CompTIA PenTest+ Objectifs de l'examen de certification

NUMÉRO D'EXAMEN : PT0-003

À propos de l'examen

L'examen de certification CompTIA PenTest+ certifie que le candidat retenu possède les connaissances et les compétences requises pour :

- Planifier, définir le périmètre et réaliser la collecte d'informations dans le cadre d'un test de pénétration.
- Mener des attaques conformes aux exigences légales et de conformité.
- Effectuer chaque phase d'un test de pénétration en utilisant et en modifiant les outils appropriés et utiliser les tactiques, techniques et procédures appropriées.
- Analyser les résultats de chaque phase d'un test de pénétration pour élaborer un rapport écrit, communiquer efficacement les résultats aux parties prenantes et fournir des recommandations pratiques.

ACCRÉDITATION DES EXAMENS

L'examen CompTIA PenTest+ est accrédité par l'ANSI pour démontrer sa conformité à la norme ISO 17024 et, en tant que tel, fait l'objet de révisions et de mises à jour régulières des objectifs de l'examen.

DÉVELOPPEMENT DE L'EXAMEN

Les examens CompTIA sont basés sur des ateliers d'experts en la matière et de résultats d'enquêtes menées dans l'ensemble du secteur qui mettent en avant les compétences et les connaissances nécessaires pour réussir en tant que professionnel de l'informatique.

POLITIQUE D'UTILISATION DES MATÉRIAUX AUTORISÉS DE CompTIA

CompTIA Certifications, LLC n'est pas affilié à des sites de formation tiers non autorisés (également appelés « brain dumps ») et n'autorise, n'approuve ni ne tolère l'utilisation de leur contenu. Les personnes qui utilisent ce type de matériel pour se préparer à un examen CompTIA verront leur certification révoquée et seront suspendues de tout examen futur, conformément au CompTIA Candidate Agreement. Afin de communiquer plus clairement les politiques d'examen de CompTIA concernant l'utilisation de matériel d'étude non autorisé, CompTIA oriente tous les candidats à la certification à consulter les Politiques de l'examen de certification CompTIA. Veuillez prendre connaissance de toutes les politiques de CompTIA avant d'entamer le processus d'étude de tout examen de CompTIA. Les candidats devront se conformer au CompTIA Candidate Agreement. Si un candidat souhaite savoir si les supports d'étude sont considérés comme non autorisés (alias « brain dumps »), il doit contacter CompTIA à l'adresse suivante examsecurity@CompTIA.org pour confirmer.

REMARQUE

Les listes d'exemples fournies sous forme de puces ne sont pas exhaustives. D'autres exemples de technologies, de processus ou de tâches se rapportant à chaque objectif peuvent également être inclus dans l'examen, même s'ils ne sont pas énumérés ou couverts dans le présent document sur les objectifs. CompTIA examine constamment le contenu de nos examens et met à jour les questions de test pour s'assurer que nos examens sont à jour et que la sécurité des questions est protégée. Si nécessaire, nous publierons des examens mis à jour sur la base des objectifs d'examen existants. Sachez que tous les documents de préparation à l'examen seront toujours valables.

DÉTAILS DU TEST

Examen requis	PT0-003
Nombre de questions	Maximum de 90
Types de questions	Questions à choix multiples et questions basées sur la performance
Durée du test	165 minutes
Expérience recommandée	3-4 ans dans un poste de conseiller en test d'intrusion
Score de réussite	750

OBJECTIFS DE L'EXAMEN (DOMAINES)

Le tableau ci-dessous énumère les domaines mesurés par cet examen et la mesure dans laquelle ils sont représentés.

DOMAINE		POURCENTAGE DE L'EXAMEN
1.0	Gestion de l'engagement	13 %
2.0	Reconnaissance et dénombrement	21 %
3.0	Découverte et analyse des vulnérabilités	17 %
4.0	Attaques et exploits	35 %
5.0	Post-exploitation et mouvement latéral	14 %
Total		**100 %**

1.0 Gestion de l'engagement

1.1 Résumer les activités préalables à l'engagement.

- **Définition du champ d'application**
  - Règlements, cadres, et normes
    - Vie privée
    - Sécurité
  - Règles d'engagement
    - Exclusions
    - Cas de test
    - Processus d'escalade
    - Fenêtre de test
  - Types d'accords
    - Accord de non-divulgation (NDA)
    - Accord-cadre de services (ACS)
    - Déclaration de travail (SoW)
    - Conditions d'utilisation (ToS)
  - Sélection de la cible
    - Plages de routage inter-domaines sans classe (CIDR)
    - Domaines
    - Adresses de protocole Internet (IP)
    - Localisateur de ressources uniformes (URL)
  - Types d'évaluation
    - Web
    - Réseau
    - Mobile
    - Cloud
    - Interface de programmation d'applications (API)
    - Application
    - Sans fil
- **Modèle de responsabilité partagée**
  - Responsabilités du fournisseur d'hébergement
  - Responsabilités des clients
  - Responsabilités du conseiller en test d'intrusion
  - Responsabilités des tiers
- **Considérations juridiques et éthiques**
  - Lettres d'autorisation
  - Exigences en matière de rapports obligatoires
  - Risque pour le conseiller en test d'intrusion

