ETHICAL HACKING LINUX FUNDAMENTALS (EHLF)

DESCRIÇÃO

(Nível Básico/Intermediário)

Carga Horária: 40hrs

O curso Ethical Hacking Linux Fundamentals (EHLF) apresenta o conhecimento necessário para te colocar no controle de um Sistema Operacional Linux. Seja para realizar atividades ofensivas (Pentesters, Red Team) ou atividades de defesa (Blue Team, Thread Hunting, CSIRT, SOC), é fundamental a capacidade de interação eficiente com o ambiente do Linux, principalmente, a linha de comando, o Shell. Utilizando o Shell é possível potencializar o uso de ferramentas simples para solução de desafios complexos. Por exemplo, é possível transformar um simples cliente de rede em uma ferramenta de ataque de força bruta de diretórios em servidores Web. Ou ainda, utilizar ferramentas de pesquisa em texto para realizar auditorias, ou sanitizar logs.

Durante o curso o aluno construirá o conhecimento começando do básico e chegando em tópicos avançados de maneira progressiva. Inicialmente abordaremos fundamentos de Shell para ensinar o aluno a interagir com esse ambiente. Após a conquista dessa etapa, vamos aprender a automatizar tarefas do dia a dia utilizando Shell Script, sempre trazendo exemplos de uso do mundo real e do dia a dia de times de defesa e ataque. Na terceira fase do curso, abordaremos temas mais avançados com o intuito de prover os fundamentos necessários para realizar atividades de exploração e pós-exploração em ambientes "*Unix Like*". Entre esses temas podemos destacar "Vetores comuns de escalação de privilégio" que traz um entendimento do porquê e como é possível escalar privilégio, utilizando exemplos didáticos. Ou ainda, "O protocolo SSH" que traz as principais características desse protocolo e como podemos utilizá-lo para exploração ou pós-exploração.

MÓDULO 0

1. História do Linux
2. Distribuições Linux modernas
   - Debian, Red Hat, Fedora, Arch Linux, Ubuntu
3. O Linux para usuários comuns
   - É possível utilizar o ambiente Linux sem utilizar a “tela preta”
   - Conhecendo uma distribuição Linux
4. Para que utilizamos os Linux nos dias atuais?

MÓDULO 1

1. Introdução ao Shell
   - Entendendo a estrutura da linha de comando
   - Comandos básicos para manipular arquivos e diretórios:
     - ✔ Navegar na árvore de diretórios
     - ✔ Criar, editar, renomear e remover arquivos e diretórios
     - ✔ Pesquisa por padrões de texto em arquivos
   - Variáveis no Shell
     - ✔ Variáveis locais
     - ✔ Variáveis globais
     - ✔ Variáveis reservadas
   - Compreender o controle de acesso básico de arquivos e diretórios
     - ✔ Gerenciando as permissões
   - Compreender os tipos básicos de redirecionamento: >, >>, 2>, 2>> e | (pipe)
   - Compreender o funcionamento dos operadores lógicos && e ||
   - Concatenação de comandos
   - Compreender o funcionamento da estrutura de substituição de comandos: $() e ``

MÓDULO 2

1. Shell Script Básico
   - Conceito de Shell Script
   - Parâmetros especiais
   - Recebendo parâmetros dos usuários
     - ✔ Parâmetros posicionais
     - ✔ Perguntando ao usuário
2. Estrutura de controle de fluxo: IF/THEN/ELSE
   - O comando test:
     - ✔ Comparando valores
     - ✔ Testando arquivos
     - ✔ Operadores de string
     - ✔ Operadores aritméticos
3. Estrutura de controle de fluxo: IF/THEN/ELIF/ELSE;
4. Implementando IF/THEN/ELSE utilizando apenas () e ||
5. Utilizando CASE/ESAC

MÓDULO 3

1. Estruturas de repetição
   - O laço for
     - ✔ Iterando listas
     - ✔ Iterando o conteúdo de arquivos
     - ✔ Iterando o conteúdo de variáveis
     - ✔ For condicional

   - O laço while
     - ✔ Exemplo de while com test
     - ✔ Exemplo de while com comando
     - ✔ Processamento de texto com while

   - continue/break

2. Expansão do Shell
   - *Brace Expansion*

MÓDULO 4

1. Tratamento de conteúdo. Comandos para filtrar dados
   - sed
     - ✔ Localizar e substituir
     - ✔ Trabalhando com linhas específicas
     - ✔ Filtrando intervalos de texto
     - ✔ Apagando caracteres específicos
   - cut
   - grep
   - cut + sed + grep
   - Buscando dados na Web:
     - ✔ Curl, Lynx, wget

