Hewlett Packard
Enterprise

HPE Digital Learner CompTIA - CySA +PenT Content Pack

HPE Content Pack number	CP033
Content Pack length	22 Hours
Content Pack category	Category 2
Learn more	**View now**

Why HPE Education Services?

- IDC MarketScape leader 5 years running for IT education and training*
- Recognized by IDC for leading with global coverage, unmatched technical expertise, and targeted education consulting services*
- Key partnerships with industry leaders OpenStack®, VMware®, Linux®, Microsoft®, ITIL, PMI, CSA, and SUSE
- Complete continuum of training delivery options—self-paced eLearning, custom education consulting, traditional classroom, video on-demand instruction, live virtual instructor-led with hands-on lab, dedicated onsite training
- Simplified purchase option with HPE Training Credits

Courses are independent of each other but combined provide proof of advanced capabilities

CySA+ certification covers advanced persistent threats in a cybersecurity environment
Pentest+ certification for penetration testing and vulnerability management.

Supplementing this programme with additional material prior to sitting an exam is recommended

Audience

These courses extend the skills and competency of the security professional focusing on analysis and prevention in the protection of the enterprise.

CySA+

For security professionals looking to consolidate and extend existing security knowledge to incorporate cyber security into the design and implementation of software and software products

PenTest+

For security professionals who wish to extend their existing knowledge in order to

- Obtain the management skills used to plan, scope, and manage weaknesses, not just exploit them
- Demonstrate a hands-on capability and knowledge to test devices (in addition to traditional desktops and servers) within new environments such as the cloud and mobile

Content Pack Objectives

- To provide confirmation of the capability and competency of an individual in the security and cyber security domains
- To demonstrate practical and hands-on solutions-based capability of an individual, based on current technology, to support the integrity of the enterprise

*Realize Technology Value with Training, IDC Infographic 2037, Sponsored by HPE, October 2017

Detailed Content Pack outline

CompTIA Cybersecurity Analyst+ CS0-001: Network Architecture and Reconnaissance

- Map network hardware and software to the OSI model
- Identify when to use specific network hardware
- Understand IPv4 settings
- Understand IPv6 settings
- Understand transport protocols
- Understand which Windows tools to use when configuring and troubleshooting TCP/IP
- Understand which Linux tools to use when configuring and troubleshooting TCP/IP
- Configure and scan for service ports
- Configure network services securely
- Explain common wired and wireless network concepts
- Scan for wireless networks and understand the returned results
- Determine placement of network devices
- Explain the purpose of cloud computing
- Recognize the use of cloud service models
- Recognize the role of virtualization in cloud computing
- Identify cloud security options
- Explain how to discover network devices
- Use logs to learn about the network environment
- Use packet capturing tools for network traffic analysis
- Capture and interpret FTP and HTTP traffic
- Discover network configurations
- Explain harvesting techniques
- Recognize social engineering techniques
- Identify details within acceptable use policies
- Identify details within data ownership and retention policies
- Identify details within data classification policies
- Identify details within a password policy
- Recognize various network configurations and perform network reconnaissance

CompTIA Cybersecurity Analyst+ CS0-001: Threat Identification

- Identify assets and related threats
- Recognize known, unknown persistent, and zero-day threats
- Identify what constitutes PII
- Explain payment card data
- Identify intellectual property
- Control how valuable data is used
- Configure group policy to prevent data leakage
- Determine the effect of negative incidents
- Identify stakeholders related to incident response
- Recognize incident response roles
- Describe incident disclosure options
- Analyze host symptoms to determine the best response
- Analyze network symptoms to determine the best response
- Analyze application symptoms to determine the best response
- Contain negative incidents
- Thoroughly remove data
- Identify positive learned outcomes resulting from incidents
- Identify how OEM documentation can be used to reverse engineering products
- Recognize the relevance of up-to-date network documentation
- Recognize the ongoing maintenance of incident response plans
- Create proper incident forms
- Protect the integrity of collected evidence
- Implement changes to processes resulting from lessons learned
- Determine which type of report provides the best data for a specific situation
- Determine if SLA details are aligned with business needs
- Explain the purpose of a MOU
- Use existing inventory to drive decisions related to security
- Recognize threat impact and design an incident response plan