1.2 Expliquer les activités de collaboration et de communication.

- **Examen par les pairs**
- **Alignement des parties prenantes**
- **Analyse des causes profondes**
- **Chemin d'escalade**
- **Distribution sécurisée**
- **Articulation du risque, de la gravité et de l'impact**
- **Redéfinition des priorités des objectifs**
- **Analyse de l'impact sur les entreprises**
- **Acceptation du client**

1.3 Comparer et opposer les cadres et les méthodologies de test.

- **Manuel de méthodologie des tests de sécurité à la source ouverte (OSSTMM)**
- **Conseil des testeurs de sécurité éthique agréés (CREST)**
- **Norme d'exécution des tests de pénétration (PTES)**
- **MITRE ATT&CK**
- **Top 10 de l'Open Worldwide Application Security Project (OWASP)**
- **Norme de vérification de la sécurité des applications mobiles (MASVS) de l'OWASP**
- **Modèle Purdue**
- **Cadres de modélisation des menaces**
  - Potentiel de dommages, reproductibilité, exploitabilité, utilisateurs affectés, découvrabilité (DREAD)
  - Usurpation d'identité, falsification, répudiation, divulgation d'informations, déni de service, élévation de privilèges (STRIDE)
  - Évaluation des menaces, des actifs et des vulnérabilités critiques sur le plan opérationnel (OCTAVE)

CompTIA

1.4 Expliquer les éléments d'un rapport de test de pénétration.

- Alignement du format
- Spécifications de la documentation
- Évaluation des risques
- Définitions
- Composants du rapport
  - Résumé exécutif
  - Méthodologie
  - Constatations détaillées
  - Récit de l'attaque
  - Recommandations
    - Conseils de remédiation
- Limites et hypothèses des tests
- Considérations relatives aux rapports
  - Juridique
  - Éthique
  - Contrôle qualité (QC)
  - Intelligence artificielle (IA)

1.5 À partir d'un scénario, analyser les résultats et recommander les mesures correctives appropriées dans un rapport.

- Contrôles techniques
  - Durcissement du système
  - Assainissement de l'entrée utilisateur/paramétrage des requêtes
  - Authentification multifactorielle
  - Cryptage
  - Remédiation au niveau du processus
  - Gestion des correctifs
  - Rotation des touches
  - Gestion des certificats
  - Solution de gestion des secrets
  - Segmentation du réseau
  - Contrôles de sécurité de l'infrastructure
- Contrôles administratifs
  - Contrôle d'accès basé sur les rôles
  - Développement de logiciels sécurisés cycle de vie
  - Exigences minimales en matière de mot de passe
  - Politiques et procédures
- Contrôles opérationnels
  - Rotation des emplois
  - Restrictions liées à l'heure de la journée
  - Vacances obligatoires
  - Formation des utilisateurs
- Contrôles physiques
  - Vestibule de contrôle d'accès
  - Contrôles biométriques
  - Vidéosurveillance

2.0 Reconnaissance et dénombrement

2.1 À partir d'un scénario, appliquer les techniques de collecte d'informations.

- Reconnaissance active et passive
- Renseignements de source ouverte (OSINT)
  - Médias sociaux
  - Sites d'emploi
  - Scanner les référentiels de codes
  - Système de noms de domaine (DNS)
    - Recherches DNS
    - Recherche inversée de DNS
  - Pages mises en cache
  - Défauts cryptographiques
  - Fuites de mots de passe
- Reconnaissance du réseau
- Analyse du protocole
  - Analyse du protocole de contrôle de transmission (TCP)/protocole de datagramme de l'utilisateur (UDP)
- Journaux de transparence des certificats
- Divulgation d'informations
- Analyse des moteurs de recherche/ dénombrement
- Reniflage de réseau
  - Internet des objets (IoT) et protocoles de technologie opérationnelle (OT)
- Accrochage de bannière
- Langage de balisage hypertexte (HTML) scraping

2.2 À partir d'un scénario, appliquer les techniques de dénombrement.

