Cyberyami CPTP Certification Exam Objectives

CYBERYAMI

About the Certification

The Cyberyami Certified Penetration Testing Professional (CCPTP) is a globally recognized and vendor-neutral certification designed to validate the skills necessary for effective and professional penetration testing. CCPTP ensures that individuals understand and can apply a systematic and thorough approach to penetration testing, ensuring a methodical and effective assessment. Successful candidates will be able to gather relevant information and perform reconnaissance to identify potential vulnerabilities and weaknesses in a target system or network.

Skills You Learn

Advanced Penetration Testing Skills: Successful candidates will acquire expertise in assessing and enhancing the security of systems and networks.

Comprehensive Understanding of Methodologies: Candidates will learn systematic and organized approaches to penetration testing for increased effectiveness.

Proficient Information Gathering Techniques: The certification hones skills in collecting and analyzing crucial data for identifying vulnerabilities.

Effective Vulnerability Assessment and Exploitation: Gain hands-on experience in assessing and ethically exploiting vulnerabilities.

Professional Reporting and Documentation Skills: Candidates master the creation of clear and detailed reports for effective communication of findings.

Ethical Hacking and Responsible Conduct: The CCPTP emphasizes ethical hacking principles, ensuring graduates conduct assessments responsibly and within legal boundaries.

CYBERYAMI

Pre-Requisites:

Networking and Cybersecurity Knowledge: A strong understanding of networking concepts and cybersecurity principles is essential.

Operating Systems and Programming Skills: Proficiency in Linux and Windows, coupled with basic programming and scripting abilities, is recommended.

Web Technologies and Security Tools: A grasp of web technologies and familiarity with security tools like Nmap and Metasploit is advantageous.

Practical Experience: While specific requirements may vary, practical experience in cybersecurity roles enhances exam readiness.

Target Audience:

The CCPTP certification is ideal for aspiring and experienced cybersecurity professionals, including ethical hackers, penetration testers, security analysts, and network administrators. It caters to individuals seeking to validate and enhance their skills in conducting thorough and effective penetration tests across various systems and networks.

Target Job Roles:

Completing the CCPTP certification opens doors to a range of cybersecurity roles, including:

Penetration Tester: Conduct security assessments to identify and address vulnerabilities in systems, networks, and applications.

Ethical Hacker: Employ ethical hacking techniques to proactively assess and improve the security posture of organizations.

Target Job Roles:

Security Analyst: Analyze and respond to security incidents, monitoring and safeguarding against potential threats.

Security Consultant: Provide expert advice on security measures, conduct risk assessments, and assist in developing robust security strategies.

Network Security Engineer: Design, implement, and manage security measures for networks to protect against unauthorized access and cyber threats.

Information Security Manager: Oversee and manage an organization's overall information security program, ensuring compliance and risk mitigation.

Incident Responder: Investigate and respond to security incidents, minimizing the impact and preventing future occurrences.

Security Engineer: Design and implement security solutions, including firewalls, encryption, and other protective measures.

IT Auditor: Assess and evaluate the effectiveness of an organization's information systems and security controls.

System Administrator: Administer and secure computer systems, ensuring their proper functioning and protection against potential threats.

Exam Details:

EXAM CODE	PT101
Launch Date	15 October 2023
Number of Questions	100
Length of Test	140 Mintues
Types of Questions	Multiple choice & Case based questions
Passing Score	72%
Testing Provider	CyberYami Levelup Online
Language	English

CYBERYAMI

Exam Domain:

TOPICS	WEIGHTAGE (IN PERCENTAGE)
VAPT Planning and Scoping	5%
Reconnaissance and Enumeration	10%
Vulnerability Assessment and Scanning	15%
Exploitation and Post-Exploitation	20%
Web Application Security	15%
Wireless Security	15%
Cloud Security	15%
Documentation & Reporting	5%

1.0 VAPT Planning and Scoping

1.1 Rules of Engagement

- Rules of Engagement
- Ethical Conduct
- Testing Objectives
- Scope Definition
- Limitations
- Authorization and Consent
- Communication Protocols
- Reporting Procedures
- Data Confidentiality
- Impact Mitigation
- Legal Compliance
- Contingency Plans
- Professionalism

1.2 Compliance Planning

- Compliance obligations
- Information security
- Data protection
- Legal requirements
- Regulatory compliance
- Contractual obligations
- Industry-specific standards
- Privacy and confidentiality
- Collaboration with legal teams
- Consent and authorization
- Scope alignment
- Risk management
- Reporting
- Confidentiality
- Data protection laws
- Security vulnerabilities
- Cybersecurity practices
- Sensitive information

2.0 Reconnaissance and Enumeration

2.1 Recon Techniques

- Internet protocol
- Domain names
- IP addresses
- Autonomous system numbers (ASNs)
- Registration details
- Ownership information
- Contact details
- Administrative information
- Domain Name Lookup
- IP Address Lookup
- Ownership and Contact Information
- Administrative and Technical Contacts
- Registrar and Name Server Information
- Domain Status and Expiration
- Domain registration
- Cybersecurity
- Network administration
- Law enforcement
- Intellectual property rights
- Research and analysis
- Compliance
- DNS Recon