CompTIA Cybersecurity Analyst+ CS0-001: Threat Mitigation

- Identify SDLC phases
- Apply secure coding practices
- Properly test technology solutions for security
- Reduce the attack surface of a network host
- Recognize the importance of keeping hardware and software up to date
- Apply patches properly to secure network hosts
- Set the correct access to file systems while adhering to the principle of least privilege
- Recognize the purpose of controlling network access with NAC
- Recognize the purpose of network segregation using VLANs
- Identify various conditions that control access to resources
- Recognize the purpose of intentionally creating vulnerable hosts to monitor malicious use
- Recognize the purpose of a jump box
- Explain how proper IT governance results in secured IT resources
- Recognize how regulatory compliance can influence security controls
- Apply NIST's Cybersecurity Framework to your digital assets
- Apply ISO security standards to harden your environment
- Recognize how the TOGAF enterprise IT architecture can increase efficiency of security controls
- Recognize how to assess risk and apply effective security controls to mitigate that risk
- Recognize how to apply ITIL to increase the efficiency of IT service delivery
- Identify physical security controls
- Identify logical security controls
- Configure router ACL rules to block ICMP traffic
- Identify administrative security controls
- Identify compensating security controls
- Recognize the importance of continuous monitoring
- Explain how firmware must be accredited before universal trust is established
- Identify factors related to conducting penetration tests
- List categories of security controls and threat mitigations

CompTIA Cybersecurity Analyst+ CS0-001: Reducing Vulnerabilities

- Recognize how crypto is used to secure data in the enterprise
- Differentiate symmetric from asymmetric encryption
- Differentiate asymmetric from symmetric encryption
- Identify the PKI hierarchy
- Request a security certificate from a CA
- Encrypt files on a Windows system using EFS
- Explain how file integrity can be maintained
- Enable file integrity using Linux
- Enable file integrity using Windows
- Recognize authentication methods used to prove one's identity
- Require VPN connections to use MFA
- Recognize how resource access gets authorized
- Configure centralized authentication using RADIUS
- Describe what user provisioning entails
- Describe how identity federation differs from traditional authentication
- Identify security weaknesses in server OSs
- Identify security weaknesses on endpoint devices
- Identify security weaknesses at the network level
- Identify security weaknesses on mobile devices
- Recognize the overall process of scanning for vulnerabilities
- Configure appropriate vulnerability scanning settings
- Explain how the SCAP standard is used to measure vulnerability issues and compliance
- Conduct a vulnerability scan using Nessus
- Distinguish various vulnerability scanning tools from one another
- Conduct a vulnerability scan using MBSA
- Understand vulnerability scan results
- Put controls in place to mitigate threats
- Reduce vulnerabilities that can be exploited

CompTIA Cybersecurity Analyst+ CS0-001: Investigate Security Incidents

- Recognize the purpose of various firewall types
- Recognize how firewall rules are created based on what type of traffic should or should not be allowed
- Recognize how packet filters work
- Configure a packet filtering firewall
- Explain the purpose of a proxy server
- Explain the purpose of a security appliance
- Recognize the unique capabilities of web application firewalls
- Explain the importance of intrusion detection and prevention
- Recognize when to use HIDS
- Recognize when to use NIDS
- Recognize when to use NIPS
- Identify different types of malware
- Identify viruses
- Identify worms
- Identity spyware and adware
- Explain how ransomware works
- Mitigate malware using antimalware solutions
- Explain why user training and awareness is one of the most important security defenses
- IDescribe digital forensics
- Determine which forensic hardware is best suited for a specific situation
- Determine which forensic software is best suited for a specific situation
- Explain how forensic tools can be used against data stored on media
- Distinguish common forensic tools from one another
- Explain the sequence of steps that should be followed when conducting mobile device forensics
- Create a memory dump
- Retrieve and view deleted files
- Prevent threat materialization and follow proper forensic procedures

