HPE Digital Learner CompTIA - CySA +PenT Content Pack

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

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

---

*Realize Technology Value with Training IDC Infographic 2017, 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 password policies
- 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

### CompTIA Cybersecurity Analyst+ CS0-001: Investigate Security Incidents
- Recognize when to use HIDS
- Recognize when to use NIDS
- Recognize when to use NIPS
- Identify different types of malware
- Identify viruses
- Identify worms
- Identify 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

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

### CompTIA PenTest+: Planning for an Engagement
- Define impact analysis and remediation timelines
- Describe impact analysis and remediation timelines
- Examine engagement support resources
- Examine pertinent contracts and agreements
- Evaluate environmental differences
- Obtain written authorization
- Describe engagement
<table>
<thead>
<tr>
<th>Component Name</th>
<th>Topics</th>
<th>Techniques</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CompTIA PenTest+: Scoping an Engagement</strong></td>
<td>• Compare types of assessments</td>
<td>• Strategize scoping</td>
</tr>
<tr>
<td></td>
<td>• Define special scoping factors</td>
<td>• Explain risk acceptance and impact tolerance</td>
</tr>
<tr>
<td></td>
<td>• Select targets</td>
<td>• Describe scheduling and scope creep</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Explain threat actors and threat agents</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Describe compliance-based assessments and caveats</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Base objectives on regulations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Describe engagement scoping and compliance testing</td>
</tr>
<tr>
<td><strong>CompTIA PenTest+: Information Gathering</strong></td>
<td>• Describe scanning</td>
<td>• Conduct fingerprinting</td>
</tr>
<tr>
<td></td>
<td>• Describe enumeration</td>
<td>• Inspect X509v3 certificates</td>
</tr>
<tr>
<td></td>
<td>• Compare packet crafting and inspection</td>
<td>• Perform eavesdropping</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Describe decompilation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Conduct debugging</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Describe open source intelligence gathering</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Describe mapping and prioritizing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Describe common techniques to complete an attack</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Describe information gathering and preparation</td>
</tr>
<tr>
<td><strong>CompTIA PenTest+: Vulnerability Identification</strong></td>
<td>• Compare different types of scans</td>
<td>• Categorize assets for scans</td>
</tr>
<tr>
<td></td>
<td>• Define scanning considerations</td>
<td>• Describe adjudication and prioritization of scans</td>
</tr>
<tr>
<td></td>
<td>• Scan applications and containers</td>
<td>• Define common scanning themes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Perform a vulnerability scan</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Analyze a vulnerability scan</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Describe vulnerability scanning</td>
</tr>
<tr>
<td><strong>CompTIA PenTest+: Social Engineering and</strong></td>
<td>• Compare weaknesses in specialized systems</td>
<td>• Define interrogation techniques</td>
</tr>
<tr>
<td><strong>Specialized System Attacks</strong></td>
<td>• Compare phishing attacks</td>
<td>• Compare impersonation and hoaxing</td>
</tr>
<tr>
<td></td>
<td>• Specify elicitation exploits</td>
<td>• Describe shoulder surfing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Describe USB key dropping</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Realize motivation techniques</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Choose the best software for a pentesting lab</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Configure a pentesting lab environment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Describe social attacks and exploits</td>
</tr>
<tr>
<td><strong>CompTIA PenTest+: Network-Based Exploits</strong></td>
<td>• Compare name resolution and SMB exploits</td>
<td>• Define pass the hash</td>
</tr>
<tr>
<td></td>
<td>• Exploit SNMP and SMTP protocols</td>
<td>• Describe man-in-the-middle attacks</td>
</tr>
<tr>
<td></td>
<td>• Describe FTP and DNS exploits</td>
<td>• Classify denial-of-service exploits</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Describe NAC bypass and VLAN hopping</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Describe evil twin and deauthentication</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Classify fragmentation and WPS exploits</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Compare bluejacking to bluesnarfing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Identify cloning, jamming, and repeating</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Describe network exploits</td>
</tr>
<tr>
<td><strong>CompTIA PenTest+: Application-Based Vulnerabilities</strong></td>
<td>• Identify injection attacks</td>
<td>• Describe authorization exploits</td>
</tr>
<tr>
<td></td>
<td>• Define authentication exploits</td>
<td>• Recognize XSS attacks</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Recognize CSRF/XSRF attacks</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Define clickjacking</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Compare security misconfigurations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Describe file inclusion exploits</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Describe unsecure coding practices</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Describe application exploits</td>
</tr>
<tr>
<td><strong>CompTIA PenTest+: Local Host Vulnerabilities</strong></td>
<td>• Recognize host OS vulnerabilities</td>
<td>• Specify Windows privilege escalation</td>
</tr>
<tr>
<td></td>
<td>• Describe service and protocol configurations</td>
<td>• Classify additional host-based exploits</td>
</tr>
<tr>
<td></td>
<td>• Define Linux privilege escalation</td>
<td>• Recognize account setting vulnerabilities</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Describe escape exploits</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Describe local host exploits</td>
</tr>
<tr>
<td><strong>CompTIA PenTest+: Post-Exploitation and</strong></td>
<td>• Define lateral movement</td>
<td>• Describe piggybacking and tailgating</td>
</tr>
<tr>
<td><strong>Facilities Attacks</strong></td>
<td>• Classify persistence</td>
<td>• Define fence jumping</td>
</tr>
<tr>
<td></td>
<td>• Identify ways to cover tracks</td>
<td>• Define dumpster diving</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Compare lock picking and lock bypass</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Describe egress sensors</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Recognize badge cloning</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Describe aspects of facility attacks and post-exploitation</td>
</tr>
</tbody>
</table>
Learn more at
www.hpe.com/ww/digitallearner
www.hpe.com/ww/digitallearner-contentpack

Follow us: