**Curso de pentest em redes**

*Segurança ofensiva*

* Análise de vulnerabilidades
* Testes de intrusão (pentest)

**A metodologia**

A utilização de uma metodologia permite dividir um processo complexo em uma série de tarefas menores e mais administráveis.

**Reflexão**

A lógica da metodologia representa as fases do mais amplo para o mais específico.

**A metodologia *possibilita conhecer o alvo:***

* Onde ele está localizado?
* Qual o endereço IP?
* Que sistema operacional o alvo está executando?
* Quais serviços estão sendo executados?
* Quais versões de softwares estão sendo executados?

**Metodologia de pentest baseada em cinco passos**

* Reconhecimento
* Scanning
* Exploração de falhas
* Preservação do acesso
* Gerando relatórios

**Reconhecimento (coleta de informações sobre o alvo)**

Esta fase tem como foco aprender tudo sobre o alvo. Documentando o máximo possível de informações sobre o alvo.

**Principais técnicas de reconhecimento**

* Espelhamento de sites
* Pesquisas no google
* Google Dorks
* Mídias sociais
* Sites de ofertas de emprego
* DNS e ataques DNS

Principais ferramentas de reconhecimento

* Netcraft
* Whois
* Nslookup
* Dig
* Engenharia social

**Scanning**

(Scanning de portas e scanning de vulnerabilidades). Possibilita ter uma melhor definição da rede e da infraestrutura do sistema de informação que será alvo da exploração de falhas.

**Principais técnicas scanning**

**Conhecimentos de protocolos:**

* TCP
* UDP
* IP
* ICMP

**Principais ferramentas scanning**

* Nmap
* Zenmap
* Hping3
* Nessus

**Exploração de falhas**

De posse das informações inicia-se o ataque aos alvos através de várias técnicas e ferramentas.

Objetivo final é ter acesso completo (administrador) sobre o alvo. Pode ser local ou remota. Entrar no sistema alvo e sair com informações sem ser notado usando as vulnerabilidades e técnicas comprovadas.

**Principais técnicas de exploração**

* Teste de vulnerabilidades
* Quebra de senhas
* Obter acesso a serviços
* Sniffing do tráfego de rede

**Principais ferramentas de exploração**

* Metasploit
* John the Ripper (JtR)
* Netcat
* Exploits

Preservação do acesso

(criar uma porta dos fundos permanente para acesso ao sistema) Após explorar falhas, backdoors e rootkits serão deixados nos sistemas para permitir acesso futuro.

**Principais técnicas**

* Instalação de backdoors
* Instalação de rootkits

**Principais ferramentas de preservação de acesso**

* Netbus, Sub7 e Back orifice (Backdoors)
* Netcat (canivete suíço)
* Hacker defender(rootkit)
* Meterpreter (payload)

**Gerando relatórios**

Gerar relatórios detalhados gerenciais e técnicos sobre o alvo para explicar o processo de hacking.

**Principais técnicas e componentes do relatório que será definido pelo cliente:**

* Sumário executivo
* Procedimentos ligados ao teste
* Arquitetura e composição do alvo
* Descobertas
* Ações recomendadas

**Principais técnicas**

* Conclusões
* Apêndices
* Apresentação
* Armazenamento do relatório e evidências

**Principais ferramentas**

* Maltego
* Keepnote
* Casefile
* MagicTree

Referências bibliográficas

ENGEBRETSON, Patrick – Introdução ao web hacking: Ferramentas e técnicas para invasão de aplicações – São Paulo: Novatec, 2014. PAULI, Josh – Introdução ao hacking e aos testes de invasão: Facilitando o hacking ético e os testes de invasão – São Paulo: Novatec, 2014.