

PENTEST + CEH

Análise de Vulnerabilidade e Pentest

PENTEST E ANÁLISE DE VULNERABILIDADES

SOBRE O CURSO:

A área de segurança da informação nunca este tão em evidência. Você fez tudo o que pôde para garantir logicamente seus sistemas, juntamente com a camada de educação do usuário e segurança física. No entanto, a única maneira de saber se as suas defesas serão efetivas é testá-las. O Curso PenTest aborda uma das habilidades mais importantes de qualquer profissional de segurança de TI: testes de invasão.

O Curso de Pentest/ Análise de Vulnerabilidades tem por objetivo é ensinar técnicas e ferramentas que são usadas por hackers, crackers, auditores de segurança e profissionais em testes de invasão em redes. Dessa forma o aluno aprende de forma prática como aplicar o conhecimento adquirido para fortalecer a rede interna, realizando testes de intrusão e análise de vulnerabilidades de maneira ética e profissional.

Ao decorrer deste treinamento o aluno estará totalmente apto à:

– Fazer um Pentest na Rede;
– Identificar Vulnerabilidade e Mitigar Vulnerabilidades;
– Atuar como Red Team.
– Entrega de Relatório.

CARGA HORÁRIA:

60 Horas**.**
Sendo **4 horas** 100% com foco na prova **CEH.**

APÓS ESTE CURSO VOCÊ ESTARÁ APTO A:

- ✓ **Realizar um Pentest de forma profissional.**
- ✓ Atuar na área de segurança da informação.
- ✓ **Mapear as vulnerabilidades em sistemas, dispositivos e serviços.**
- ✓ Entender e mapear os tipos de pentest que mais se adequam.
- ✓ **Conhecer e compreender como um Hacker Ético se comporta.**
- ✓ Se preparar para a Certificação EC-Council “Certified Ethical Hacker”.
- ✓ **Se preparar para a Certificação Hacking e Comptia Pentest.**
- ✓ Criar políticas de segurança.
- ✓ Realizar varreduras ativas.
- ✓ **Realizar ataques de Engenharia Social.**
- ✓ Entender, realizar e se proteger de ataques DoS e DDoS. Brutal Force, entre outros.
- ✓ **Criar vírus indetectáveis.**
- ✓ Detecção de vulnerabilidades em servidores WEB.
- ✓ **SQL Injection.**
- ✓ Iniciar sua carreira em Segurança da Informação.
- ✓ **Compreender e interagir com diferentes camadas de rede, como ARP, DNS, HTT.**
- ✓ Interceptar e modificar pacotes de rede dinamicamente
- ✓ **Analisar e modificar solicitações e respostas HTTP**

PENTEST E ANÁLISE DE VULNERABILIDADES



- ✓ **Injetar código em páginas HTML carregadas por qualquer computador na mesma rede**
- ✓ Downgrade de HTTPS para HTTP

PRÉ-REQUISITOS:

- ✓ Conhecimentos de informática básica
- ✓ Conhecimentos em Linux e Windows.
- ✓ Conhecimentos em redes de Computadores.

EMENTA:

- **Sobre o curso de pentest**
  - Introdução ao pentest e aos pilares da segurança da informação
  - Metodologias internacionais e a metodologia proprietária Kali Linux
  - Definindo e montado um escopo de projeto para pentest
  - Avisos Legais
  - Apresentação do Treinamento
  - Introdução a Segurança da Informação
  - Introdução ao Penetration Testing
- **Dominando Pré-Requisitos para o Treinamento.**
  - Carreira em Pentest
  - Virtualização e Sistemas Operacionais
  - Dominando o terminal do Linux
  - Dominando o prompt do Windows
  - Visão geral sobre WEB e HTTP
  - Análise de Logs
- **Coleta de informações públicas (Footpriting)**
  - Analisadores de Protocolos
  - Bash Scripting (Linux)
  - Power Shell para Pentesters
  - Linguagem C para Pentesters
  - Coleta de DNS
  - Coleta de e-mails
  - Coleta de informações inteligente (Maltego)

