worldskills

Test Project

Cyber Security

Infrastructure Setup and Security Hardening

Submitted by: Module A group
Kamadchisundaram Sureshkumar UK

Sangamesh Shivaputrappa IN

Joey Joseph Villota PH

Guadalupe de Jesus Mejia Servin MX

Manal Al Rawahi OM

Yi-Ming Chen TW

Contents

Introduction to Test Project

The following is a list of sections or information that must be included in all Test Project proposals that are submitted to WorldSkills.

- Contents including list of all documents, drawings and photographs that make up the Test Project
- Introduction/overview
- Short description of project and tasks
- Instructions to the Competitor
- Equipment, machinery, installations and materials required to complete the Test Project
- Marking scheme (incl. assessment criteria)
- Other

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!

Please do not touch the VMware configuration as well as the configuration of the VM itself except the CD-ROM / HDD drives

PHYSICAL MACHINE (HOST)

FOLDER PATHS

ISO Images:	VMware ESXi Datastore

LOGIN

Username:	root / skill54 / LDAP-Users
Password:	LdSkill54
Domain:	wsc19.cloud

SYSTEM CONFIGURATION

Region:	Russian Federation
Locale:	English US (UTF-8)
Key Map:	English US

Description of project and tasks

You are a junior Information Security Analyst and you have the task to implement a complex security infrastructure environment for an international assembly of professional experts. The requirements are gathered where possible and documented. Please get an overview of the project by studying the topology diagram at the end of this document.

System configuration (general)

Please install and configure all networking, server and client systems according to the specification. Please use the credentials and settings stated.

Configure all servers with the correct hostname and network settings found in the appendix and in topology.

Please use the default configurations if you are not given any details.

You are provided with following equipment and accessories:

- Windows 2016 Server
- CentOS 7
- Windows 10 client
- Cisco 2960 Switch
- Cisco 4221 router
- ASA 5506-X
- Cisco Rollover cable
- RJ45 UTP LAN cables
- Wireless Access Point

General tasks

Part 1: Start-up configuration

Network device/Label	IP address	Host ID / Passwords	VM ID / Passwords
Outside	209.165.200.226/30		
DMZ	192.168.2.1/24		
INSIDE	192.168.10.1/24		
R1	**Start-up Configuration** hostname R1 no ip domain lookup interface G0/1 ip address 130.18.30.1 255.255.255.0 no shut int G0/0 ip address 209.165.200.234 255.255.255.252 no shutdown ip route 0.0.0.0 0.0.0.0 209.165.200.233		

Network device/Label	IP address	Host ID / Passwords	VM ID / Passwords
SW-1	**Startup Configuration** hostname SW-1 no ip domain lookup		
SW-2	**start-up Configuration** hostname SW-2 no ip domain lookup		
AD-Svr	IP Address: 192.168.10.10 Subnet Mask: 255.255.255.0 Default Gateway: 192.168.10.1	wss/P@ssw0rd1	VM1
CentOS-01	IP Address: 192.168.10.11 Subnet Mask: 255.255.255.0 Default Gateway: 192.168.10.1	wss/P@ssw0rd1	VM2
CentOS-02	IP Address: 192.168.2.10 Subnet Mask: 255.255.255.0 Default Gateway: 192.168.2.1	wss/P@ssw0rd1	VM3
CentOS-03	IP Address: 192.168.2.11 Subnet Mask: 255.255.255.0 Default Gateway: 192.168.2.1	wss/P@ssw0rd1	VM4
CentOS-04	**Start-up Configuration** hostname CentOS-04 interface to WS-ASA ip address 209.165.200.225 255.255.255.252 interface to R1 ip address 209.165.200.233 255.255.255.252	wss/P@ssw0rd1	VM5
Windows outside host	IP Address: 130.18.30.10 Subnet Mask: 255.255.255.0 Default Gateway: 130.18.30.1	wss/P@ssw0rd1	
Linux Client host	IP address setting varies for testing purpose. Please set appropriate IP addresses when you are testing.		

Network device/Label	IP address	Host ID / Passwords	VM ID / Passwords
Win Client host	IP address setting varies for testing purpose. Please set appropriate IP addresses when you are testing.		

Part 2: Windows server configuration

In Part 2 you will be responsible for preparing the new domain

1. Windows server configuration

- Hostname: **AD-Svr**
- Configure this server as the root domain controller for RUSSIA.LOCAL
- Add new Network Admin and Corporate user groups and accounts in Microsoft AD
  (For ease of checking by judges – set to "User cannot change password" and "Password never expires").
- Configure Windows Network Policy Server (NPS) according to the requirements.
- Configure user profiles, home drives and shared folders
  - Enable Roaming Profile and store the profiles at \\AD-Svr\profiles\username
  - Create for every user a home folder stored at \\AD-Svr\home\username and ensure that this mapped to H: drive automatically.
  - Set the quota for every home drive folder to 20MB
  - Prevent any 3 known malware files to be stored on home folders. Allow other file extensions.
- Perform a baseline analysis of the client computer using the Performance monitor. Create a User Defined Data Collector set with the following settings:
  - Create a performance counter log containing the following counters:
    - Average disk queue length
    - % Processor time
    - Available memory in MB
  - Samples should be taken every 30 seconds
  - The log should be saved to a new folder named Baseline on the C drive.
  - Allow the Data Collector to run for about 1 minute and then stop it running.
- GPO
  - Place the warning banner in the Message Text for users attempting to log on.
    - Message text - Unauthorized Access is prohibited!
  - Configure Login/Logoff audit policy.
  - Configure policy Change audit policy.
  - Configure the policy to audit object access.
  - Set RDP connection encryption level to high.
  - Disable the guest account.
  - Configure Event Log retention method and size. Set maximum log size to 3 GB.
- WSUS

- Setup the AD-Svr as a WSUS server. I know you cannot connect to the internet but I need it ready for when we can.
- Configure the AD-Svr to collect updates for All Products but only Critical and Security Classifications. The server must synchronize manually and approvals set to be automatic.
- Configure all windows computers to get updates from the WSUS server.

- Configure that the following programs/services are allowed through the client and server firewalls:
  - Windows Remote Management
  - Remote Desktop
  - Remote Assistance
  - Network Discovery
- Implement IPsec communication using Kerberos authentication.

2. Windows Client configuration

- Hostname: WIN-CLI
- Join the RUSSIA.LOCAL domain

Part 3: CentOS-01 configuration

In part 3 you will be responsible for preparing the CentOS-01 server.

1. User Creation

Create the following users:

User	Password
Kevin Smith	P@ssw0rd2
Muhsin Jumaa	P@ssw0rd3
Rachel Jones	P@ssw0rd4
Kelly Cutforth	P@ssw0rd5

2. Passwords security

The password must be set to achieve the following:

- Passwords must be changed every 30 days
- You cannot use any of the previous 5 passwords
- Passwords must have a minimum of 8 characters
- Passwords must be complex. Use the following types of characters:
  (a) 1 uppercase letter as the first letter,
  (b) 4 lowercase letters,
  (c) 2 numbers,
  (d) 1 special character.

3. Account security

The account must be set to achieve the following:

- Accounts will be locked after 2 bad password attempts
- The number of bad password attempts will reset after 1 hour.

4. Secondary DNS Server

Install and configure a secondary DNS server for AD-Svr. Set up secure communication between DNS servers.

5. Syslog Server

Configure the CentOS-01 server as a Syslog server to perform necessary configurations to log severity "Informational" messages from WS-ASA, SW-1 and SW-2.

6. Splunk

Install and configure Splunk to monitor AD-Svr's Event Log.

Part 4: Secure Layer 2 Switches

In Part 4 you will configure security settings on the indicated switch using the CLI. Configuration tasks include the following:

1. Assign and encrypt a privileged EXEC password.
   - Hostname: SW-1
   - Password: P@ssw0rd123
2. Add a user in the local database for administrator access
   - Username: Admin01
   - Privilege level: 15
   - Password: adminSkills54
3. Configure the MOTD banner.
   - Banner: Unauthorized Access is prohibited!
4. Configure Console login via Windows Radius authentication (use AD groups) with Local authentication as a backup.
5. Configure Telnet login (vty 0 – 4) via Radius authentication with Localauthentication as backup.
6. Configure IEEE 802.1x Port-based Network Access Control for Corporate users using Radius authentication

7. Configure basic port security.
    - Port: F0/18
    - Maximum limit: 1
    - Remember MAC Address
    - Violation Action: Shutdown
8. Assign and encrypt a privileged EXEC password.
    - Hostname: SW-2
    - Password: P@ssw0rd123
9. Configure VLAN 2 for the wireless network on SW-2.
10. Mirror incoming traffic from WS-ASA to SW-2, switch port 20.
11. Shutdown all unused ports on both SW-1 and SW-2.
12. Configure all switching devices to synchronize using NTP with authentication. Use an NTP password of NtpSkills54. WS-ASA must be set as the NTP master. Ensure the clocks are accurate on all devices.

DMZ zone

Part 5: CentOS-02 configuration

In part 5 you will be responsible for preparing the CentOS-02 server.

1. DNS

- Install Bind9.
- Configure a forward zone called “wsc2019.cloud”.
- Create for each host an A record to the respective IP
- Create a CNAME record for ‘www’ that points to the appropriate host that serves websites for all clients
- Create a CNAME record for ‘ftp’ that points to the ftp server
- Configure a reverse zone for the IP range defined in the DMZ network.

