Objetivos do Exame de Certificação CompTIA PenTest+

NÚMERO DO EXAME: PT0-003

Sobre o exame

O exame de certificação CompTIA PenTest+ certificará se o candidato tem o conhecimento e as habilidades necessárias para:

- Planejar, dimensionar e executar a coleta de informações como parte de um teste de intrusão.
- Executar ataques que estejam alinhados e cumpram os requisitos legais e de conformidade.
- Executar cada fase de um teste de intrusão usando e modificando ferramentas apropriadas e usar as táticas, técnicas e procedimentos apropriados.
- Analisar os resultados de cada fase de um teste de intrusão para desenvolver um relatório escrito, comunicar efetivamente as descobertas às partes interessadas e fornecer recomendações práticas.

CREDENCIAMENTO DO EXAME

O exame CompTIA PenTest+ é credenciado pelo ANSI para demonstrar conformidade com a norma ISO 17024 e, como tal, passa por revisões e atualizações regulares dos objetivos do exame.

ELABORAÇÃO DO EXAME

O resultado dos exames CompTIA é proveniente de workshops especializados e focados no assunto e pesquisas abrangentes em toda a indústria quanto às habilidades e conhecimentos exigidos de um profissional de TI.

POLÍTICA DE USO AUTORIZADO DE MATERIAIS DA COMPTIA

A CompTIA Certifications, LLC não está afiliada a, nem autoriza, endossa ou admite o uso de qualquer conteúdo fornecido por sites de treinamento externos não autorizados (também conhecidos como “brain dumps”). Os candidatos que usarem esses materiais como preparação para qualquer exame da CompTIA terão suas certificações anuladas e serão suspensos de futuros testes de acordo com o Contrato do Candidato CompTIA. Com o intuito de comunicar com maior clareza as políticas dos exames CompTIA referentes ao uso de materiais de estudo não autorizados, a CompTIA encaminha todos os candidatos à certificação para as Políticas do Exame de Certificação da CompTIA. Leia todas as políticas da CompTIA antes de iniciar o processo de estudo para qualquer exame CompTIA. Os candidatos serão obrigados a respeitar o Contrato do Candidato CompTIA. Se um candidato não tiver certeza se determinado material de estudo é considerado não autorizado (conhecido como “brain dump”), deverá entrar em contato com a CompTIA pelo e-mail examsecurity@comptia.org para confirmação.

OBSERVAÇÃO

As listas de exemplos fornecidas em formato de marcadores não são listas abrangentes. Outros exemplos de tecnologias, processos ou tarefas pertinentes a cada objetivo podem ser incluídos no exame, embora não estejam listados ou cobertos neste documento de objetivos. A CompTIA revisa constantemente o conteúdo de seus exames e atualiza as perguntas para assegurar que sejam atuais, e que a segurança das perguntas estejam protegidas. Quando necessário, publicaremos exames atualizados baseados nos objetivos do exame existentes. Lembre-se que todos os materiais de preparação dos exames ainda serão válidos.

DETALHES DO TESTE

Exame exigido	PT0-003
Número de perguntas	No máximo 90
Tipos de perguntas	Múltipla escolha e baseadas em desempenho
Duração do teste	165 minutos
Experiência recomendada	3–4 anos em uma função de analista de teste de intrusão
Pontuação de aprovação	750

OBJETIVOS DO EXAME (DOMÍNIOS)

A tabela abaixo lista os domínios avaliados por este exame e o peso que cada um representa.

DOMÍNIO		PORCENTAGEM DO EXAME
1.0	Gerenciamento de engajamento	13%
2.0	Reconhecimento e enumeração	21%
3.0	Descoberta e análise de vulnerabilidades	17%
4.0	Ataques e explorações	35%
5.0	Pós-exploração e movimento lateral	14%
Total		**100%**