- DNS infrastructure
- DNS Zone Transfers
- DNS Enumeration
- Reverse DNS Lookup
- DNS Brute Forcing
- DNS Cache Snooping
- Subdomain Enumeration
- Dig
- Recon-ng
- Nslookup

3.0 Vulnerability Assessment and Scanning

3.1 Network Scanning

- Nmap
- Network Mapper
- Open-source
- Network scanning
- Vulnerabilities
- Port scanning
- Service detection
- Operating system detection
- Scripting engine
- Stealth scanning
- Output formats
- Integration
- Cross-platform support
- Security auditing
- Network monitoring
- System administration
- Metasploitable-2
- Host discovery

3.2 Vulnerability Scanning with Nessus

- Vulnerability Assessment
- Tenable
- Plugin Architecture
- CVE and OVAL Databases
- Customizable Scans
- Compliance Auditing
- Agentless Architecture
- Scheduled Scans
- Results Analysis
- Integration and APIs
- Security Updates
- Authorized Scanning

- Vulnerability Scanning
- Installation Steps
- Activation Code
- Policies
- Scan Templates
- HTML Report
- Detailed Scan Report

3.3 Vulnerability Scanning with Zap Proxy

- OWASP ZAP
- Web Application Security
- Security Tool
- Open Source
- Vulnerability Assessment
- Intercepting Proxy
- Automated Scanning
- Manual Testing
- Spidering and Fuzzer
- Reporting
- Scripting and Automation
- Installation Steps
- Configuration
- Target Configuration
- Java SE Runtime Environment
- Desktop UI
- Automated Scan
- Manual Explore
- Alert Tab
- Scope Tab

3.4 Service Enumeration

- Network File System
- Security assessments
- Network configurations
- Showmount
- Nmap
- NFS clients
- Metasploit
- Enum4linux
- RPCScan
- Hydra
- Medusa
- Nessus
- Windows Server
- Kali machine
- Port 2049
- FTP (File Transfer Protocol)
- FTP server
- Directory structure
- Permissions
- Manual enumeration
- Anonymous login
- Banner grabbing
- FTP Nmap scripts
- Metasploit Framework
- FTP client commands
- Firewall
- SMB enumeration
- Null session enumeration

4.0 Exploitation and Post-Exploitation

4.1 Exploitation of FTP Service

- Active FTP
- Passive FTP
- Encryption
- Security
- Vulnerabilities
- Anonymous Access
- Brute Force Attacks
- Hydra
- Weak Passwords
- Information Leakage
- Data Protection
- Security Cameras
- FTP Server
- Packet Capture
- Wireshark
- Anonymous Login
- Enumeration
- File Tampering

4.2 Exploitation of NFS Service

- Exploit
- Mounting
- Network File System
- File Sharing
- Centralized Storage
- Enumeration Process
- Nmap Script Engine
- Shared Folder
- Mount Command
- Privilege Escalation
- SSH
- .ssh Directory
- Private Keys
- id_rsa
- Root Squash
- SUID
- Set User ID
- File Permissions
- Bash Shell Executable

4.3 Exploitation of SMB Service

- CVE-2017-7494
- Samba
- Vulnerability
- Unauthorized Access
- Data Breaches
- System Compromise
- Mounting
- Command Prompt
- smbclient
- SMBv1 Exploits
- EternalBlue
- Nmap Script Engine
- Remote Code Execution
- Metasploit Framework
- SMB Relay Attack
- Port 445

4.4 Exploitation of Telnet Service

- Unencrypted Data Transmission
- Wireshark
- Data Interception
- Encrypted Transmission
- Follow TCP Stream
- /etc/passwd Command
- Default Credentials
- Hydra
- Brute Force Attacks
- Banner Grabbing
- Telnet Banners
- System Information
- Operating System
- Telnet-NTLM-Info
- Command Injection
- Input Fields
- Malicious Commands

4.5 Privilege Escalation

- Privilege escalation
- Evil-winrm
- WinRM (Windows Remote Management) protocol
- PowerShell
- Enumeration
- PowerUp
- PowerSploit
- Windows-Exploit-Suggester
- Seatbelt
- Sherlock
- JAWS
- winPEAS
- SharpUp
- Dual-homed
- ARP (Address Resolution Protocol) table
- MAC (Media Access Control) address
- Sudo privileges
- sudo -l command
- /etc/sudoers configuration file

- NOPASSWD option
- User privileges
- sudoers file
- /usr/bin/su command
- Shell access
- Unauthorized access
- gtfobins
- sudo su - root
- Escalate privileges
- Switch user
- Configuration option
- PATH variable
- Executable files
- Absolute path

5.0 Exploitation and Post-Exploitation

5.1 File Upload Vulnerability

- File Upload Vulnerability
- Unrestricted File Upload
- Security Weakness
- Web Application
- Malicious Files
- Remote Code Execution (RCE)
- Web Shell Upload
- Denial of Service (DoS)
- Malicious File Distribution
- File Content Manipulation
- Mitigation
- File Type Validation
- Content Validation
- Secure File Permissions
- File Size and Quantity Restriction
- Disable Execution
- Content Security Policy (CSP)