2. CA

- Configure as CA using OpenSSL.
- CA attributes should be set as follows:
    - Country code is set to RU
    - Organisation is set to WorldSkills RU
    - The common name is set to “WorldSkills 2019 CA”
- Create a root CA certificate.
- All certificates required in the Test Project should be published by CA.

3. Web server – Apache

- Install Apache
- Configure a HTTPS-only website for "www.wsc2019.cloud" domain
- Use certificate signed by root CA.
- Configure log files to capture Error and Access logs.
- Restrict access only for LDAP usernames.
- Configure a web application firewall to generate log messages and activate all base rules.

- Take necessary steps to harden the web server. Use the table below to answer it.

VULNERABILITIES	COUNTERMEASURES (INDICATE THE STEPS TAKEN CLEARLY)

4. LDAP

- Install the LDAP service.
- Configure the directory service of wsc2019.cloud.
- Create users with OU and password specified in the appendix.
- Create an OU named "CentOS-03" and use this to grant SSH access to "CentOS-03". User not in this group must be denied access. Root access must not be allowed.
- Create a new second domain "competition.Ru".
- In this domain create the users as stated in the appendix.

5. Wireless Access Point

Wireless Access Point WS-WAP is connected to WS-ASA via SW-2 to provide wireless client LIN-CLI-2 with access to the network. The WS-WAP 'Internet' interface is connected to VLAN 2 on SW-2, and the wireless network provides client addresses in the 192.168.2.0/24 network.

Default username: **admin**

Default password: **admin**

You are tasked with completing the following tasks on WS-WAP:

- Assign an IP address to the 'Internet' interface in accordance with the topology diagram.
- Configure DHCP for the wireless client, using an appropriate default gateway and starting the client pool at 192.168.2.50.
- Configure wireless mixed mode on channel 1(depending on local wireless channel allocations on the day), with a broadcast SSID of 'WS-WAP'
- Configure WPA 2 AES encryption, using a passphrase of 'wsruwap'. (exclude quotation mark)
- Configure administration settings to prevent wireless clients from accessing the GUI, and set the password to 'admin01w@p'
- Set up MAC filter for clients in the 192.168.2.0 network.
- Use radius server to authenticate WS-WAP clients (Free Radius server is hosted on CentOS-03).

Part 6: CentOS-03 configuration

In part 6 you will be responsible for preparing the CentOS-03 server.

1. FTP

- Setup FTP with vsFTPD
  - Use a virtual user configuration (not system users)
    - User: skill54-ftp / Password: FtpSkill54
    - Home directory: "/files/users/skill54-ftp"
  - The virtual user must be mapped to the system user/group "ftpuser/ftpgroup"
  - Per-user only one active concurrent session is allowed
  - Only allow explicit SSL / TLS (ftpes://)
  - File renaming is not allowed
  - Configure vsFTP a repository for CentOS
  - Take necessary steps to harden the FTP server. Use the table below to answer it.

VULNERABILITIES	COUNTERMEASURES (INDICATE THE STEPS TAKEN CLEARLY)

2. RADIUS (freeradius)

- Create 50 local UNIX users with password "RaSkills54"
  - Username: user[1-50]
  - These users should not be able to login locally
- Authenticate users against /etc/passwd file

3. SNORT

- Configure snort port to listen to DMZ network from SW-2 port 20.
- Write a snort rule to alert and log for any FTP traffic from an external network.
- Write a snort rule to alert and log for pings from any external network.
- Write a snort rule to alert and log for payload "malware" in content outside network from DMZ.

4. NTP Client

- Configure CentOS-03 to synchronize using NTP with authentication. Use an NTP password of NtpSkills54. WS-ASA must be set as the NTP master.

5. Proxy (Squid)

- Configure a reverse SSL proxy for www.wsc2019.cloud website, which is hosted by CentOS-02.

Part 7: Configure ASA Management and Firewall Settings

Note: By default, the privileged EXEC password is blank. Press Enter at the password prompt.

In Part 7, you will configure the ASA's setting and firewall using the CLI. Configuration tasks include the following:

1. Configure the ASA hostname.
   - Name: **WS-ASA**
2. Configure the domain name.
   - Domain Name: **wsc2019.cloud**
3. Configure the privileged EXEC password.
   - Password: P@ssw0rd123
4. Add a user to the local database for administrator console access.
   - User: Admin01
   - Password: adminSkills54
5. Configure AAA to use the local database for SSH user authentication for console access.
6. Configure interface G1/1
   - Name: outside
   - IP address: 209.165.200.226
   - Subnet Mask: 255.255.255.252
   - Security Level: 0
   - Activate the VLAN.
7. Configure interface G1/2
   - Name: inside
   - IP address: 192.168.10.1
   - Subnet Mask: 255.255.255.0
   - Security Level: 100
8. Configure interface G1/3
   - Name: DMZ
   - IP address: 192.168.2.1
   - Subnet Mask: 255.255.255.0
   - Security Level: 50