1.0 Gerenciamento de engajamento

1.1 Resuma as atividades de pré-engajamento.

- Definição do escopo
  - Regulamentos, estruturas e normas
    - Privacidade
    - Segurança
  - Regras de engajamento
    - Exclusões
    - Casos de teste
    - Processo de escalonamento
    - Janela de teste
  - Tipos de acordo
    - Acordo de confidencialidade (NDA)
    - Contrato de serviço mestre (MSA)
    - Declaração de trabalho (SoW)
    - Termos de serviço (ToS)
  - Seleção de destino
    - Intervalos de Encaminhamento interdomínio sem classe (CIDR)
    - Domínios
    - Endereçamento de Protocolo de Internet (IP)
    - Localizador uniforme de recursos (URL)
  - Tipos de avaliação
    - Web
    - Rede
    - Móvel
    - Nuvem
    - Interface de programação de aplicativos (API)
    - Aplicação
    - Wireless
- Modelo de responsabilidade compartilhada
  - Responsabilidades do provedor de hospedagem
  - Responsabilidades do cliente
  - Responsabilidades do analista de teste de intrusão
  - Responsabilidades de terceiros
- Considerações legais e éticas
  - Cartas de autorização
  - Requisitos de relatórios obrigatórios
  - Risco para o analista de teste de intrusão

1.2 Explique as atividades de colaboração e comunicação.

- Análise de par
- Alinhamento das partes interessadas
- Análise de causa raiz
- Caminho de escalonamento
- Distribuição segura
- Articulação de risco, gravidade e impacto
- Repriorização de metas
- Análise do impacto nos negócios
- Aprovação do cliente

1.3 Compare e contraste estruturas e metodologias de teste.

- Manual de metodologia de teste de segurança de código aberto (OSSTMM)
- Conselho de analistas de teste de segurança ética registrados (CREST)
- Padrão de execução de teste de intrusão (PTES)
- MITRE ATT&CK
- Os 10 melhores Open Worldwide Application Security Project (OWASP)
- Padrão de verificação de segurança de aplicativos móveis OWASP (MASVS)
- Modelo Purdue
- Estruturas de modelagem de ameaças
  - Potencial de dano, reprodutibilidade, explorabilidade, usuários afetados, descoberta (DREAD)
  - Spoofing, adulteração, repúdio, divulgação de informações, negação de serviço, elevação de privilégio (STRIDE)
  - Avaliação de ameaças, ativos e vulnerabilidades operacionais críticas (OCTAVE)

1.4 Explique os componentes de um relatório de teste de intrusão.

- Alinhamento de formato
- Especificações da documentação
- Pontuação de risco
- Definições
- Componentes do relatório
  - Resumo executivo
  - Metodologia
  - Descobertas detalhadas
  - Narrativa de ataque
  - Recomendações
    - Orientação de remediação
- Limitações e suposições do teste
- Considerações sobre relatórios
  - Jurídico
  - Ética
  - Controle de qualidade (GQ)
  - Inteligência artificial (IA)

1.5 Considerando um determinado cenário, analise as descobertas e recomende a correção apropriada em um relatório.

- Controles técnicos
  - Hardening do sistema
  - Sanitizar as entradas do usuário/ parametrizar consultas
  - Autenticação multifator
  - Criptografia
  - Correção no nível do processo
  - Gerenciamento de patch
  - Rotação de chave
  - Gerenciamento de certificados
  - Solução de gerenciamento de segredos
  - Segmentação de redes
  - Controles de segurança de infraestrutura
- Controles administrativos
  - Controle de acesso baseado em função
  - Ciclo de vida de desenvolvimento de software seguro
  - Requisitos mínimos de senha
  - Políticas e procedimentos
- Controles operacionais
  - Rotatividade do trabalho
  - Restrições de horas do dia
  - Férias obrigatórias
  - Treinamento de usuário
- Controles físicos
  - Entrada de controle de acesso
  - Controles biométricos
  - Vigilância de vídeo

2.0 Reconhecimento e enumeração

2.1 Considerando um determinado cenário, aplique técnicas de coleta de informações.

- Reconhecimento ativo e passivo
- Inteligência de código aberto (OSINT)
  - Redes sociais
  - Quadros de empregos
  - Repositórios de códigos de varredura
  - Domain Name System (DNS)
    - Pesquisas de DNS
    - Pesquisas reversas de DNS
  - Páginas em cache
  - Falhas criptográficas
  - Dumping de senhas
- Reconhecimento de rede
- Varredura de protocolo
  - Varredura do Protocolo de controle de transmissão (TCP)/Protocolo de datagrama de usuário (UDP)
- Registros de transparência de certificados
- Divulgação de informações
- Análise/enumeração de mecanismos de busca
- Farejamento de rede
  - Internet das Coisas (IoT) e protocolos de tecnologia operacional (OT)
- Captura de banner
- Extração de dados de Linguagem de marcação de hipertexto (HTML)