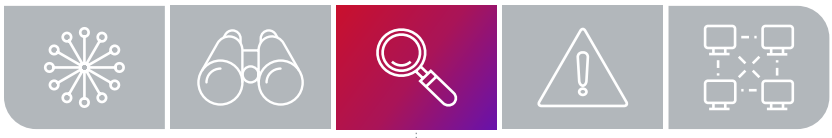
- Empreinte du système d'exploitation (OS)
- Découverte des services
- Dénombrement des protocoles
- Dénombrement DNS
- Dénombrement des répertoires
- Découverte de l'hôte
- Dénombrement des actions
- Dénombrement des utilisateurs locaux
- Dénombrement des comptes de messagerie
- Dénombrement sans fil
- Dénombrement des permissions
- Dénombrement des secrets
  - Clés d'accès au nuage
  - Mots de passe
  - Clés API
  - Jetons de session
- Cartographie du chemin d'attaque
- Pare-feu d'application Web (WAF) dénombrement
  - Adresse d'origine
- Recherche sur le Web
- Dénombrement manuel
  - Robots.txt
  - Plan du site
  - Plugins pour la plate-forme

2.3 À partir d'un scénario, modifier les scripts de reconnaissance et de dénombrement.

- Collecte d'informations
- Manipulation des données
- Langages de script
  - Bash
  - Python
  - PowerShell
- Constructions logiques
  - Boucles
  - Conditionnels
  - Opérateur booléen
  - Opérateur de chaîne
  - Opérateur arithmétique
- Utilisation de bibliothèques, de fonctions, et des classes

2.4 À partir d'un scénario, utiliser les outils appropriés pour la reconnaissance et le dénombrement.

- Wayback Machine
- Maltego
- Recon-ng
- Shodan
- SpiderFoot
- WHOIS
- nslookup/dig
- Censys.io
- Hunter.io
- DNSdumpster
- Amass
- Nmap
  - Nmap Scripting Engine (NSE)
- theHarvester
- WiGLE.net
- InSSIDer
- OSINTframework.com
- Wireshark/tcpdump
- Aircrack-ng



3.0 Découverte et analyse des vulnérabilités

3.1 À partir d'un scénario, identifier les vulnérabilités en utilisant différentes techniques.

- **Types d'analyses**
  - Analyses des conteneurs
    - Analyses Sidecar
  - Analyses d'application
    - Tests dynamiques de sécurité des applications (DAST)
    - Tests interactifs de sécurité des applications (IAST)
    - Analyse de la composition des logiciels (SCA)
    - Tests statiques de sécurité des applications (SAST)
      - Infrastructure as Code (IaC)
      - Analyse du code source
    - Analyse mobile
  - Analyses du réseau
    - Analyse TCP/UDP
    - Analyses furtives
  - Analyses basées sur l'hôte
  - Analyses authentifiées ou non authentifiées
  - Secrets scanning
  - Sans fil
    - Analyse de l'identifiant de l'ensemble de services (SSID)
    - Analyse des canaux
    - Analyse de l'intensité du signal
- **Systèmes de contrôle industriel (SCI) évaluation de la vulnérabilité**
  - Évaluation manuelle
  - Mise en miroir des ports
- **Outils**
  - Nikto
  - Greenbone/Open Vulnerability Assessment Scanner (OpenVAS)
  - TruffleHog
  - BloodHound
  - Tenable Nessus
  - PowerSploit
  - Grype
  - Trivy
  - Kube-hunter

3.2 À partir d'un scénario, analyser les résultats des phases de reconnaissance, d'analyse et de dénombrement.

- **Valider les résultats de l'analyse, de la reconnaissance et du dénombrement**
  - Faux positifs
  - Faux négatifs
  - Vrais positifs
  - Complétude de l'analyse
  - Dépannage des configurations de l'analyse
- **Sélection de l'exploit public**
- **Utiliser des scripts pour valider les résultats**

3.3 Expliquer les concepts de sécurité physique.

- **Tailgating**
- **Enquêtes sur le terrain**
- **Gouttes de bus universel en série (USB)**
- **Clonage de badge**
- **Crochetage de serrure**

4.0 Attaques et exploits

4.1 À partir d'un scénario, analyser les résultats pour établir des priorités et préparer des attaques.