5.2 SQL Injection Vulnerability

- Web application
- Database
- Structured Query Language
- Input validation
- Malicious actors
- Unauthorized access
- Data manipulation
- Security vulnerability

Prepared statements
Parameterized queries
Input sanitization
In-Band SQL Injection
Blind SQL Injection
Out-of-Band SQL Injection
SQLmap

5.3 Cross-Site Scripting Vulnerability

- Malicious scripts
- JavaScript
- Stored XSS (Persistent XSS)
- Reflected XSS (Non-Persistent XSS)
- DOM-based XSS
- Metasploitable2
- Vulnerable machine
- DVWA (Damn Vulnerable Web Application)

- Security settings
- High to Low security
- Name and Message section
- XSS payload
- Script injection
- Pop-up
- Payload execution
- Session cookies
- Session Hijacking

5.4 Command Injection Vulnerability

- Shell Injection
- Arbitrary operating system commands
- Inadequate input validation
- Improper handling of user-supplied data
- User input
- Insufficient validation
- Sanitize
- Exploitation
- Special characters
- Command execution
- Unauthorized access

- Data exfiltration
- Parameterized queries
- Prepared statements
- Least privilege
- Avoid shell execution
- Vulnerable machine
- DVWA (Damn Vulnerable Web Application)
- High to Low security
- IP address
- Ping

- Source code
- Unix/Linux
- Semicolon (;)
- Filtering

- Linux commands
- 'pwd'
- 'whoami'
- 'id'

6.0 Exploitation and Post-Exploitation

6.1 Wireless Penetration Testing

- Internet connectivity
- Radio signals
- Security protocols
- WPA (Wi-Fi Protected Access)
- WPA2 (Wi-Fi Protected Access 2)
- Temporal Key Integrity Protocol (TKIP)
- Extensible Authentication Protocol (EAP)
- Dynamic encryption keys
- Advanced Encryption Standard (AES)
- Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP)
- Exploitable vulnerabilities
- KRACK (Key Reinstallation Attack)
- Brute force attacks
- Rogue access points
- Man-in-the-middle attacks
- Evil Twin attacks
- Password cracking
- WPA3 (Wi-Fi Protected Access 3)
- Virtual Machine
- Wireless adapter
- Kali Linux
- Virtual Box
- USB port
- Port alert
- Security configuration
- iwconfig
- ifconfig
- Airmon-ng

7.0 Cloud Security

7.1 Cloud Penetration Testing Methodology

- Cloud Service Providers
- Security Problems
- Cloud Applications
- Security Posture
- Attack Vectors
- Security Misconfigurations
- Vulnerable Components
- Outdated Components
- Broken Authentication
- Cryptographic Failures
- Insufficient Logging
- Access Control
- Cross-Site Scripting
- Injection Attacks
- Insecure Design
- Data Integrity Failures

7.2 Cloud Penetration Testing Tools

- WeirdAAL
- AWS Attack Library
- ScoutSuite
- Multi-cloud Security Auditing
- GitOops
- GitHub Organization Security
- Lateral Movement
- Privilege Escalation
- Pacu
- BAWS Exploitation Framework
- Offensive Security Testing
- Configuration Flaws
- IAM Users
- Lambda Functions
- CI/CD Pipelines
- Security Tools Installation
- Cloud Environment

7.3 Cloud Penetration Testing Tools

- Pacu
- AWS Account
- Terminal
- Session
- Modules
- IAM User
- Penetration Testing
- GitHub
- Open Source
- Spencer Gietzen
- Rhino Security Labs
- Access Keys
- Kali Linux
- AWS CLI
- IAM Role
- Console
- EC2
- Reconnaissance
- Exploitation
- Security Groups

8.0 Documentation & Reporting

8.1 Proof of Concept

- Creating effective proof of concept documents
- POC documentation standards
- Visual representation in POC
- Networks
- Techniques
- Report Writing
- Findings
- Vulnerabilities
- Recommendations
- Risk Assessment
- Methodology
- Executive Summary
- Exploitation
- Proof of Concept
- Remediation
- Scope
- Objectives
- Network Security
- System Configuration
- Documentation
- Business Impact
- Technical Details
- Conclusion

8.1 Proof of Concept

- Creating effective proof of concept documents
- POC documentation standards
- Visual representation in POC
- Networks
- Techniques
- Report Writing
- Findings
- Vulnerabilities
- Recommendations
- Risk Assessment
- Methodology
- Executive Summary
- Exploitation
- Proof of Concept
- Remediation
- Scope
- Objectives
- Network Security
- System Configuration
- Documentation
- Business Impact
- Technical Details
- Conclusion

Tools that you will learn

- Metaspoilt
- Nmap
- Nessus
- Zap Proxy
- Curl
- WinSCP
- Hydra
- SMBclient
- SQLmap