Objetivos do Exame de Certificação CompTIA PenTest+

NÚMERO DO EXAME: PT0-002

Sobre o exame

Os candidatos são incentivados a usar este documento a fim de se prepararem para o exame de certificação CompTIA PenTest+ (PT0-002). O exame de certificação CompTIA PenTest+ (PT0-002) verificará se o candidato tem o conhecimento e as habilidades necessárias para:

- **Planejar e definir o escopo de um engajamento de teste de intrusão**
- **Compreender os requisitos legais e de conformidade**
- **Realizar verificação de vulnerabilidades e testes de intrusão usando ferramentas e técnicas apropriadas e, depois, analisar os resultados**
- **Produzir um relatório escrito contendo técnicas de correção propostas, comunicar efetivamente os resultados à equipe de gerenciamento e fornecer recomendações práticas**

Isso equivale de três a quatro anos de experiência prática trabalhando em um cargo de consultor de segurança ou analista de teste de intrusão.

Esses exemplos de conteúdo destinam-se a esclarecer os objetivos do exame, portanto, não devem ser considerados como uma lista completa de todo o conteúdo deste exame.

ACREDITAÇÃO DO EXAME

O exame CompTIA PenTest+ (PT0-002) é credenciado pela ANSI para demonstrar conformidade com a norma ISO 17024 e, devido a isso, passa por revisões e atualizações regulares dos objetivos do exame.

ELABORAÇÃO DO EXAME

Os exames CompTIA são provenientes de seminários especializados e focados no assunto e pesquisas abrangentes em todo o setor quanto às habilidades e conhecimentos exigidos de um profissional de TI.

POLÍTICA DE USO DE MATERIAIS AUTORIZADOS 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 a todos os candidatos a 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 a 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 obter 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 questões para assegurar que sejam atuais e que a segurança de suas perguntas esteja protegida. Quando necessário, publicaremos exames atualizados baseados nos objetivos existentes. Lembre-se que todos os materiais de preparação dos exames ainda serão válidos.

DETALHES DO TESTE

Exame exigido	PT0-002
Número de questões	No máximo 85
Tipos de perguntas	Múltipla escolha e baseadas em desempenho
Duração do teste	165 minutos
Experiência recomendada	3-4 anos de experiência prática realizando testes de intrusão, avaliações de vulnerabilidade, e análise de código
Pontuação de aprovação	750 (em uma escala de 100 a 900)

OBJETIVOS DO EXAME (DOMÍNIOS)

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

DOMÍNIO	PORCENTAGEM DO EXAME
1.0 Planejamento e escopo	14%
2.0 Coleta de informações e verificação de vulnerabilidades	22%
3.0 Ataques e explorações	30%
4.0 Relatórios e comunicação	18%
5.0 Ferramentas e análise de código	16%
Total	**100%**

1.0 Planejamento e escopo

1.1 Compare e diferencie os conceitos de governança, risco e conformidade.

- **Considerações de conformidade regulatória**
  - Payment Card Industry Data Security Standard (PCI DSS)
  - General Data Protection Regulation (GDPR)
- **Restrições de localização**
  - Limitações do país
  - Restrições de ferramentas
  - Legislações locais
  - Requisitos do governo local
    - Requisitos de privacidade
- **Conceitos jurídicos**
  - Service-level agreement (SLA)
  - Sigilo
  - Declaração de trabalho
  - Non-disclosure agreement (NDA)
  - Principal contrato de serviços
- **Permissão para atacar**

1.2 Explique a importância do escopo e dos requisitos organizacionais e/ou do cliente.

- **Padrões e metodologias**
  - MITRE ATT&CK
  - Open Web Application Security Project (OWASP)
  - National Institute of Standards and Technology (NIST)
  - Open-source Security Testing Methodology Manual (OSSTMM)
  - Penetration Testing Execution Standard (PTES)
  - Information Systems Security Assessment Framework (ISSAF)
- **Regras de engajamento**
  - Horário
  - Tipos de testes permitidos/ não permitidos
  - Outras restrições
- **Considerações do ambiente**
  - Rede
  - Aplicação
  - Nuvem
- **Lista de alvos/ativos no escopo**
  - Redes sem fio
  - Faixas de protocolo de Internet (IP)
  - Domínios
  - Application programming interfaces (APIs)
  - Localidades fisicas
  - Domain name system (DNS)
  - Alvos externos x internos
  - Hospedagem própria x hospedagem de terceiros
- **Validar o escopo do engajamento**
  - Questionar o cliente/revisar contratos
  - Gerenciamento de tempo
  - Estratégia
    - Teste de ambiente desconhecido x ambiente conhecido