- **Priorité à la cible**
  - Identification des biens de grande valeur
  - Descripteurs et métriques
    - Score de base du système CVSS (Common Vulnerability Scoring)
    - Vulnérabilités et expositions communes (CVE)
    - Common Weakness Enumeration (CWE) (énumération des faiblesses communes)
    - Système de notation de la prédiction des exploits (EPSS)
  - Logiciels/systèmes en fin de vie
  - Configurations par défaut
  - Services d'exécution
  - Méthodes de chiffrement vulnérables
  - Capacités défensives
  - Dépendances
  - Prise en compte des limites du champ d'application
  - Étiquetage de systèmes sensibles
- **Sélection des capacités**
  - Sélection des outils
  - Sélection et personnalisation des exploits
    - Analyse du code
  - Documentation
    - Chemin d'attaque
    - Création de diagrammes de bas niveau
    - Storyboard

4.2 À partir d'un scénario, effectuer des attaques réseau à l'aide des outils appropriés.

- **Types d'attaques**
  - Informations d'identification par défaut
  - Attaque par le chemin
  - Services de certificats
  - Exploitation de services mal configurés
  - Saut de réseau local virtuel (VLAN)
  - Hôtes multiréseau
  - Attaque par relais
  - Dénombrement des actions
  - Fabrication de paquets
- **Outils**
  - Metasploit
  - Netcat
  - Nmap
    - NSE
  - Impacket
  - CrackMapExec (CME)
  - Wireshark/tcpdump
  - msfvenom
  - Répondant
  - Hydra

4.3 À partir d'un scénario, effectuer des attaques d'authentification à l'aide des outils appropriés.

- **Types d'attaques**
  - Attaques de fatigue de l'authentification multifactorielle (MFA)
  - Attaques Pass-the-hash
  - Attaques Pass-the-ticket
  - Attaques Pass-the-token
  - Attaques Kerberos
  - Injection du protocole LDAP (Lightweight Directory Access Protocol)
  - Attaques par dictionnaire
  - Attaques par force brute
  - Attaques par masque
  - Pulvérisation du mot de passe
  - Remplissage de lettres de créance
  - Attaques OpenID Connect (OIDC)
  - Attaques SAML (Security Assertion Markup Language)
- **Outils**
  - CME
  - Répondant
  - hashcat
  - John the Ripper
  - Hydra
  - BloodHound
  - Medusa
  - Burp Suite

4.4 À partir d'un scénario, effectuer des attaques basées sur l'hôte à l'aide des outils appropriés.

- **Types d'attaques**
  - Escalade de privilèges
  - Dumping d'identité
  - Contourner les outils de sécurité
  - Points d'extrémité mal configurés
  - Obfuscation de la charge utile
  - Contournement de l'accès contrôlé par l'utilisateur
  - Échappement du shell
  - Échappement de kiosque
  - Injection de bibliothèque
  - Processus d'évidage et d'injection
  - Falsification du journal
  - Injection d'un chemin de service non quoté
- **Outils**
  - Mimikatz
  - Rubeus
  - Certify
  - Seatbelt
  - PowerShell/PowerShell Integrated Scripting Environment (ISE)
  - PsExec
  - Evil-WinRM
  - Living off the land binaries (LOLbins)

4.5 À partir d'un scénario, effectuer des attaques d'applications Web à l'aide des outils appropriés.

- **Types d'attaques**
  - Attaque par force brute
  - Attaque par collision
  - Traversée de répertoire
  - Falsification des requêtes côté serveur (SSRF)
  - Falsification des demandes intersites (CSRF)
  - Attaque de désérialisation
  - Attaques par injection
    - Injection en langage de requête structuré (SQL)
    - Injection de commandes
    - Cross-site scripting (XSS)
    - Injection de modèles côté serveur
  - Référence à un objet direct non sécurisé
  - Détournement de session
  - Exécution de code arbitraire
  - Inclusions de fichiers
    - Inclusion de fichiers à distance (RFI)
    - Inclusion de fichiers locaux (LFI)
    - Web shell
  - Abus de l'API
  - Manipulation de jetons Web JSON (JWT)
- **Outils**
  - TruffleHog
  - Burp Suite
  - Zed Attack Proxy (ZAP)
  - Postman
  - sqlmap
  - Gobuster/DirBuster
  - Wfuzz
  - WPScan

4.6 À partir d'un scénario, effectuer des attaques basées sur le cloud à l'aide des outils appropriés.

- **Types d'attaques**
  - Attaques contre les services de métadonnées
  - Mauvaise configuration de la gestion des identités et des accès
  - Intégrations de tiers
  - Mauvaise configuration des ressources
    - Segmentation du réseau
    - Contrôles du réseau
    - Identifiants de gestion des identités et des accès (IAM)
    - Seaux de stockage exposés
    - Accès du public aux services
  - Exposition des informations de journalisation
  - Altération de l'image et des artefacts
  - Attaques de la chaîne d'approvisionnement
  - Attaques de la charge de travail en cours d'exécution
  - Échappement de conteneurs
  - Abus de relation de confiance
- **Outils**
  - Pacu
  - Docker Bench
  - Kube-hunter
  - Prowler
  - ScoutSuite
  - Outils de fournisseurs natifs du cloud

4.7 À partir d'un scénario, effectuer des attaques sans fil à l'aide des outils appropriés.

