Skill 54 –

Cyber Security

State level Competition Test Project

Table of Contents

Section – A

Preface

Skill Explained:

A Cyber Security Professional works to protect an organization's computer systems networks, to ensure their robustness and prevent hackers from accessing and/or stealing sensitive information and data. The role typically involves configuring firewalls, IPS/IDS, server roles/services and web security solutions to protect confidential information.

A Cyber Security Professional also monitors security breaches and investigates violations. They may conduct penetration testing by simulating attacks to search for vulnerabilities in their networks before they can be exploited for malicious reasons. Their forensic tasks include gathering, preserving, processing, analyzing, and presenting computer-related evidence to mitigate networks' vulnerability to criminal, fraud, and other hostile activities. They have a range of tactics, techniques, and procedures, using a full range of investigative tools and processes.

A Cyber Security Professional usually also supports organizations' disaster recovery plans, which describes the steps and procedures to restore proper function of an organization's IT systems and networks after a disaster or attack. These are of paramount importance, financially, reputationally, and for the continuation of essential services. Plans normally include preventative measures such as regular backing up of and transfer of data to an offsite location.

In a fast-moving sector, Cyber Security Professionals must stay one step ahead of potential cyber-attackers. They must keep up with the latest methods attackers used to infiltrate computer systems, as well as with the new security technologies that can help organizations to counter these threats with robust systems and measures.

The Objective of the test project is that the competitor should be able to complete the assigned tasks in the below areas within ***4 hours*** of time.

- Windows Hardening
- IIS Hardening
- Application Code Analysis (Python)

Section – B

Test Project

Total Duration: 4 hours (240 minutes)
Total Marks: 20

Note:

- The activities listed in this test project is designed to be completed within 240 minutes.
- Assessment is best to the knowledge of the Jury based on the Marking Scheme.
- Not all tasks carry same weightage of marks. Based on the complexity and difficulty, the marks are assigned.
- There is no negative marks for wrong attempts.
- The task should be completed and the same has to be ensured that the systems are working after the activity.
- Partial completion of the tasks will not be considered for marking.

Module	Description	Max. Marks
A	Infrastructure Hardening (Windows & IIS)	10
B	Vulnerability Analysis	10

Description of the Tasks:

Infrastructure Hardening involves making configuration changes in various Operating Systems to improve the security posture and eliminate default insecure configurations. In this task, the participants are expected to make policy changes such as Password Policies, Lockout policies, and Audit Policies. They also need to update the default insecure configurations of various applications running on the systems to make them difficult to exploit. The participants would be required to harden both Windows and Linux Systems.

Vulnerability Assessment involves identifying and fixing security related weaknesses in the source code of various applications. The participants are expected to identify various instances of security flaws in the source code of the provided applications and write a secure version for the same.

Infrastructure List

To complete this test project, you will be provided with below components. These are sufficient enough to complete the activities listed in this test project.

Infrastructure Type	Description	Purpose
IT Hardware	Desktop / Laptop	For participants
IT Software	VMWare ESXi / Proxmox /Cloud	Hosting the TP platform for all participants
IT Software	Windows 2019 Server	Individual instance for every participant
IT Software	Windows 11	Individual instance for every participant

Module A: Infrastructure Hardening

Credentials:

S. No	Hostname	Operating System	Username	Password
1	Win_Server	Windows 2019 Server	Administrator	T35tPr0j3ct
2	Win_Client	Windows 11	Administrator	T35tPr0j3ct

- Competitors should not change the provided credentials. In case of the Jury not able to login to the competitor system with the provided credentials for evaluation, marks will not be awarded.

Windows Hardening

Task 1: [No marks for this task. This is mandatory and pre-requisite to complete the rest of the tasks]

- Configure the Windows 2019 Server as Active Directory with the Domain name "**Test_Domain.com**"
- Make the Windows 11 client (hostname: Win_Client) joined to the Active Directory

Task 2:

- Create a new group policy named "Security Policy for Test Project" and define below security configuration.
- Enforce the configured policy to the "Domain Users" group. Create an user named "Test_User" with credentials "T35tPr0j3ct" in the Active Directory, part of Domain Users.
- The below tasks will be validated both at Windows Server and Client systems.