1.3 Em um determinado cenário, demonstre uma mentalidade ética de hackers, mantendo o profissionalismo e a integridade.

- **Verificações de antecedentes da equipe de testes de intrusão**
- **Aderir ao escopo específico de engajamento**
- **Identificar atividade criminosa**
- **Denunciar imediatamente violações/ atividade criminosa**
- **Limitar o uso de ferramentas a um engajamento específico**
- **Limitar a intrusão com base no escopo**
- **Manter a confidencialidade dos dados/informações**
- **Riscos para o profissional**
  - Taxas/multas
  - Acusações criminais

2.0 Coleta de informações e verificação de vulnerabilidades

2.1 Em um determinado cenário, realize o reconhecimento passivo.

- **Pesquisas de DNS**
- **Identificar contatos técnicos**
- **Contatos do administrador**
- **Nuvem x hospedado internamente**
- **Varredura de redes sociais**
  - Principais contatos/ responsabilidades do trabalho
  - Lista de empregos/tecnologias
- **Falhas criptográficas**
  - Certificados SSL (Secure Sockets Layer)
  - Revogação
- **Reputação da empresa/postura de segurança**
- **Dados**
  - Dumping de credenciais
  - Metadados do arquivo
  - Análise/enumeração estratégica de mecanismos de busca
  - Arquivo/cache do site
  - Repositórios de código-fonte públicos
- **Open-source intelligence (OSINT)**
  - Ferramentas
    - Shodan
    - Recon-ng
  - Fontes
    - Common weakness enumeration (CWE)
    - Common vulnerabilities and exposures (CVE)

2.2 Em um determinado cenário, realize o reconhecimento ativo.

- **Enumeração**
  - Hosts
  - Serviços
  - Domínios
  - Usuários
  - Uniform resource locators (URLs)
- **Reconhecimento do site**
  - Rastreamento de sites
  - Varredura de sites
  - Inspeção manual de links da web
    - robots.txt
- **Criação de pacotes**
  - Scapy
- **Detecção de defesa**
  - Detecção do balanceador de carga
  - Detecção de Web application firewall (WAF)
  - Antivírus
  - Firewall
- **Tokens**
  - Escopo
  - Emissão
  - Revogação
- **Wardriving**
- **Tráfego de rede**
  - Capturar solicitações e respostas da API
  - Sniffing
- **Descoberta de ativos na nuvem**
- **Serviços hospedados por terceiros**
- **Prevenção de detecção**

2.3 Em um determinado cenário, analise os resultados de um exercício de reconhecimento.

- **Impressão digital**
  - Sistemas operacionais (SOs)
  - Redes
  - Dispositivos de rede
  - Software
- **Analisar a saída de:**
  - Pesquisas de DNS
  - Rastreamento de sites
  - Tráfego de rede
  - Tráfego de Address Resolution Protocol (ARP)
  - Verificações de Nmap
  - Registros da web

2.4 Em um determinado cenário, realize a verificação de vulnerabilidades.

- **Considerações sobre a verificação de vulnerabilidades**
  - Horário para executar verificações
  - Protocolos
  - Topologia de rede
  - Limitações de largura de banda
  - Limitação de consultas
  - Sistemas frágeis
  - Ativos não tradicionais
- **Verificar alvos identificados em busca de vulnerabilidades**
- **Definir as configurações de verificação para evitar a detecção**
- **Métodos de verificação**
  - Escaneamento furtivo
  - Verificação de conexão de Transmission Control Protocol (TCP)
  - Com credencial x sem credencial
- **Nmap**
  - Scripts de Nmap Scripting Engine (NSE)
  - Opções comuns
    - -A
    - -sV
    - -sT
    - -Pn
    - -O
    - -sU
    - -sS
    - -T 1-5
    - -script=vuln
    - -p
- **Ferramentas de teste de vulnerabilidade que facilitam a automação**