CompTIA Cybersecurity Analyst+ CS0-001: Monitoring for Security Issues

- Recognize proper hiring practices
- Provision new user accounts in accordance with organizational security policies
- Apply personnel management best practices
- Distinguish the difference between threats, vulnerabilities, and exploits
- Explain the concept of spoofing
- Craft forged packets using free tools
- Recognize how impersonation can be used to gain unauthorized access
- Recognize CSS attacks
- Recognize root kits
- Explain the concept of privilege escalation
- Distinguish the difference between common exploit tools
- Use Metasploit tools to further understand the attacker toolset
- Use Kali Linux tools to further understand the attacker toolset
- Crack passwords
- Recognize the importance of continuous monitoring of various systems
- Distinguish the difference between common monitoring tools
- Monitor the Linux OS
- Monitor the Windows OS
- Configure Windows event log forwarding
- Identify where SIEM is used
- Identify where SCADA and ICS are used in different industries
- View network utilization
- Analyze timestamped data from various sources
- Identify trends in network usage
- Identify events from specific types of logs
- Describe the difference between vulnerabilities and exploits as well as use various reporting tools

CompTIA PenTest+: Planning for an Engagement

- Describe the need for penetration testers
- Explain the CompTIA PenTest+ exam
- Understand your audience and rules of engagement
- Compare resources, requirements, and budgets
- Define impact analysis and remediation timelines
- Describe disclaimers and technical constraints
- Examine engagement support resources
- Examine pertinent contracts and agreements
- Evaluate environmental differences
- Obtain written authorization
- Describe engagement

CompTIA PenTest+: Scoping an Engagement

- Compare types of assessments
- Define special scoping factors
- Select targets
- Strategize scoping
- Explain risk acceptance and impact tolerance
- Describe scheduling and scope creep
- Explain threat actors and threat agents
- Describe compliance-based assessments and caveats
- Base objectives on regulations
- Describe engagement scoping and compliance testing

CompTIA PenTest+: Information Gathering

- Describe scanning
- Describe enumeration
- Compare packet crafting and inspection
- Conduct fingerprinting
- Inspect X509v3 certificates
- Perform eavesdropping
- Describe decompilation
- Conduct debugging
- Describe open source intelligence gathering
- Describe mapping and prioritizing
- Describe common techniques to complete an attack
- Describe information gathering and preparation

CompTIA PenTest+: Vulnerability Identification

- Compare different types of scans
- Define scanning considerations
- Scan applications and containers
- Categorize assets for scans
- Describe adjudication and prioritization of scans
- Define common scanning themes
- Perform a vulnerability scan
- Analyze a vulnerability scan
- Describe vulnerability scanning

CompTIA PenTest+: Social Engineering and Specialized System Attacks

- Describe weaknesses in specialized systems
- Compare phishing attacks
- Specify elicitation exploits
- Define interrogation techniques
- Compare impersonation and hoaxing
- Describe shoulder surfing
- Describe USB key dropping
- Realize motivation techniques
- Choose the best software for a pentesting lab
- Configure a pentesting lab environment
- Describe social attacks and exploits

CompTIA PenTest+: Network-Based Exploits

- Compare name resolution and SMB exploits
- Exploit SNMP and SMTP protocols
- Describe FTP and DNS exploits
- Define pass the hash
- Describe man-in-the-middle attacks
- Classify denial-of-service exploits
- Describe NAC bypass and VLAN hopping
- Describe evil twin and deauthentication
- Classify fragmentation and WPS exploits
- Compare bluejacking to bluesnarfing
- Identify cloning, jamming, and repeating
- Describe network exploits

CompTIA PenTest+: Application-Based Vulnerabilities

- Identify injection attacks
- Define authentication exploits
- Describe authorization exploits
- Recognize XSS attacks
- Recognize CSRF/XSRF attacks
- Define clickjacking
- Compare security misconfigurations
- Describe file inclusion exploits
- Describe unsecure coding practices
- Describe application exploits

CompTIA PenTest+: Local Host Vulnerabilities

- Recognize host OS vulnerabilities
- Describe service and protocol configurations
- Define Linux privilege escalation
- Specify Windows privilege escalation
- Classify additional host-based exploits
- Recognize account setting vulnerabilities
- Describe escape exploits
- Describe local host exploits

CompTIA PenTest+: Post-Exploitation and Facilities Attacks

- Define lateral movement
- Classify persistence
- Identify ways to cover tracks
- Describe piggybacking and tailgating
- Define fence jumping
- Define dumpster diving
- Compare lock picking and lock bypass
- Describe egress sensors
- Recognize badge cloning
- Describe aspects of facility attacks and post-exploitation

Learn more at

www.hpe.com/ww/digitallearner

www.hpe.com/ww/digitallearner-contentpack

Follow us:

Hewlett Packard
Enterprise