2.2 Considerando um determinado cenário, aplique técnicas de enumeração.

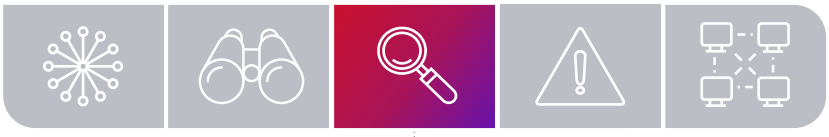
- Impressão digital do sistema operacional (SO)
- Descoberta de serviço
- Enumeração de protocolo
- Enumeração DNS
- Enumeração de diretórios
- Descoberta de host
- Enumeração de compartilhamento
- Enumeração de usuário local
- Enumeração de contas de e-mail
- Enumeração de sem fio
- Enumeração de permissão
- Enumeração de segredos
  - Chaves de acesso à nuvem
  - Senhas
  - Chaves API
  - Tokens de sessão
- Mapeamento do caminho de ataque
- Enumeração de Web application firewall (WAF)
  - Endereço de origem
- Web crawling
- Enumeração manual
  - Robots.txt
  - Mapa do site
  - Plugins de plataforma

2.3 Considerando um determinado cenário, modifique scripts para reconhecimento e enumeração.

- Coleta de informações
- Manipulação de dados
- Linguagens de script
  - Bash
  - Python
  - PowerShell
- Construções lógicas
  - Loops
  - Condicionais
  - Operador booleano
  - Operador de string
  - Operador aritmético
- Uso de bibliotecas, funções e classes

2.4 Considerando um determinado cenário, use as ferramentas apropriadas para reconhecimento e enumeração.

- 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 Descoberta e análise de vulnerabilidades

3.1 Considerando um determinado cenário, conduza a descoberta de vulnerabilidades usando várias técnicas.

- Tipos de varreduras
  - Varreduras de contêineres
    - Varreduras secundárias
  - Varreduras de aplicações
    - Teste dinâmico de segurança para aplicações (DAST)
    - Teste interativo de segurança para aplicações (IAST)
    - Análise de composição de software (SCA)
    - Teste estático de segurança para aplicações (SAST)
      - » Infraestrutura como código (IaC)
      - » Análise de código-fonte
    - Varredura móvel
  - Varreduras de rede
    - Varredura TCP/UDP
    - Varreduras furtivas
  - Varredura baseada em host
  - Verificações autenticadas vs. não autenticadas
  - Verificação de segredos
  - Sem fio
    - Verificação do Identificador de conjunto de serviços (SSID)
    - Varredura de canais
    - Varredura de intensidade do sinal
- Avaliação de vulnerabilidade dos Sistemas de controle industrial (ICS)
  - Avaliação manual
  - Espelhamento de portas
- Ferramentas
  - Nikto
  - Varredura de avaliação de vulnerabilidade Greenbone/ Open (OpenVAS)
  - TruffleHog
  - BloodHound
  - Tenable Nessus
  - PowerSploit
  - Grype
  - Trivy
  - Kube-hunter

3.2 Considerando um determinado cenário, analise a saída das fases de reconhecimento, varredura e enumeração.

- Validar resultados de varredura, reconhecimento e enumeração
  - Falsos positivos
  - Falsos negativos
  - Verdadeiros positivos
  - Completude da varredura
  - Solução de problemas de configurações de varredura
- Seleção de exploração pública
- Usar scripts para validar resultados

3.3 Explique os conceitos de segurança física.

- Tailgating
- Pesquisas de site
- Quedas do Barramento universal serial (USB)
- Clonagem de crachá
- Arrombamento de fechaduras

4.0 Ataques e explorações

4.1 Considerando um determinado cenário, analise a saída para priorizar e preparar ataques.

- **Priorização de alvos**
  - Identificação de ativos de alto valor
  - Descritores e métricas
    - Pontuação base do Sistema de pontuação de vulnerabilidade comum (CVSS)
    - Vulnerabilidades e exposições comuns (CVE)
    - Common Weakness Enumeration (CWE)
    - Sistema de pontuação de previsão de exploração (EPSS)
  - Software/sistemas em fim de vida útil
  - Configurações padrão
  - Serviços em execução
  - Métodos de criptografia vulneráveis
  - Capacidades defensivas
- **Seleção de capacidade**
  - Seleção de ferramentas
  - Seleção e personalização de explorações
    - Análise de código
  - Documentação
    - Caminho de ataque
    - Criação de diagrama de baixo nível
    - Quadro de histórias
  - Dependências
  - Consideração das limitações do escopo
  - Rotulagem de sistemas sensíveis

