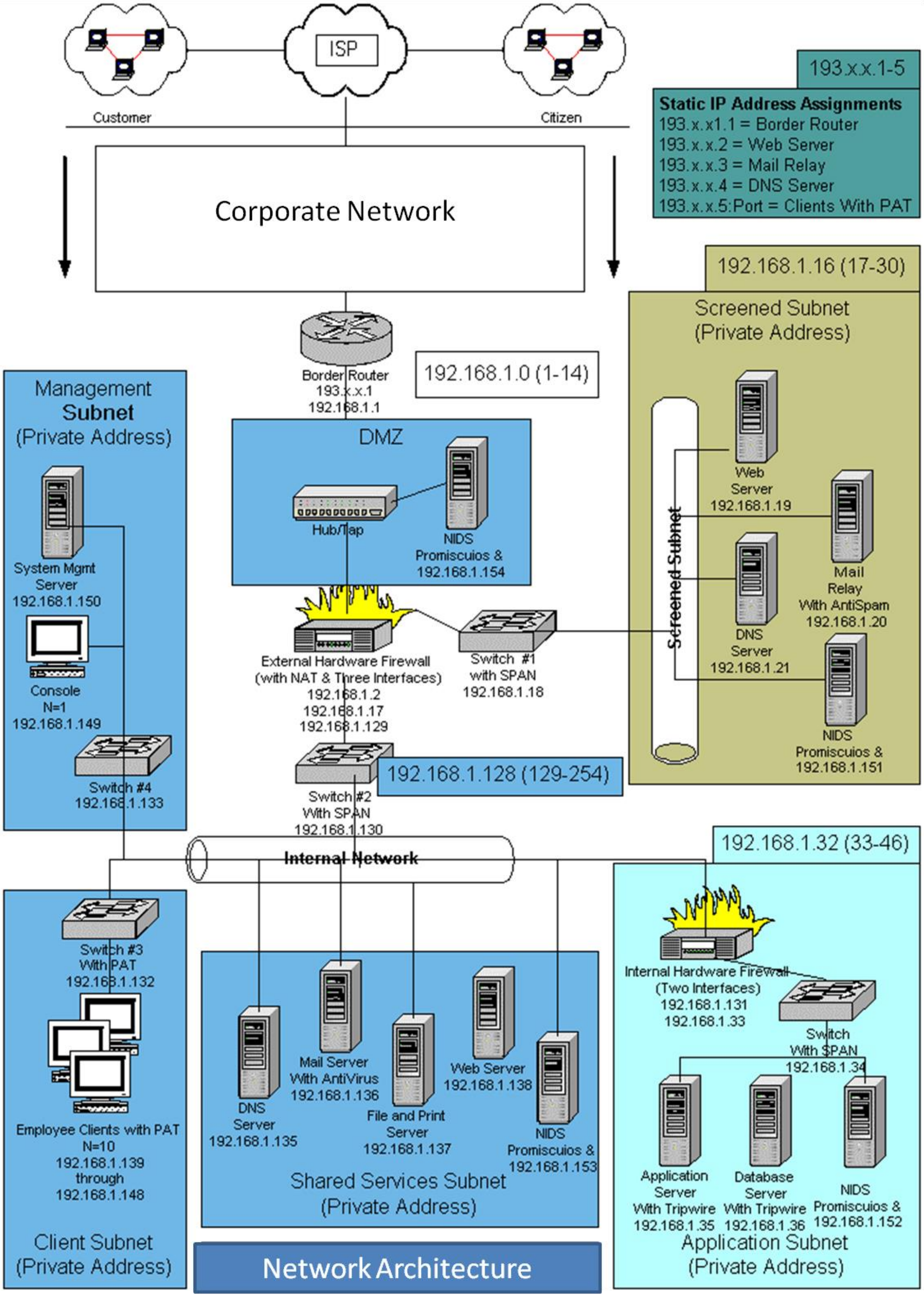
Part 3: Malware Analysis (4)

On the desktop, analyze the malwares in the folder malware using IDA and leave a comprehensive report on the system. The filename should be *YourState_YourName.pdf*. You can use Google docs for creating the report.

Part 4: Network Architecture Review (3.5)

Study the architecture diagram and put answers to the following question in your report:

1. What are the best practices followed in this network architecture?
2. Is there any device placed / positioned wrongly? If so, list down device(s) and justify the reason. Also suggest on the appropriate positioning/placement of the device(s).
3. Any specific recommendation to enhance security on this architecture (can be controls, technology, devices etc)



Network Architecture