3.0 Ataques e explorações

3.1 Em um determinado cenário, pesquise vetores de ataque e execute ataques de rede.

- **Teste de estresse para disponibilidade**
- **Explorar recursos**
  - Exploit database (DB)
  - Packet storm
- **Ataques**
  - ARP poisoning
  - Encadeamento de exploração
  - Ataques a senhas
    - Password spraying
    - Hash cracking
    - Força bruta
    - Dicionário
  - On-path (anteriormente conhecido como man-in-the-middle)
  - Kerberoasting
  - DNS cache poisoning
  - Virtual local area network (VLAN) hopping
  - Contorno de Network access control (NAC)
  - Falsificação de Media access control (MAC)
  - Poisoning de Link-Local Multicast Name Resolution (LLMNR)/ NetBIOS-Name Service (NBT-NS)
  - Ataques de retransmissão de New Technology LAN Manager (NTLM)
- **Ferramentas**
  - Metasploit
  - Netcat
  - Nmap

3.2 Em um determinado cenário, pesquise vetores de ataque e execute ataques às redes sem fio.

- **Métodos de ataque**
  - Eavesdropping
  - Modificação de dados
  - Corrupção de dados
  - Ataques de retransmissão
  - Spoofing
  - Desautenticação
  - Jamming
  - Capturar handshakes
  - On-path
- **Ataques**
  - Evil twin
  - Captive portal
  - Bluejacking
  - Bluesnarfing
  - Clonagem de Radio-frequency identification (RFID)
  - Ataque de Bluetooth Low Energy (BLE)
  - Ataques de amplificação (Near-field communication (NFC))
  - Ataque de PIN de WiFi protected setup (WPS)
- **Ferramentas**
  - Aircrack-ng suite
  - Antena amplificada

3.3 Em um determinado cenário, pesquise vetores de ataque e execute ataques baseados em aplicativos.

- **OWASP Top 10**
- **Server-side request forgery**
- **Falhas na lógica de negócios**
- **Ataques de injeção**
  - Injeção de Structured Query Language (SQL)
    - Blind SQL
    - Boolean SQL
    - Aninhamento de consultas
  - Injeção de comando
  - Cross-site scripting
    - Persistente
    - Refletido
  - Injeção de Lightweight Directory Access Protocol (LDAP)
- **Vulnerabilidades de aplicações**
  - Condições de corrida
  - Falta de manuseio de erro
  - Falta de assinatura de código
  - Transmissão de dados insegura
  - Ataques de sessão
    - Sequestro de sessão
    - Cross-site request forgery (CSRF)
    - Escalação de privilégio
    - Repetição de sessão
    - Fixação de sessão
- **Ataques à API**
  - Restful
  - Extensible Markup Language-Remote Procedure Call (XML-RPC)
  - Soap
- **Directory traversal**
- **Ferramentas**
  - Proxies web
    - OWASP Zed Attack Proxy (ZAP)
    - Burp Suite community edition
  - SQLmap
  - DirBuster
- **Recursos**
  - Listas de palavras

3.4 Em um determinado cenário, pesquise vetores de ataque e execute ataques em tecnologias de nuvem.

- **Ataques**
  - Roubo de credenciais
  - Escalação de privilégio
  - Account takeover
  - Ataque de serviço de metadados
  - Ativos de nuvem mal configurados
    - Identity and access management (IAM)
    - Configurações incorretas de federação
    - Armazenamento de objetos
    - Tecnologias de conteinerização
  - Esgotamento de recursos
  - Ataques de injeção de malware na nuvem
  - Ataques de negação de serviço
  - Side-channel attacks
  - Ataques diretos à origem
- **Ferramentas**
  - Software development kit (SDK)