PENTEST E ANÁLISE DE VULNERABILIDADES



- **Fingerprinting manual e automatizado**
    - Estudo sobre protocolos de rede
    - A ferramenta Nmap
    - Principais varreduras do Nmap
    - Burlando filtros do firewall Iptables
    - Nmap Scripting Engine
    - Netcat
    - Capturando banners de aplicações
    - Determinação manual da versão do sistema operacional com traceroute e ping
    - Burlando regras restritivas de bloqueio (DROP) do IPTables com Hping3
    - Enviando e-mails falsos em nome de outra pessoa
- **Exploração de vulnerabilidades e Programação**
    - Meterpreter e antivírus
    - Porque o antivírus falha
    - Python para Pentesters
    - Swiss Army Knife
    - Information Gathering - Business
    - Information Gathering - INFRA
    - Information Gathering - WEB
    - Programando um vírus indetectável por antivírus
    - Escalonamento de privilégios
    - Ganhando acesso administrativo em sistemas Windows 10 de 64 e 32 bits
    - Scanning
- **Engenharia social**
    - SET – Social Engineering Toolkit
    - Corrigindo vários bugs do SET
- **Sniffers remotos**
    - ARP Spoof
    - DNS Spoof
    - SSLStrip2
    - Rogue DHCP
    - DHCP Starvation
    - Injetando código e tornando arquivos executáveis em arquivos maliciosos via falso
    - Proxy
    - Criando um servidor DHCP falso e forçando a atribuição de IPs
- **Manutenção do acesso**



- Aprendendo a programar em Python
- Criando um ExeJoiner (pyJoiner)
- Juntando dois arquivos em um único executável

- **Análise de Vulnerabilidades**

  - Análise de Vulnerabilidade
  - Etapa - Análise de Vulnerabilidade
  - Pesquisa manual por vulnerabilidades
  - Scanners de Vulnerabilidades
  - Vantagens e Desvantagens
  - Exemplos de uso
  - Trabalhando com o Nessus
  - Análise de um scan básico
  - Análise em aplicações web
  - Realizando um Patch Assessment
  - Realizando testes de força bruta
  - Scan avançado (Like a pro)
  - Compliance PCI-DSS
  - Exemplo: Compliance PCI-DSS
  - Falsos Negativos
  - Revisão e dicas
  - NMAP NSE
  - Shadow Brokers

- Metasploit Framework

  - Burlando Mecanismos de Defesa
  - Trabalhando com Scapy
  - Enumeração (Enumeration)
  - Hashes e Senhas - Linux
  - Hashes e Senhas - Windows

- **Negação de serviço (Denial Of Service) e Brutal Force**

  - Definição
  - Objetivo
  - Ferramentas para paralisar sites com ataques DoS
  - Ataques de Força Bruta
  - Wordlists
  - Gerando mutação em wordlist
  - Gerando wordlists personalizadas
  - Key Space Brute Force
  - Brute force com Hydra
  - Reverse Brute force
  - Low Hanging Fruit
  - Dicas Extras
  - Construindo sua própria ferramenta

PENTEST E ANÁLISE DE VULNERABILIDADES



- Criando um cliente ssh em Python
- Criando um script para brute force em ssh
- Construindo um script em bash

- **Web Hacking**

  - Encontrando páginas vulneráveis via Google Hacking
  - Principais dorks
  - Google Hacking Database
  - Principais vulnerabilidades em aplicações Web
  - SQLi
  - Command Injection
  - Local File Include
  - Cross Site Scripting

- **Pentest Interno**

  - Pentest em ambientes modernos
  - Identificando o escopo na rede
  - Capturando hashes na rede
  - Validando as credenciais
  - Enumerando as contas do AD
  - Conseguindo Domain Admin
  - Obtendo acesso ao servidor
  - Conclusão: Acesso completo

- **Dev Exploitation:**

  - Dev Exploitation: Assembly para Pentesters - Windows
  - Dev Exploitation: Assembly para Pentesters - Linux
  - Buffer Overflow para Pentesters: Windows 10
  - Desenvolvimento de Exploits: Windows 10

- **Mecanismos de proteção:**

  - EP e ASLR
  - Buffer Overflow - Linux
  - Trabalhando com Exploits Públicos
  - Pentest Web: Web Hacking
  - Pós Exploração
  - Engenharia Social

FORMA DE PAGAMENTO:

- ✓ Em até **12 vezes** sem juros no **Cartão de Crédito** ou Boleto.
- ✓ Em até 18 vezes com juros de 0.69% a.m.
- ✓ Em até 24 vezes com juros de 1.29% a.m.

Atenciosamente,

GRUPO UTAH - SECURITY
Sales Training – Grupo Utah
55 11 2649-4410
comercial@utah.com.br
www.utah.com.br