- **Attaques**
  - Wardriving
  - Attaque du jumeau maléfique
  - Brouillage des signaux
  - Fuzzing de protocoles
  - Fabrication de paquets
  - Désauthentification
  - Portail captif
  - Wi-Fi Protected Setup (WPS) numéro d'identification personnel (PIN) attaque
- **Outils**
  - WPAD
  - WiFi-Pumpkin
  - Aircrack-ng
  - WiGLE.net
  - InSSIDer
  - Kismet

4.8 À partir d'un scénario, effectuer des attaques d'ingénierie sociale à l'aide des outils appropriés.

- **Types d'attaques**
  - Phishing
  - Vishing
  - Chasse à la baleine
  - Spearphishing
  - Smishing
  - Plongée dans les bennes à ordures
  - Surveillance
  - Surf sur l'épaule
  - Tailgating
  - Écoute clandestine
  - Point d'eau
  - Usurpation d'identité
  - Récolte de données d'identification
- **Outils**
  - Boîte à outils d'ingénierie sociale (SET)
  - Gophish
  - Evilginx
  - theHarvester
  - Maltego
  - Recon-ng
  - Cadre d'exploitation des navigateurs (BeEF)

4.9 Expliquer les attaques courantes contre les systèmes spécialisés.

- **Types d'attaques**
  - Attaques mobiles
    - Divulgation d'informations
    - Jailbreak/rooting
    - Abus de permis
  - Attaques par IA
    - Injection rapide
    - Modèle de manipulation
  - TO
    - Manipulation d'enregistrements
    - Attaque du bus CAN
    - Attaque Modbus
    - Attaque en texte intégral
    - Attaque par répétition
  - Communication en champ proche (NFC)
  - Bluejacking
  - Identification par radiofréquence (RFID)
  - Spam Bluetooth
- **Outils**
  - Scapy
  - tcprelay
  - Wireshark/tcpdump
  - MobSF
  - Frida
  - Drozer
  - Android Debug Bridge (ADB)
  - Bluestrike

4.10 À partir d'un scénario, utiliser des scripts pour automatiser les attaques.

- **PowerShell**
  - PowerSploit
  - PowerView
  - PowerUpSQL
  - Recherche AD
- **Bash**
  - Gestion des entrées/sorties
  - Manipulation de données
- **Python**
  - Impacket
  - Scapy
- **Simulation de brèche et d'attaque (BAS)**
  - Caldera
  - Infection Monkey
  - Atomic Red Team

5.0 Post-exploitation et mouvement latéral

5.1 À partir d'un scénario, effectuer des tâches pour établir et maintenir la persistance.

- Tâches planifiées/travaux de synchronisation
- Création de services
- Coquille inversée
- Coquille de liaison
- Ajouter de nouveaux comptes
- Obtenir des identifiants de compte valides
- Clés de registre
- Cadres de commandement et de contrôle (C2)
- Porte dérobée
  - Web shell
  - Cheval de Troie
- Rootkit
- Extensions de navigateur
- Falsification des contrôles de sécurité

5.2 À partir d'un scénario, effectuer des tâches pour se déplacer latéralement dans l'environnement.

- Pivotant
- Création de relais
- Dénombrement
  - Découverte des services
  - Découverte du trafic réseau
  - Saisie des identifiants supplémentaires
  - Dumping d'identité
  - Recherche de chaînes

- Découverte des services
  - Server Message Block (SMB)/fileshares
  - Remote Desktop Protocol (RDP)/ Virtual Network Computing (VNC)
  - Secure Shell (SSH)
  - Texte clair
  - LDAP
  - Appel de procédure à distance (RPC)
  - Protocole de transfert de fichiers (FTP)
  - Telnet
  - Hypertext Transfer Protocol (HTTP)/Hypertext Transfer Protocol Secure (HTTPS)
    - Interfaces Web
  - Line Printer Daemon (LPD)
  - JetDirect
  - RPC/Modèle d'objets à composants distribués (DCOM)
  - ID des processus
- Instrumentation de gestion des fenêtres (WMI)
- Gestion à distance des fenêtres (WinRM)
- Outils
  - LOLBins
    - Netstat
    - Commandes nets
    - cmd.exe
    - explorer.exe
    - ftp.exe
    - mmc.exe
    - rundll32
    - msbuild
    - route
    - strings/findstr.exe
  - Pacte
  - CrackMapExec
  - Impacket
  - Netcat
  - sshuttle
  - Proxychains
  - PowerShell ISE
  - Fichiers batch
  - Metasploit
  - PsExec
  - Mimikatz