3.5 Explique ataques e vulnerabilidades comuns contra sistemas especializados.

- **Móvel**
  - Ataques
    - Engenharia reversa
    - Análise de sandbox
    - Envio de spam
  - Vulnerabilidades
    - Armazenamento inseguro
    - Vulnerabilidades de senha
    - Fixação de certificado
    - Uso de componentes vulneráveis conhecidos
    - (i) Vulnerabilidades de dependência
    - (ii) Fragmentação de patches
    - Execução de atividades usando root
    - Excesso de permissões
    - Integrações de biometria
    - Vulnerabilidades de lógica de negócios
  - Ferramentas
    - Burp Suite
    - Drozer
    - Mobile Security Framework (MobSF)
    - Postman
    - Ettercap
    - Frida
    - Objection
    - Android SDK tools
    - ApkX
    - APK Studio
- **Dispositivos de Internet das Coisas (IoT)**
  - Ataques BLE
  - Considerações especiais
    - Ambiente frágil
    - Preocupações com a disponibilidade
    - Corrupção de dados
    - Extração de dados
  - Vulnerabilidades
    - Padrões inseguros
    - Comunicação em texto simples
    - Configurações codificadas
    - Firmware/hardware desatualizado
    - Vazamento de informações
    - Uso de componentes inseguros ou desatualizados
- **Vulnerabilidades do sistema de armazenamento de dados**
  - Configurações incorretas — no local e baseadas em nuvem
    - Nome de usuário/senha padrão/em branco
    - Exposição da rede
    - Falta de sanitização de entradas do usuário
    - Vulnerabilidades de software subjacentes
    - Mensagens de erro e manuseio de depuração
    - Vulnerabilidades de injeção
      - Single quote method
- **Vulnerabilidades da interface de gerenciamento**
  - Intelligent platform management interface (IPMI)
- **Vulnerabilidades relacionadas a Supervisory Control and Data Acquisition (SCADA)/ Industrial Internet of Things (IIoT)/ Industrial Control System (ICS)**
- **Vulnerabilidades relacionadas a ambientes virtuais**
  - Fuga de Virtual machine (VM)
  - Vulnerabilidades do hipervisor
  - Vulnerabilidades do repositório de VM
- **Vulnerabilidades relacionadas a cargas de trabalho conteinerizadas**

3.6 Em um determinado cenário, realize uma engenharia social ou ataque físico.

- **Pretexto para uma abordagem**
- **Ataques de engenharia social**
  - E-mail de phishing
    - Whaling
    - Spear phishing
  - Vishing
  - Phishing de Short Message Service (SMS)
  - Universal Serial Bus (USB) drop key
  - Ataque watering hole
- **Ataques físicos**
  - Tailgating
  - Dumpster diving
  - Shoulder surfing
  - Clonagem de cartão
- **Personificação**
- **Ferramentas**
  - Browser exploitation framework (BeEF)
  - Kit de ferramentas de engenharia social
  - Ferramentas de falsificação de chamadas
- **Métodos de influência**
  - Autoridade
  - Escassez
  - Prova social
  - Urgência
  - Semelhança
  - Medo

3.7 Em um determinado cenário, execute técnicas de pós-exploração.

- **Ferramentas de pós-exploração**
  - Empire
  - Mimikatz
  - BloodHound
- **Movimentação lateral**
  - Pass the hash
- **Teste de segmentação de rede**
- **Escalação de privilégio**
  - Horizontal
  - Vertical
- **Escalação de um shell restritivo**
- **Criação de um ponto de apoio/ persistência**
  - Trojan
  - Backdoor
    - Bind shell
    - Shell reversa
  - Daemons
  - Tarefas agendadas
- **Prevenção de detecção**
  - Técnicas Living-off-the-land/ fileless malware
    - PsExec
    - Windows Management Instrumentation (WMI)
    - PowerShell (PS) remoting/ Windows Remote Management (WinRM)
  - Extração de dados
  - Ocultação dos rastros
  - Esteganografia
  - Estabelecimento de um canal secreto
- **Enumeração**
  - Usuários
  - Grupos
  - Florestas
  - Dados confidenciais
  - Arquivos não criptografados

4.0 Relatórios e comunicação

4.1 Compare e diferencie componentes importantes de relatórios escritos.

- **Relato público**
  - C-suite (Diretoria)
  - Partes interessadas de terceiros
  - Equipe técnica
  - Desenvolvedores
- **Conteúdo do relatório (** não em uma determinada ordem)**
  - Resumo executivo
  - Detalhes do escopo
  - Metodologia
    - Narrativa de ataque
  - Descobertas
    - Classificação de risco (estrutura de referência)
    - Priorização de risco
    - Análise do impacto nos negócios
  - Métricas e medidas
  - Remediação
  - Conclusão
  - Anexos
- **Tempo de armazenamento para relatório**
- **Distribuição segura**
- **Fazer anotações**
  - Documentação contínua durante o teste
  - Capturas de tela
- **Temas comuns/Causas raízes**
  - Vulnerabilidades
  - Observações
  - Falta de boas práticas

4.2 Em 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 implementada
  - Criptografar senhas
  - Correção no nível do processo
  - Gerenciamento de patch
  - Rotação de chave
  - Gerenciamento de certificados
  - Solução de gerenciamento de segredos
  - Segmentação de redes
- **Controles administrativos**
  - Controle de acesso com base em funções
  - Ciclo de vida de desengajamento de software seguro
  - Requisitos mínimos de senha
  - Políticas e procedimentos
- **Controles operacionais**
  - Rotatividade do trabalho
  - Restrições do horário
  - Férias obrigatórias
  - Treinamento de usuário
- **Controles físicos**
  - Controle de acesso
  - Controles biométricos
  - Vigilância de vídeo

4.3 Explique a importância da comunicação durante o processo de teste de intrusão.

- **Caminho de comunicação**
  - Contato principal
  - Contato técnico
  - Contato de emergência
- **Acionadores de comunicação**
  - Descobertas críticas
  - Relatórios de status
  - Indicadores de comprometimento anterior
- **Motivos da comunicação**
  - Percepção situacional
  - Desescalada
  - Desconflito
  - Identificação de falsos positivos
  - Atividade criminal
- **Redefinição de metas**
- **Apresentação das descobertas**

4.4 Explique as atividades de entrega pós-relatório.

- **Limpeza pós-engajamento**
  - Remoção de shells
  - Remoção de credenciais criadas pelo analista
  - Remoção das ferramentas
- **Aprovação do cliente**
- **Lições aprendidas**
- **Ações de acompanhamento/reteste**
- **Declaração das descobertas**
- **Processo de destruição de dados**

5.0 Ferramentas e análise de código

5.1 Explique os conceitos básicos de scripting e desengajamento de software.

- **Construções lógicas**
  - Loops
  - Condicionais
  - Operador booleano
  - Operador de string
  - Operador aritmético
- **Estruturas de dados**
  - JavaScript Object Notation (JSON)
  - Chave principal
  - Conjuntos
  - Dicionários
  - Comma-separated values (CSV)
  - Listas
  - Árvores
- **Bibliotecas**
- **Classes**
- **Procedimentos**
- **Funções**

5.2 Em um determinado cenário, analise um script ou amostra de código para uso em um teste de intrusão.

- **Shells**
  - Bash
  - PS
- **Linguagens de programação**
  - Python
  - Ruby
  - Perl
  - JavaScript
- **Analisar o código de exploração para:**
  - Baixar arquivos
  - Iniciar acesso remoto
  - Enumerar usuários
  - Enumerar ativos
- **Oportunidades de automação**
  - Automatizar o processo de teste de intrusão
    - Executar a varredura de portas e automatizar próximas etapas com base nos resultados
    - Verificar as configurações e produzir um relatório
  - Script para modificar endereços IP durante um teste
  - Script do Nmap para enumerar cifras e produzir relatórios

5.3 Explique os casos de uso das seguintes ferramentas durante as fases de um teste de intrusão.

*(**A intenção deste objetivo NÃO é testar conjuntos de recursos de fornecedores específicos.)*

- **Scanners**
  - Nikto
  - Open vulnerability assessment scanner (Open VAS)
  - SQLmap
  - Nessus
  - Open Security Content Automation Protocol (SCAP)
  - Wapiti
  - WPScan
  - Brakeman
  - Scout Suite
- **Ferramentas de teste de credenciais**
  - Hashcat
  - Medusa
  - Hydra
  - CeWL
  - John the Ripper
  - Cain
  - Mimikatz
  - Patator
  - DirBuster
- **Depuradores**
  - OllyDbg
  - Immunity Debugger
  - GNU Debugger (GDB)
  - WinDbg
  - Interactive Disassembler (IDA)
  - Covenant
  - SearchSploit
- **OSINT**
  - WHOIS
  - Nslookup
  - Fingerprinting Organization with Collected Archives (FOCA)
  - theHarvester
  - Shodan
  - Maltego
  - Recon-ng
  - Censys
- **Wireless**
  - Aircrack-ng suite
  - Kismet
  - Wifite2
  - Rogue access point
  - EAPHammer
  - mdk4
  - Spooftooph
  - Reaver
  - Wireless Geographic Logging Engine (WiGLE)
  - Fern
- **Ferramentas de aplicações web**
  - OWASP ZAP
  - Burp Suite
  - Gobuster
  - w3af
- **Ferramentas de engenharia social**
  - Social Engineering Toolkit (SET)
  - BeEF
- **Ferramentas de acesso remoto**
  - Secure Shell (SSH)
  - Ncat
  - Netcat
  - ProxyChains
- **Ferramentas de rede**
  - Wireshark
  - Hping
- **Misc.**
  - SearchSploit
  - Responder
  - Impacket tools
  - Empire
  - Metasploit
  - mitm6
  - CrackMapExec
  - TruffleHog
  - Censys
- **Ferramentas de esteganografia**
  - Openstego
  - Steghide
  - Snow
  - Coagula
  - Sonic Visualiser
  - TinEye
- **Ferramentas de nuvem**
  - Scout Suite
  - CloudBrute
  - Pacu
  - Cloud Custodian

Lista de acrônimos para PenTest+ (PT0-002)

Veja abaixo uma lista de acrônimos que aparecem nos exames CompTIA PenTest+. 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
AAA	Authentication, Authorization and Accounting
ACL	Access Control List
AES	Advanced Encryption Standard
AP	Access Point
API	Application Programming Interface
APT	Advanced Persistent Threat
ARP	Address Resolution Protocol
AS2	Applicability Statement 2
BeEF	Browser Exploitation Framework
BLE	Bluetooth Low Energy
BSSID	Basic Service Set Identifiers
CA	Certificate Authority
CAPEC	Common Attack Pattern Enumeração e classificação
CLI	Command-Line Interface
CSRF	Cross-Site Request Forgery
CSV	Comma-Separated Values
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring Systems
CWE	Common Weakness Enumeration
DB	Database
DDoS	Distributed Denial-of-Service
DHCP	Dynamic Host Configuration Protocol
DLL	Dynamic Link Library
DLP	Data Loss Prevention
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
EAP	Extensible Authentication Protocol
FOCA	Fingerprinting Organization with Collected Archives
FTP	File Transfer Protocol
FTPS	File Transfer Protocol Secure
GDB	GNU Debugger
GDPR	General Data Protection Regulation
GPU	Graphics Processing Unit
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure

ACRÔNIMO	ESCRITO POR EXTENSO
IaaS	Infrastructure as a Service
IAM	Identity and Access Management
ICMP	Internet Control Message Protocol
ICS	Industrial Control System
IDA	Interactive Disassembler
IDS	Intrusion Detection System
IIoT	Industrial Internet of Things
IMEIs	International Mobile Equipment Identity
IoT	Internet of Things
IP	Internet Protocol
IPMI	Intelligent Platform Management Interface
IPS	Intrusion Prevention System
ISO	International Organization for Standardization
ISP	Internet Service Provider
ISSAF	Information Systems Security Assessment Framework
JSON	JavaScript Object Notation
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LLMNR	Link-Local Multicast Name Resolution
LSASS	Local Security Authority Subsystem Service
MAC	Media Access Control
MDM	Mobile Device Management
MobSF	Mobile Security Framework
MOU	Memorandum of Understanding
MSA	Master Service Agreement
MX	Mail Exchange
NAC	Network Access Control
NBT-NS	NetBIOS Name Service
NDA	Non-disclosure Agreement
NFC	Near-Field Communication
NIST	National Institute of Standards and Technology
NIST SP	National Institute of Standards and Technology Special Publication
NS	Name Server
NSE	Nmap Scripting Engine
NTLM	New Technology LAN Manager

ACRÔNIMO	ESCRITO POR EXTENSO
NTP	Network Time Protocol
OS	Operating System
OSINT	Open-source Intelligence
OSSTMM	Open-source Security Testing Methodology Manual
OWASP	Open Web Application Security Project
PBKDF2	Password-Based Key Deviation Function 2
PCI DSS	Payment Card Industry Data Security Standard
PHP	PHP: Hypertext Preprocessor
PII	Personal Identifiable Information
PKI	Public Key Infrastructure
PLC	Programmable Logic Controller
PS	PowerShell
PSK	Pre-Shared Key
PTES	Penetration Testing Execution Standard
RAT	Remote Access Trojan
RDP	Remote Desktop Protocol
RF	Radio Frequency
RFC	Request for Comment
RFID	Radio-Frequency Identification
ROE	Rules of Engagement
SCADA	Supervisory Control and Data Acquisition
SCAP	Security Content Automation Protocol
SDK	Software Development Kit
SDLC	Software Development Life Cycle
SDR	Software-defined Radio
SET	Social Engineering Toolkit
SGID	Set Group ID
SIEM	Security Information and Event Management
SIP	Session Initiation Protocol
SLA	Service-level Agreement
SMB	Server Message Block
S/MIME	Secure/Multipurpose Internet Mail Extensions
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOC	Security Operations Center
SOW	Statement of Work
SQL	Structured Query Language
SSD	Solid-State Drive
SSH	Secure Shell
SSHD	Solid-State Hybrid Drive
SSID	Service Set Identifier
SSL	Secure Sockets Layer
SSO	Single Sign-On
SUID	Definir ID de usuário (Set User ID)
TCP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TTL	Time to Live
TTPs	Tactics, Techniques and Procedures
UDP	User Datagram Protocol

ACRÔNIMO	ESCRITO POR EXTENSO
URL	Uniform Resource Locator
URI	Uniform Resource Identifier
USB	Universal Serial Bus
UTF	Unicode Transformation Format
VAS	Vulnerability Assessment Scanner
VLAN	Virtual Local Area Network
VM	Virtual Machine
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
VPS	Virtual Private Server
WAF	Web Application Firewall
WEP	Wired Equivalent Privacy
WiGLE	Wireless Geographic Logging Engine
WinRM	Windows Remote Management
WMI	Windows Management Instrumentation
WPA	Wi-Fi Protected Access
WPS	Wi-Fi Protected Setup
XML-RPC	Extensible Markup Language-Remote Procedure Call
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 desejam criar um componente laboratorial para sua oferta de treinamento. As listas com marcadores abaixo de cada tópico são listas de exemplo e não são definitivas.

EQUIPAMENTO

- Notebooks
- Pontos de acesso sem fio
- Servidores
- Unidades de processamento gráfico (GPUs)
- Switches
- Cabos
- Monitores
- Firewalls
- Controles de acesso HID/porta
- Adaptadores sem fio compatíveis com injeção de pacotes
- Antena direcional
- Dispositivo móvel
- Equipamento de IoT (câmeras, Raspberry Pi, TV smart, etc.)
- Adaptador Bluetooth
- Acesso ao ambiente de nuvem
  - Acesso à interface de linha de comando (CLI)
  - Acesso ao console de gerenciamento
  - Instâncias de serviços em nuvem
- Impressoras multifuncionais (com fio/sem fio)
- Impressora associada ao domínio
- Leitores RFID
- Dispositivo biométrico
- Controlador lógico programável
  - Kit de rádio definido por software (SDR)
- Unidades flash USB
  - Unidade USB bélica

EQUIPAMENTOS DE REPOSIÇÃO

- Cabos
- Teclados
- Mouse
- Fontes de energia
- Adaptadores

PEÇAS DE REPOSIÇÃO

- Cabos HDMI
- Discos rígidos
- Monitores de reposição

FERRAMENTAS

- Ferramentas de chaveiro
- Clonagem de cartão
- Identificador de impressão digital
- Esmalte (para ocultar as impressões digitais)

SOFTWARE

- Licenciamento do SO
- SO de código aberto
- Framework de teste de intrusão
- Software de virtualização
- Ferramentas de verificação
- Ferramentas de teste de credenciais
  - Ferramentas de spraying
  - Cracking de senha
- Depuradores
- Ferramentas de fuzzing
- Ferramentas de qualidade de software
- Ferramentas de teste sem fio
- Ferramentas de proxy web
- Ferramentas de engenharia social
- Ferramentas de acesso remoto
- Ferramentas de rede
- Ferramentas de teste de mobilidade
- Sistema de informações de segurança e gerenciamento de eventos (SIEM)/ sistema de detecção de intrusão (IDS)/ sistema de prevenção de intrusão (IPS)
- Ferramentas de comando e controle
- Ferramentas de detecção e prevenção

CompTIA