○ **Password Policy**

Task No.	Policy	Configuration
2.1	Enforce Password History	5 passwords remembered
2.2	Maximum Password Age	45 days
2.3	Minimum Password age	3 days

2.4	Minimum Password Length	10 characters
2.5	Enforce Password Complexity	Enable
2.6	Implement the best practice for password storage	Enable

- **Account Policy**

Task No.	Policy
2.7	User account not to get unlocked automatically
2.8	User account should get locked out after 5 invalid password attempts
2.9	Account lockout reset counter to be set to 1 day

- **Audit Policy**

Task No.	Policy Configuration to be enabled
2.10	Audit Credential Validation
2.11	Audit Kerberos Authentication Services
2.12	Audit Kerberos Service Ticket Operations
2.13	Audit other account login events

- **Advanced Audit Policy [Logon / Logoff]**

Task No.	Policy	Configuration
2.14	Audit Account Lockout	Success, Failure
2.15	Audit Group Membership	Success, Failure
2.16	Audit IPSEC Extended Mode	Success, Failure
2.17	Audit IPSEC Main Mode	Success, Failure
2.18	Audit IPSEC Quick Mode	Success, Failure
2.19	Audit Logoff	Success, Failure
2.20	Audit Logon	Success, Failure
2.21	Audit Logon	Success, Failure
2.22	Audit Network Policy Server	Success, Failure
2.23	Audit Other Logon/Logoff Events	Success, Failure
2.24	Audit Special Logon	Success, Failure
2.25	Audit User / Device Claims	Success, Failure

- **Advanced Audit Policy [Object Access]**

Task No.	Policy	Configuration
2.26	Audit Application Generated	Failure
2.26	Audit Certification Services	Failure
2.27	Audit Detailed File Share	Failure
2.28	Audit File System	Failure
2.29	Audit Filtering Platform Connection	Failure
2.30	Audit Filtering Platform Packet Drop	Failure
2.31	Audit Handle Manipulation	Failure
2.32	Audit Kernel Object	Failure

2.33	Audit other object access events	Failure
2.34	Audit Registry	Failure
2.35	Audit Removable Storage	Failure
2.36	Audit SAM	Failure
2.37	Audit Central Access Policy Staging	Failure

- **Advanced Audit Policy [Policy Change]**

Task No.	Policy	Configuration
2.38	Audit Policy Change	Success, Failure
2.39	Audit Authentication Policy Change	Success, Failure
2.40	Audit Authorization Policy Change	Success, Failure
2.41	Audit Filtering Platform Policy Change	Success, Failure
2.42	Audit MPSSVC Rule-level Policy change	Success, Failure
2.43	Audit other policy change events	Success, Failure

- **Advanced Audit Policy [Privilege Use]**

Task No.	Policy	Configuration
2.44	Audit Non sensitive privilege use	Success, Failure
2.45	Audit other privilege use events	Success, Failure
2.46	Audit sensitive privilege use	Success, Failure

- **Advanced Audit Policy [System]**

Task No.	Policy	Configuration
2.47	Audit IPSEC Driver	Success, Failure
2.48	Audit Other System Events	Success, Failure
2.49	Audit Security State Change	Success, Failure
2.50	Audit Security System Extension	Success, Failure
2.51	Audit System Integrity	Success, Failure

- **Advanced Audit Policy [Global Object Access Auditing]**

Task No.	Policy	Configuration
2.52	File System	Failure
2.53	Registry	Failure

- **User Rights Assignment**

Task No.	Policy Configuration to be configured
2.54	Ensure only Administrators and Authenticated Users group are authorized to logon to the computer in the network
2.55	Restrict the system time and time zone change privilege only to the Administrators group & Local Service
2.56	Guests user account should not be allowed to login to the system

2.57	Allow only Administrators and Remote Desktop Users to logon remotely (interactive logon)
2.58	Allow Administrators and Power Users to force shutdown remotely
2.59	Enable auditing and security log management for Administrators and Power Users
2.60	Administrators alone should have the privilege for taking ownership of the files or other objects

- **Security Options**

Task No.	Policy Configuration to be configured
2.61	Disabling USB Storage Devices access
2.62	Not to display logged on user information either when locked
2.63	Not to display logged on user information either when logged off
2.64	Enable Interactive Logon: Machine inactivity limit to 10 minutes
2.65	Ensure to prompt for credentials for User Account control: Behavior of the elevation prompt for standard users.

- **Miscelleneous**

Task No.	Policy Configuration to be configured
2.66	Disable "NetBIOS over TCP/IP"
2.67	Disable POSIX subsystem
2.68	Disable SMB v1 support
2.69	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
2.70	Disable Multicast Name resolution

Sub-Task 1: [No marks for this task. This is mandatory task to complete the next set of tasks]

- Install IIS Web Server on Windows Server 2019 and configure all the roles and features required for the webserver

Sub-Task 2:

- Harden the IIS Web Server as per below listed tasks
- Remove unused script mappings

Task No.	Configuration setting	File extension to be removed
2.71	Web-based password reset	.htr
2.72	Internet database connector	.idc
2.73	Server side includes	.stm, .shtm and .shtml
2.74	Internet Printing	.printer
2.75	Index Server	.htw, .ida and .idq
2.76	Compound index	.cdx

- Miscellaneous

Task No.	Configuration setting
2.77	Remove Internet Printing
2.78	Remove Parent Path
2.79	Map the IIS logs to D:\WebLogs\
2.80	Restrict internet facing interfaces only to port 80 and 443
2.81	Disable TRACE method
2.82	Disable Debug Compilation
2.83	Enable Request Filtering
2.84	Disable URL Rewriting
2.85	Avoid disclosure of Internal IP Disclosure
2.86	Configure Force redirection of http to https
2.87	Configure httpOnlyCookies value to true for the default site
2.88	Configure requireSSL value to true for the default site
2.89	Enforce Strict Transport Security and set the maximum age to 1 day
2.90	Harden the web server to suppress the web server header information while remote fingerprinting

- Configure below on the IIS webserver

Task No.	Server Level Setting
2.91	Create a new site in IIS and map the web directory to folder D:\Web_Server\ and create a sample html file
2.92	Map the created html file as a default web page
2.93	Configure the website access only on port 443 (https). If it is accessed over port 80 (http), it should automatically redirect to port 443 (https)
2.94	Enable Web Server logging
2.95	Enable TLS 1.2 and disable TLS 1.1,TLS 1.0, SSL 3.0, SSL 2.0

Module B: Vulnerability Analysis

Task 3:

1. **Python Code:**

```
def search_books(user_query):
    book_list = eval("BookDatabase.search(\"" + user_query + "\")")
    return book_list

user_input = input("Enter your book search query: ")
results = search_books(user_input)
print("Search results:", results)
```

Task No.	Question
3.1	What type of vulnerability is present in the code snippet?
3.2	For the code snippet available above, based on the vulnerability, explain why it is vulnerable.
3.3	Recommend how the vulnerability shall be fixed.
3.4	Best practices on handling this vulnerability