4.2 Considerando um determinado cenário, execute ataques de rede usando as ferramentas apropriadas.

- **Tipos de ataque**
  - Credenciais padrão
  - Ataque on-path
  - Serviços de certificação
  - Exploração de serviços mal configurados
  - Salto de rede de área local virtual (VLAN)
  - Hosts multihomed
  - Ataque de retransmissão
  - Enumeração de compartilhamento
  - Criação de pacotes
- **Ferramentas**
  - Metasploit
  - Netcat
  - Nmap
    - NSE
  - Impacket
  - CrackMapExec (CME)
  - Wireshark/tcpdump
  - msfvenom
  - Responder
  - Hydra

4.3 Considerando um determinado cenário, execute ataques de autenticação usando as ferramentas apropriadas.

- **Tipos de ataque**
  - Fadiga da autenticação multifator (MFA)
  - Ataques pass-the-hash
  - Ataques pass-the-ticket
  - Ataques pass-the-token
  - Ataques Kerberos
  - Injeção de Lightweight Directory Access Protocol (LDAP)
  - Ataques de dicionário
  - Ataques de força bruta
  - Ataques de máscara
  - Spraying de senha
  - Preenchimento de credenciais
  - Ataques OpenID Connect (OIDC)
  - Ataques de Linguagem de marcação de asserção de segurança (SAML)
- **Ferramentas**
  - CME
  - Responder
  - hashcat
  - John the Ripper
  - Hydra
  - BloodHound
  - Medusa
  - Burp Suite

4.4 Considerando um determinado cenário, execute ataques baseados em host usando as ferramentas apropriadas.

- Tipos de ataque
  - Escalação de privilégio
  - Dumping de credenciais
  - Burlar ferramentas de segurança
  - Endpoints mal configurados
  - Ofuscação de carga útil
  - Bypass de acesso controlado pelo usuário
  - Escape de shell
  - Escape de quiosque
  - Injeção de biblioteca
  - Esvaziamento e injeção de processo
  - Violação de log
  - Injeção de caminho de serviço não citado
- Ferramentas
  - Mimikatz
  - Rubeus
  - Certify
  - Seatbelt
  - PowerShell/PowerShell Integrated Scripting Environment (ISE)
  - PsExec
  - Evil-WinRM
  - Living off the land binaries (LOLbins)

4.5 Considerando um determinado cenário, execute ataques a aplicações web usando as ferramentas apropriadas.

- Tipos de ataque
  - Ataque de força bruta
  - Ataque de colisão
  - Travessia de diretórios
  - Falsificação de solicitação do lado do servidor (SSRF)
  - Cross-site request forgery (CSRF)
  - Ataque de desserialização
  - Ataques de injeção
    - Injeção de Linguagem de consulta estruturada (SQL)
    - Injeção de comando
    - Cross-site scripting (XSS)
    - Injeção de modelo do lado do servidor
  - Referência direta insegura de objeto
  - Sequestro de sessão
  - Execução de código arbitrário
  - Inclusões de arquivo
    - Inclusão de arquivo remoto (RFI)
    - Inclusão de arquivo local (LFI)
    - Web shell
  - Abuso de API
  - Manipulação de JSON Web Token (JWT)
- Ferramentas
  - TruffleHog
  - Burp Suite
  - Zed Attack Proxy (ZAP)
  - Postman
  - sqlmap
  - Gobuster/DirBuster
  - Wfuzz
  - WPScan

4.6 Considerando um determinado cenário, execute ataques baseados em nuvem usando as ferramentas apropriadas.

- Tipos de ataque
  - Ataques de serviço de metadados
  - Configurações incorretas de gerenciamento de identidade e acesso
  - Integrações de terceiros
  - Configuração incorreta de recursos
    - Segmentação de redes
    - Controles de rede
    - Credenciais de Gerenciamento de identidade e acesso (IAM)
    - Buckets de armazenamento expostos
    - Acesso público aos serviços
  - Exposição de informações de log
  - Violação de imagem e artefato
  - Ataques à cadeia de suprimentos
  - Ataques de tempo de execução de carga de trabalho
  - Escape do contêiner
  - Abuso de relação de confiança
- Ferramentas
  - Pacu
  - Docker Bench
  - Kube-hunter
  - Prowler
  - ScoutSuite
  - Ferramentas de fornecedores nativas da nuvem

4.7 Considerando um determinado cenário, execute ataques sem fio usando as ferramentas apropriadas.

- **Ataques**
  - Wardriving
  - Ataque evil twin
  - Bloqueio de sinal
  - Fusão de protocolo
  - Criação de pacotes
  - Desautenticação
  - Portal cativo
  - Ataque de número de identificação pessoal (PIN) Wi-Fi Protected Setup (WPS)
- **Ferramentas**
  - WPAD
  - WiFi-Pumpkin
  - Aircrack-ng
  - WiGLE.net
  - InSSIDer
  - Kismet

4.8 Considerando um determinado cenário, execute ataques de engenharia social usando as ferramentas apropriadas.

- **Tipos de ataque**
  - Phishing
  - Vishing
  - Whaling
  - Spearphishing
  - Smishing
  - Dumpster diving
  - Vigilância
  - Shoulder surfing
  - Tailgating
  - Eavesdropping
  - Watering hole
  - Personificação
  - Roubo de credenciais
- **Ferramentas**
  - Social Engineering Toolkit (SET)
  - Gophish
  - Evilginx
  - theHarvester
  - Maltego
  - Recon-ng
  - Browser Exploitation Framework (BeEF)

4.9 Explique ataques comuns contra sistemas especializados.

- **Tipos de ataque**
  - Ataques móveis
    - Divulgação de informações
    - Jailbreak/rooting
    - Abuso de permissão
  - Ataques de IA
    - Injeção de prompt
    - Manipulação de modelos
  - OT
    - Manipulação de registro
    - Ataque de barramento CAN
    - Ataque Modbus
    - Ataque de texto simples
    - Ataques por repetição
  - Comunicação a curta distância (NFC)
  - Bluejacking
  - Identificação de radiofrequência (RFID)
  - Spam por Bluetooth
- **Ferramentas**
  - Scapy
  - tcprelay
  - Wireshark/tcpdump
  - MobSF
  - Frida
  - Drozer
  - Android Debug Bridge (ADB)
  - Bluestrike

4.10 Considerando um determinado cenário, use scripts para automatizar ataques.

- **PowerShell**
  - PowerSploit
  - PowerView
  - PowerUpSQL
  - Pesquisa AD
- **Bash**
  - Gerenciamento de entrada/saída
  - Manipulação de dados
- **Python**
  - Impacket
  - Scapy
- **Simulação de violação e ataque (BAS)**
  - Caldera
  - Infection Monkey
  - Atomic Red Team

5.0 Pós-exploração e movimento lateral

5.1 Considerando um determinado cenário, execute tarefas para estabelecer e manter persistência.

- Tarefas agendadas/jobs do cron
- Criação de serviço
- Shell reverso
- Bind shell
- Adicionar novas contas
- Obter credenciais de conta válidas
- Chaves de registro
- Estruturas de comando e controle (C2)
- Backdoor
  - Web shell
  - Trojan
- Rootkit
- Extensões de navegador
- Violação de controles de segurança

5.2 Considerando um determinado cenário, execute tarefas para se mover lateralmente pelo ambiente.

- **Pivoting**
- **Criação de relé**
- **Enumeração**
  - Descoberta de serviço
  - Descoberta de tráfego de rede
  - Captura de credenciais adicionais
  - Dumping de credenciais
  - Pesquisas de strings

- **Descoberta de serviço**
  - Bloco de mensagem do servidor (SMB)/compartilhamentos de arquivos
  - Remote Desktop Protocol (RDP)/ Virtual Network Computing (VNC)
  - Shell Seguro (SSH)
  - Texto simples
  - LDAP
  - Chamada de procedimento remoto (RPC)
  - File Transfer Protocol (FTP)
  - Telnet
  - Hypertext Transfer Protocol (HTTP)/Hypertext Transfer Protocol Secure (HTTPS)
    - Interfaces da web
  - Line Printer Daemon (LPD)
  - JetDirect
  - RPC/Distributed Component Object Model (DCOM)
  - IDs do processo