5.3 Résumer les concepts liés à la stadification et à l'exfiltration.

- Cryptage et compression de fichiers
- Canal caché
  - Stéganographie
  - DNS
  - Internet Control Message Protocol (ICMP)
  - HTTPS
- Courriel
- Ressources inter-comptes
- Stockage dans le cloud
- Autres flux de données
- Sites de stockage de texte
- Montage du lecteur virtuel

5.4 Expliquer les activités de nettoyage et de restauration.

- Supprimer les mécanismes de persistance
- Revenir sur les changements de configuration
- Supprimer les identifiants créés par le testeur
- Retirer les outils
- Réduire les infrastructures
- Préserver les artefacts
- Destruction sécurisée des données

CompTIA PenTest+ PT0-003 Liste des acronymes

Voici une liste d'acronymes qui apparaissent dans l'examen CompTIA PenTest+ PT0-003. Les candidats sont encouragés à consulter la liste complète et à acquérir une connaissance pratique de tous les acronymes énumérés dans le cadre d'un programme complet de préparation à l'examen.

ACRONYME	DÉFINITION
AD	Active Directory (Répertoire actif)
ADB	Android Debug Bridge (Pont de débogage Android)
AI	Artificial Intelligence (Intelligence artificielle)
AP	Access Point (Point d'accès)
API	Application Programming Interface (Interface de programmation d'applications)
APT	Advanced Persistent Threat (Menace persistante avancée)
BAS	Breach and Attack Simulation (Simulation de brèche et d'attaque)
BeEF	Browser Exploitation Framework (Framework d'exploitation des navigateurs)
BGP	Border Gateway Protocol (Protocole de passerelle frontalière)
BIA	Business Intelligence Analytics (Analyse de la Business Intelligence)
C2	Command and Control (Commandement et contrôle)
CI/CD	Continuous Integration/Continuous Delivery (Intégration continue/Livraison continue)
CIDR	Classless Inter-domain Routing (Routage inter-domaines sans classe)
CGI	Common Gateway Interface (Interface de passerelle commune)
CLI	Command-line Interface (Interface de ligne de commande)
CME	CrackMapExec
CNAME	Canonical Name (Nom canonique)
COFF	Common Object File Format (Format de fichier objet commun)
CREST	Council of Registered Ethical Security Testers (Conseil des testeurs de sécurité éthiques agréés)
CSRF	Cross-site Request Forgery (Falsification de requête intersite)
CVE	Common Vulnerabilities and Exposures (Vulnérabilités et expositions communes)
CVSS	Common Vulnerability Scoring System (Système commun d'évaluation des vulnérabilités)
CWE	Common Weakness Enumeration (Énumération des faiblesses communes)
DAST	Dynamic Application Security Testing (Test dynamique de la sécurité des applications)
DCOM	Distributed Component Object Model (Modèle d'objet de composant distribué)
DDos	Distributed Denial of Service (Déni de service distribué)
DMARC	Domain-based Message Authentication, Reporting, and Conformance (Authentification, notification et conformité des messages basés sur le domaine)
DNS	Domain Name System (Système de noms de domaine)
DoS	Denial of Service (Déni de service)
DREAD	Damage potential, Reproducibility, Exploitability, Affected users, Discoverability (Potentiel de dommages, reproductibilité, exploitabilité, utilisateurs concernés, découvrabilité)
DROWN	Decrypting RSA [Rivest-Shamir-Adleman] with Obsolete and Weakened Encryption (Décryptage de RSA [Rivest-Shamir-Adleman] avec un chiffrement obsolète et affaibli)
EFSRPC	Encrypting File System Remote Protocol (Protocole de chiffrement du système de fichiers à distance)
ELF	Executable and Linkable Format (Format exécutable et lisible)
EPSS	Exploit Prediction Scoring System (Système d'évaluation de la prédiction des exploits)
EXIF	Exchangeable Image File Format (Format de fichier image échangeable)