9. Generate an RSA key pair to support the SSH connections.
    - Key: RSA
    - Modulus size: 2048
10. Configure ASA to accept SSH connections from hosts on the inside LAN.
    - Inside Network: 192.168.10.0/24
    - Timeout: 15 minutes
    - Version: 2
11. Configure the default route.
    - Default route IP address: 209.165.200.225
12. Create a network object to identify internal addresses for PAT. Bind interfaces dynamically by using the interface address as the mapped IP.
    - Object name: INSIDE-NET
    - Subnet: 192.168.10.0/24
    - Interfaces: inside, outside
13. Modify the default global policy to allow returning ICMP traffic through the firewall.

Outside Zone

Part 8: CentOS-04 configuration

Install and configure the services:

- Configure routing on CentOS-04.
- Configure default routes on WS-ASA and R1.

Part 9: Configure Secure Router Administrative Access

In Part 9, you will secure administrative access on router R1 using the CLI. Configuration tasks include the following:

1. Set minimum password length.
    - Minimum Length: 10 characters
2. Configure the router to block logins for 75 seconds if 3 attempts are made within 30 seconds
3. Assign and encrypt a privileged EXEC password.
    - Password: P@ssw0rd123
4. Add a user in the local database for administrator access
5. Username: Admin01
    - Privilege level: 15
    - Password: AdminSkills54
6. Configure the MOTD banner.
    - Banner: Unauthorized Access is prohibited!

7. Configure SSH.
    - Domain name: wsc2019.cloud
    - RSA Keys size: 2048
    - Version: 2
    - Timeout: 90 seconds
    - Authentication retries: 2
8. Configure VTY 0-4 lines to allow only SSH access.

Part 10: Configure a Site-to-Site VPN

In Part 10, you will configure a Site-to-Site IPsec VPN between R1 and the ASA.

1. Configure a Site-to-Site IPsec VPN between R1 and the ASA according to the requirements.
2. Ping AD-Svr from the Outside client. This should generate interesting traffic and start site-to-site VPN.

Appendix A

LDAP Users

Username	OU	Password	Domain
user1	Web	LdSkill54	wsc19.cloud
user2	Web	LdSkill54	wsc19.cloud
user3	Web	LdSkill54	wsc19.cloud
user4	Web	LdSkill54	wsc19.cloud

AD-SVR

Setting	Value
IP	192.168.10.10/24

AD-SVR GROUPS/USERS

Details	group name	Username / password
Network Admin AD group	NetAdmin	WSNetAdmin / P@ssw0rd1
Corporate Users AD group	CorpUser	WSCorpUser /P@ssw0rd1

WIN-CLI

Setting	Value
IP	192.168.10.200/24

CentOS-01

Setting	Value
IP	192.168.10.11/24
Hostname	Centos-01.Russia.Local

CentOS-02

Setting	Value
IP	192.168.2.10/24
Hostname	Centos-02.wsc19.cloud

CentOS-03

Setting	Value
IP	192.168.2.11/24
Hostname	Centos-03.wsc19.cloud

CISCO 2960 SWITCH PARAMETERS (SW-1)

Setting	Value
Fa0/8, Fa0/24	Portfast
Dot1x Authentication Method	Radius
Fa0/24	Configure IEEE 802.1x authentication
Host Mode	Single host
VLAN 1 IP Address	192.168.10.100
Fa0/9	Connect to WIN-CLI
Fa0/10	Connect to LIN-CLI-1

CISCO 2960 SWITCH PARAMETERS (SW-2)

Setting	Value
Fa0/8, Fa0/24	Portfast
Fa0/16	Connect to WS-WPA
VLAN 2 IP Address	192.168.2.100

Radius Server Parameters

Setting	Value
IP Address / Subnet Mask	192.168.10.10 / 24
Radius Server Authentication Port	1812
Radius Server Accounting Port	1813
Radius Server Key	P@ssw0rd1

Windows 2016 Server Network Policy Server Parameters

Setting	Value
Radius Client	Friendly Name: SW-1 IP Address: 192.168.10.100 Shared Secret: P@ssw0rd1
WSSNetAdmin Network Policy	Connection Condition: Windows Netadmin group Authentication Method: Unencrypted authentication (PAP, SPAP)
WSSCorpUser Network Policy (IEEE 802.1x access)	802.1x Connection Type: Secure Wired (Ethernet) Connections Radius Client: 192.168.10.100 Radius Client Shared Secret: P@ssw0rd1 Authentication Method: Microsoft PEAP User Group: Windows CorpUser group

Appendix B