2. Analyze the below code and answer the following questions.

```
public void doFilter(ServletRequest request, ServletResponse response, FilterChain chain) {
      (...)
            httpRequest = (HttpServletRequest)request;
            logger.debug("doFilter url: " + httpRequest.getRequestURL().toString());
            boolean isAuthenticated = this.authenticateUser(httpRequest);
              ^^^ 1.5) invokes authenticateUser() (function shown below)

            String samlLogoutRequest;
            if(!isAuthenticated) {
              ^^^ 1.6) if authenticateUser() returns false, we go into this branch

                samlLogoutRequest = request.getParameter("SAMLResponse");
                logger.info("samlResponse-->" + samlLogoutRequest);
                if(samlLogoutRequest != null) {
                    this.handleSAMLReponse(request, response, chain, samlLogoutRequest);
                } else {
                  ^^^ 1.7) if there is no SAMLResponse HTTP parameter, we go into this branch

                    HttpSession session;
                    ProductAccess userBean;
                    String requestedUri;
                    if(this.isStarshipRequest(httpRequest)) {
                      ^^^ 1.8) checks if isStarshipRequest() returns true (function shown below)

                        session = null !=
httpRequest.getSession(false)?httpRequest.getSession(false):httpRequest.getSession(true);
                        userBean = (ProductAccess)session.getAttribute("USER_IN_SESSION");
                        if(userBean == null) {
                          ^^^ 1.9) if there is no session server side for this request, follow into this
branch...

                            try {
                                userBean = new ProductAccess();
                                userBean.setCredentialId("");
                                userBean.setAdminPasswordReset(true);
                                userBean.setProductId("cloupia_service_portal");
                                userBean.setProfileId(0);
                                userBean.setRestKey(httpRequest.getHeader("X-Starship-Request-Key"));
                                userBean.setStarshipUserId(httpRequest.getHeader("X-Starship-UserName-
Key"));

                                userBean.setLoginName("admin");
                                  ^^^ 1.10) and create a new session with the user as "admin"!

                                userBean.setStarshipSessionId(httpRequest.getHeader("X-Starship-
UserSession-Key"));

                                requestedUri = httpRequest.getHeader("X-Starship-UserRoles-Key");
                                userBean.setAccessLevel(requestedUri);
                                if(requestedUri != null && requestedUri.equalsIgnoreCase("admin")) {
                                    AuthenticationManager authmgr = AuthenticationManager.getInstance();
                                    userBean.setAccessLevel("Admin");
                                    authmgr.evaluateAllowedOperations(userBean);
                                }

                                session.setAttribute("USER_IN_SESSION", userBean);
                                session.setAttribute("DEFAULT_URL", STARSHIP_DEFAULT_URL);
                                logger.info("userBean:" + userBean.getAccessLevel());
                            } catch (Exception var12) {
                                logger.info("username/password wrong for rest api access - " +
var12.getMessage());
                            }

                            logger.info("userBean: " + userBean.getAccessLevel());
                        }

                        chain.doFilter(request, response);
```

Task No.	Question
3.5	What type of vulnerability is present in the code snippet?
3.6	For the code snippet available above, based on the vulnerability, explain why it is vulnerable.
3.7	Recommend how the vulnerability shall be fixed.
3.8	Best practices on handling this vulnerability

- Miscellaneous

Task No.	Question
3.9	What is the nmap command for operating system and service fingerprinting?
3.10	For the code snippet available above, based on the vulnerability, explain why it is vulnerable.

Section – C

Marking Scheme

The Assessment is done by awarding points by adopting two methods, Measurement and Judgments.

○ Measurements	-	One which is measurable
○ Judgements	-	Based on Industry Expectations

Measurements:

- Used to assess accuracy, precision, and other performance which can be measured in unambiguous way. Mark is awarded in full for a dimension with in tolerance and zero when it is out of tolerance.

Judgement

- Used to assess the quality of performance, about which there may be small differences of opinion.

Section - D

Infrastructure List

Infrastructure Type	Description	Purpose
IT Hardware	Desktop / Laptop	For participants
IT Software	VMWare ESXi / Proxmox	Hosting the TP platform for all participants
IT Software	Windows 2019 Server	Individual instance for every participant
IT Software	Windows 11	Individual instance for every participant

Section - E

Instructions to the candidates

Total Duration: 4 hours (240 minutes)
Total Marks: 20

Note:

- The activities listed in this test project is designed to be completed within 240 minutes.
- Assessment is best to the knowledge of the Jury based on the Marking Scheme.
- Not all tasks carry same weightage of marks. Based on the complexity and difficulty, the marks are assigned.
- There is no negative marks for wrong attempts.
- The task should be completed and the same has to be ensured that the systems are working after the activity.
- Partial completion of the tasks will not be considered for marking.

Module	Description	No. of tasks (A)	Marks for each task (B)	Max. Marks (A x B)
A	Infrastructure Hardening (Windows & IIS) – (Task 2.1 – 2.90)	90	0.1	9
A	Infrastructure Hardening (IIS) (Task 2.91 – 2.95)	5	0.2	1
B	Vulnerability Analysis	10	1	10
Total				**20**

Section - F

Health. Safety and Environment

- All accredited participants, and supporting volunteers will abide by rules and regulations with regards to Health, Safety, and Environment of the Competition venue.
- All participants, technicians and supporting staff will wear the required protective Personnel clothing. The Competitors must wear proper dress suiting the task and wear goggles while performing.
- All participants will assume liability for all risks of injury and damage to property, loss of property, which might be associated with or result from participation in the event. The organizers will not be liable for any damage, however in case of Injury the competitor will immediately inform the immediate organizer for medical attention.
- Proper ventilation in the work place
- Running water should be near to work plac