ACRONYMES	DÉFINITION DES
FQDN	Fully Qualified Domain Name (Nom de domaine entièrement qualifié)
FTP	File Transfer Protocol (Protocole de transfert de fichiers)
GIF	Graphic Interchange Format (Format d'échange graphique)
HID	Host-based Intrusion Detection (Détection d'intrusion basée sur l'hôte)
HSTS	HTTP Strict Transport Security (Sécurité stricte du transport)
HTML	Hypertext Markup Language (Langage de balisage hypertexte HTML)
HTTP	Hypertext Transfer Protocol (Protocole de transfert hypertexte)
HTTPS	Hypertext Transfer Protocol Secure (Protocole de transfert hypertexte sécurisé)
IaC	Infrastructure as Code (Infrastructure en tant que code)
IAM	Identity and Access Management (Gestion des identités et des accès)
IAST	Interactive Application Security Testing (Test interactif de sécurité des applications)
ICMP	Internet Control Message Protocol (Protocole de message de contrôle Internet)
ICS	Industrial Control System (Système de contrôle industriel)
IDOR	Insecure DIrect Object Reference (Référence d'objet direct non sécurisé)
IdP	Identity Provider (Fournisseur d'identité)
IDS	Intrusion Detection System (Système de détection d'intrusion)
IGRP	Interior Gateway Routing Protocol (Protocole de routage de la passerelle intérieure)
IoT	Internet of Things (Internet des objets)
IP	Internet Protocol (Protocole Internet)
IPS	Intrustion Prevention System (Système de prévention des intrusions)
ISE	Integrated Scripting Environment (Environnement de script intégré)
JWT	JSON Web Token (Jeton Web JSON)
KDC	Key Distribution Center (Centre de distribution de clés)
KRBTGT	Kerberos Ticket Granting Ticket (Ticket d'octroi de ticket Kerberos)
LDAP	Lightweight Directory Access Protocol (Protocole d'accès aux annuaires légers)
LFI	Local File Inclusion (Inclusion de fichiers locaux)
LLMNR	Link-local Multicast Name Resolution (Résolution de noms de multidiffusion locale de liaison)
LOLBins	Living off the Land Binaries (Attaque visant à vivre de la terre)
LPD	Line Printer Daemon (Protocole démon d'imprimante en ligne)
LSASS	Local Security Authority Subsystem Service (Service de sous-système de l'autorité locale de sécurité)
MAC	Media Access Control (Contrôle d'accès au média)
MASVS	Mobile Application Security Verification Standard (Norme de vérification de la sécurité des applications mobiles)
MFA	Multifactor Authentication (Authentification multifactorielle)
MIB	Management Information Base (Base d'informations de gestion)
MMS	Multimedia Messaging Service (Service de messagerie multimédia)
MSA	Master Services Agreement (Contrat-cadre de services)
MX	Mail Exchange (Échange de courriel)
NDA	Non-disclosure Agreement (Accord de non-divulgation)
NFC	Near-field Communication (Communication en champ proche)
NSE	Nmap Scripting Engine (Moteur de scripts de Nmap)
NTLM	New Technology LAN Manager (Gestionnaire LAN Nouvelles Technologies)
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation (Évaluation des menaces, des actifs et des vulnérabilités critiques sur le plan opérationnel)
OIDC	OpenID Connect
OpenVAS	Open Vulnerability Assessment Scanner (Scanner ouvert d'évaluation des vulnérabilités)
OS	Operating System (Système d'exploitation)
OSINT	Open-source Intelligence (Renseignement de source ouverte)
OSSTMM	Open-source Security Testing Methodology Manual (Manuel de méthodologie de test de sécurité à source ouverte)
OT	Operational Technology (Technologie opérationnelle)
OWASP	Open Worldwide Application Security Project (Projet mondial ouvert de sécurité des applications)
PTES	Penetration Testing Execution Standard (Norme d'exécution des tests de pénétration)