- **Window Management Instrumentation (WMI)**
- **Window Remote Management (WinRM)**
- **Ferramentas**
  - LOLBins
    - Netstat
    - Net commands
    - cmd.exe
    - explorer.exe
    - ftp.exe
    - mmc.exe
    - rundll32
    - msbuild
    - route
    - strings/findstr.exe
  - Covenant
  - CrackMapExec
  - Impacket
  - Netcat
  - sshuttle
  - Proxychains
  - PowerShell ISE
  - Arquivos em lote
  - Metasploit
  - PsExec
  - Mimikatz

5.3 Resuma conceitos relacionados à preparação e exfiltração.

- Criptografia e compactação de arquivos
- Canal secreto
  - Esteganografia
  - DNS
  - Internet Control Message Protocol (ICMP)
  - HTTPS
- E-mail
- Recursos entre contas
- Armazenamento em nuvem
- Fluxos de dados alternativos
- Sites de armazenamento de texto
- Montagem de unidade virtual

5.4 Explique as atividades de limpeza e restauração.

- Remover mecanismos de persistência
- Reverter alterações de configuração
- Remover credenciais criadas pelo analista de teste
- Remover ferramentas
- Desativar a infraestrutura
- Preservar artefatos
- Destruição segura de dados

Lista de acrônimos CompTIA PenTest+ PT0-003

Veja abaixo uma lista de acrônimos que aparecem nos exames CompTIA PenTest+ PT0-003. Os candidatos são incentivados a rever a lista completa e a obter conhecimentos de todos os acrônimos listados como parte de um programa de preparação abrangente para o exame.

ACRÔNIMO	ESCRITO POR EXTENSO
AD	Active Directory
ADB	Android Debug Bridge
AI	Artificial Intelligence
AP	Access Point
API	Application Programming Interface
APT	Advanced Persistent Threat
BAS	Breach and Attack Simulation
BeEF	Browser Exploitation Framework
BGP	Border Gateway Protocol
BIA	Business Intelligence Analytics
C2	Command and Control
CI/CD	Continuous Integration/Continuous Delivery
CIDR	Classless Inter-domain Routing
CGI	Common Gateway Interface
CLI	Command-line Interface
CME	CrackMapExec
CNAME	Canonical Name
COFF	Common Object File Format
CREST	Council of Registered Ethical Security Testers
CSRF	Cross-site Request Forgery
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
CWE	Common Weakness Enumeration
DAST	Dynamic Application Security Testing
DCOM	Distributed Component Object Model
DDos	Distributed Denial of Service
DMARC	Domain-based Message Authentication, Reporting, and Conformance
DNS	Domain Name System
DoS	Denial of Service
DREAD	Damage potential, Reproducibility, Exploitability, Affected users, Discoverability
DROWN	Decrypting RSA [Rivest-Shamir-Adleman] with Obsolete and Weakened Encryption
EFSRPC	Encrypting File System Remote Protocol
ELF	Executable and Linkable Format
EPSS	Exploit Prediction Scoring System
EXIF	Exchangeable Image File Format
FQDN	Fully Qualified Domain Name
FTP	File Transfer Protocol

ACRÔNIMO	ESCRITO POR EXTENSO
GIF	Graphic Interchange Format
HID	Host-based Intrusion Detection
HSTS	HTTP Strict Transport Security
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IaC	Infrastructure as Code
IAM	Identity and Access Management
IAST	Interactive Application Security Testing
ICMP	Internet Control Message Protocol
ICS	Industrial Control System
IDOR	Insecure DIrect Object Reference
IdP	Identity Provider
IDS	Intrusion Detection System
IGRP	Interior Gateway Routing Protocol
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrustion Prevention System
ISE	Integrated Scripting Environment
JWT	JSON Web Token
KDC	Key Distribution Center
KRBTGT	Kerberos Ticket Granting Ticket
LDAP	Lightweight Directory Access Protocol
LFI	Local File Inclusion
LLMNR	Link-local Multicast Name Resolution
LOLBins	Living off the Land Binaries
LPD	Line Printer Daemon
LSASS	Local Security Authority Subsystem Service
MAC	Media Access Control
MASVS	Mobile Application Security Verification Standard
MFA	Multifactor Authentication
MIB	Management Information Base
MMS	Multimedia Messaging Service
MSA	Master Services Agreement
MX	Mail Exchange
NDA	Non-disclosure Agreement
NFC	Near-field Communication
NSE	Nmap Scripting Engine
NTLM	New Technology LAN Manager
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
OIDC	OpenID Connect
OpenVAS	Open Vulnerability Assessment Scanner
OS	Operating System
OSINT	Open-source Intelligence
OSSTMM	Open-source Security Testing Methodology Manual
OT	Operational Technology
OWASP	Open Worldwide Application Security Project
PTES	Penetration Testing Execution Standard
PWS	Performance Work Statement
QC	Quality Control
RCE	Remote Code Execution
RDP	Remote Desktop Protocol
RFI	Remote File Inclusion
RFID	Radio Frequency Identification