ACRONYMES	DÉFINITION DES
PWS	Performance Work Statement (Déclaration de performance)
QC	Quality Control (Contrôle qualité)
RCE	Remote Code Execution (Exécution de code à distance)
RDP	Remote Desktop Protocol (Protocole de bureau à distance)
RFI	Remote File Inclusion (Inclusion de fichiers à distance)
RFID	Radio Frequency Identification (Identification par radiofréquence)
RIP	Routing Information Protocol (Protocole d'information sur le routage)
RPC	Remote Procedure Call (Appel de procédure à distance)
SaaS	Software as a Service (Logiciel en tant que service)
SAM	Security Account Manager (Gestionnaire de compte de sécurité)
SAML	Security Assertion Markup Language (Langage d'assertion de sécurité)
SAST	Static Application Security Testing (Test statique de sécurité des applications)
SCA	Software Composition Analysis (Analyse de la composition des logiciels)
SCADA	Supervisory Control and Data Acquisition (Contrôle de surveillance et acquisition de données)
SDK	Software Development Kit (Kit de développement logiciel)
SDLC	Software Development Life Cycle (Cycle de vie du développement logiciel)
SDR	Software-defined Radio (Radio logicielle)
SET	Social Engineering Toolkit (Boîte à outils d'ingénierie sociale)
SIEM	Security Information and Event Management (Gestion des informations et des événements de sécurité)
SMB	Server Message Block (Bloc de message serveur)
SMS	Short Message Service (Service de messages courts)
SNMP	Simple Network Management Protocol (Protocole de gestion de réseau simple)
SOA	Start of Authority (Début de l'autorité)
SOC	Security Operations Center (Centre d'opérations de sécurité)
SoW	Statement of Work (Déclaration de travail)
SPN	Service Principal Name (Nom principal de service)
SQL	Structured Query Language (Langage de requête structuré)
SQLi	Structured Query Language Injection (Injection de langage de requête structuré)
SSH	Secure Shell (Shell sécurisé)
SSID	Service Set Identifier (Identificateur d'ensemble de services)
SSL	Secure Socket Layer (Couche de sockets sécurisés)
SSO	Single Sign-on (Signature unique)
SSRF	Server-side Request Forgery (Falsification de requête côté serveur)
STRIDE	Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege (Usurpation d'identité, falsification, répudiation, divulgation d'informations, déni de service, élévation de privilèges)
TCP	Transmission Control Protocol (Protocole de contrôle de transmission)
TGS	Ticket Granting Service (Service d'attribution des billets)
TLS	Transport Layer Security (Sécurité de la couche transport)
ToS	Terms of Service (Conditions d'utilisation)
TTP	Techniques, Tactics, Procedures (Techniques, tactiques, procédures)
UDP	User Datagram Protocol (Protocole de datagramme utilisateur)
URL	Uniform Resource Locator (Localisateur de ressources uniformes)
USB	Universal Serial Bus (Bus universel en série)
VLAN	Virtual Local Area Network (Réseau local virtuel)
VNC	Virtual Network Computing (Informatique en réseau virtuel)
VPN	Virtual Private Network (Réseau privé virtuel)
WAF	Web Application Firewall (Web Application Firewall)
WinRM	Windows Remote Management (Gestion à distance de Windows)
WLAN	Wireless Local Area Network (Réseau local sans fil)
WMI	Windows Management Instrumentation (Instrumentation de gestion Windows)
WPAD	Web Proxy Auto Discovery (Découverte automatique du proxy Web)
WPS	Wi-Fi Protected Setup (configuration Wi-Fi protégée)
XSS	Cross-site Scripting (Script intersite)
ZAP	Zed Attack Proxy

CompTIA PenTest+ Proposition de matériel et liste de logiciels

CompTIA a inclus cette liste d'exemples de matériel et de logiciels pour aider les candidats à se préparer à l'examen PenTest+. Cette liste peut également être utile aux entreprises de formation qui souhaitent ajouter un volet laboratoire à leur offre de formation. Les listes à puces figurant sous chaque thème sont des exemples et ne sont pas exhaustives.

MATÉRIEL

- Ordinateurs
- Points d'accès sans fil
- Serveurs
- Interrupteurs
- Câblage
- Pare-feu
- Routeur
- Détection d'intrusion basée sur l'hôte (HID)/ contrôles d'accès aux portes
- Adaptateurs sans fil capables d'injecter des paquets
- Antenne directionnelle
- Appareil mobile
- Équipements IoT (caméras, micro-ordinateurs, téléviseurs intelligents, etc.)
- Adaptateur Bluetooth
- Imprimantes multifonctions (avec ou sans fil)
- Matériel de clonage NFC/RFID
- Kit de crochetage de serrure (le cas échéant)
- Dispositif biométrique
- Automate programmable
  - Kit de radio logicielle (SDR)

- Clés USB

LOGICIEL

- Accès à l'environnement cloud
  - Accès à l'interface de ligne de commande (CLI)
  - Accès à la console de gestion
  - Instances de services cloud

- Licence du système d'exploitation
- Système d'exploitation libre
- Cadres de tests de pénétration
- Logiciel de machine virtuelle
- Outils d'analyse
  - Outils d'analyse de vulnérabilité
  - SAST
  - DAST

- Outils de vérification des identifiants
  - Outils de pulvérisation
  - Craqueurs de mots de passe

- Outils de sécurité des applications
- Débogueurs
- Outils de test sans fil
- Outils de proxy Web
- Outils d'ingénierie sociale
- Outils d'accès à distance
- Outils de réseau
  - Analyseurs de protocole
  - Outils de reniflage

- Outils de test de la mobilité
- Outils de gestion des informations et des événements de sécurité (SIEM), de détection des intrusions (IDS), de prévention des intrusions (IPS) et de sécurité des points d'accès, libres ou accessibles au public
- Outils C2