ACRÔNIMO	ESCRITO POR EXTENSO
RIP	Routing Information Protocol
RPC	Remote Procedure Call
SaaS	Software as a Service
SAM	Security Account Manager
SAML	Security Assertion Markup Language
SAST	Static Application Security Testing
SCA	Software Composition Analysis
SCADA	Supervisory Control and Data Acquisition
SDK	Software Development Kit
SDLC	Software Development Life Cycle
SDR	Software-defined Radio
SET	Social Engineering Toolkit
SIEM	Security Information and Event Management
SMB	Server Message Block
SMS	Short Message Service
SNMP	Simple Network Management Protocol
SOA	Start of Authority
SOC	Security Operations Center
SoW	Statement of Work
SPN	Service Principal Name
SQL	Structured Query Language
SQLi	Structured Query Language Injection
SSH	Secure Shell
SSID	Service Set Identifier
SSL	Secure Socket Layer
SSO	Single Sign-on
SSRF	Server-side Request Forgery
STRIDE	Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege
TCP	Transmission Control Protocol
TGS	Ticket Granting Service
TLS	Transport Layer Security
ToS	Terms of Service
TTP	Techniques, Tactics, Procedures
UDP	User Datagram Protocol
URL	Uniform Resource Locator
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
VNC	Virtual Network Computing
VPN	VIrtual Private Network
WAF	Web Application Firewall
WinRM	Windows Remote Management
WLAN	Wireless Local Area Network
WMI	Windows Management Instrumentation
WPAD	Web Proxy Auto Discovery
WPS	Wi-Fi Protected Setup
XSS	Cross-site Scripting
ZAP	Zed Attack Proxy

Lista de hardware e software propostos para o PenTest+

**A CompTIA incluiu esta lista de exemplos de hardware e software para ajudar os candidatos a se prepararem para o exame PenTest+. Esta lista também pode ser útil para as empresas de treinamento que pretendam criar um componente laboratorial para sua oferta de treinamento. As listas com marcadores abaixo de cada tópico são listas de exemplo e não são exaustivas.

HARDWARE

- Computadores
- Pontos de acesso sem fio
- Servidores
- Switches
- Cabeamento
- Firewalls
- Roteador
- Detecção de intrusão baseada em host (HID)/controles de acesso de porta
- Adaptadores sem fio compatíveis com injeção de pacotes
- Antena direcional
- Dispositivo móvel
- Equipamento de IoT (câmeras, microcomputador, TV smart, etc.)
- Adaptador Bluetooth
- Impressoras multifuncionais (com fio/sem fio)
- Equipamento de clonagem NFC/RFID
- Kit de arrombamento de fechadura (quando aplicável)
- Dispositivo biométrico
- Controlador lógico programável
  - Kit de rádio definido por software (SDR)
- Unidades flash USB

SOFTWARE

- Acesso ao ambiente de nuvem
  - Acesso à interface de linha de comando (CLI)
  - Acesso ao console de gerenciamento
  - Instâncias de serviços em nuvem
- Licenciamento do SO
- SO de código aberto
- Frameworks de teste de intrusão
- Software de máquina virtual
- Ferramentas de varredura
  - Ferramentas de varredura de vulnerabilidade
  - SAST
  - DAST
- Ferramentas de teste de credenciais
  - Ferramentas de spraying
  - Cracking de senha
- Ferramentas de segurança de aplicações
- Depuradores
- Ferramentas de teste sem fio
- Ferramentas de proxy web
- Ferramentas de engenharia social
- Ferramentas de acesso remoto
- Ferramentas de rede
  - Analisadores de protocolo
  - Ferramentas de sniffing
- Ferramentas de teste de mobilidade
- Gerenciamento de informações e eventos de segurança (SIEM)/ sistema de detecção de intrusão (IDS)/sistema de prevenção de intrusão (IPS)/ferramentas de segurança de endpoint
- Ferramentas C2

CompTIA