2. Expressões regulares
   - Metacaracteres
     - ✔ Tipo representante
     - ✔ Tipo quantificador
     - ✔ Tipo âncora
     - ✔ Classes POSIX
     - ✔ Gerando *wordlists* (dicionários) e removendo letras repetidas

MÓDULO 5

1. Funções
   - Definição
   - Sintaxe da função
   - Parâmetros posicionais dentro de uma função
   - Exemplos

MÓDULO 6

1. Ferramentas uteis de rede para bind/reverse shell
   - Bash
     - ✔ Cliente de rede com bash (banner grabing);
     - ✔ Transferindo arquivos;
     - ✔ Enviando shell reverso com bash;
   - Netcat
     - ✔ Banner Grabbing
     - ✔ Transferindo arquivos com o netcat
     - ✔ Bind/Reverse shell com netcat
     - ✔ ncat – NetCat + SSL
   - OpenSSL
     - ✔ Cliente de rede com openssl
     - ✔ Bind Shell utilizando arquivos FIFO
     - ✔ Reverse Shell utilizando arquivos FIFO

MÓDULO 7

1. Vetores comuns de escalação de privilégio (Falhas de configuração)
   - Permissões especiais
     - ✔ SUID
     - ✔ SGID
   - Permissões avançadas
     - ✔ chattr/lsattr
   - Sudo
     - ✔ Política de sudo
     - ✔ Riscos e oportunidades
     - ✔ Exemplos de escalação de privilégio
   - Linux *Capabilities*
     - ✔ Gerenciando as capacidades
     - ✔ Exemplo de escalação de privilégio
   - Tarefas agendadas
     - ✔ Verificando as tarefas agendadas
     - ✔ Exemplo de escalação de privilégio

MÓDULO 8

1. O protocolo SSH
    - Visão geral do protocolo SSH (RFC 4251)
    - Mecanismos de autenticação e seus desafios
        - ✔ Username/Password
        - ✔ Chave
        - ✔ Host Based Authentication
    - Transferência de arquivos com SSH (SFTP)
    - SSH Port Forwarding e seus riscos
    - Local Port Forwarding
        - ✔ Casos de uso
    - Remote Port Forwarding
        - ✔ Casos de uso
    - Dynamic Port Forwarding
        - ✔ Casos de uso

MÓDULO 9

1. Outros comandos úteis
    - Verificando arquivos abertos
        - ✔ lsof
        - ✔ fuser
    - O comando find
        - ✔ Procurando por arquivos modificados nas últimas 24 horas
        - ✔ Procurando por arquivos modificados com menos 24 horas
        - ✔ Procurando por arquivos com permissão de SUID/SGID
        - ✔ Apagando um arquivo com um inode específico
        - ✔ Procurando arquivos pelo tamanho
        - ✔ Procurando arquivos com permissão de escrita
        - ✔ Executando comandos para os arquivos encontrados
    - O comando watch
    - O comando mount/umount
    - O comando diff/patch

MÓDULO 10

1. Recuperando a senha de root editando o grub
    - Sistemas Debian like
    - Sistemas RedHat like
    - Sistemas FreeBSD like

MÓDULO EXTRA

1. Estrutura de um pacote Deb
2. Riscos de instalação de um pacote Deb de uma fonte não confiável
3. Modificando um pacote Deb manualmente
    - Adicionando um backdoor
    - Adicionando uma tarefa agendada

PRÉ-REQUISITOS

- Conhecimentos básicos em Sistema Operacional Linux;
- Conhecimentos básicos de Rede de Computadores, Protocolos e Serviços de Rede
  - Protocolo TCP/IP, FTP, HTTP, HTTPS, SMB, SSH, DNS, ICMP
- Familiaridade com ferramentas de Virtualização – VMWare e VirtualBox

PÚBLICO ALVO

- Estudantes da área de Tecnologia da Informação
- Estudantes de Segurança da Informação
- Analistas de Segurança da Informação
- Analistas de SOC
- Membros de CSIRT
- Pentesters
- Profissionais de TI com interesse e afinidade na área de Segurança da Informação
- Entusiastas de Segurança da Informação

MATERIAL NECESSÁRIO

- Os alunos devem utilizar suas próprias estações de trabalho (Windows, Linux ou Mac OS), com a capacidade de executar até 02 (duas) Máquinas Virtuais (VM) simultaneamente.
- Configuração mínima de 8GB de RAM, 40 GB de espaço livre em disco, porta USB e placa de rede (RJ45 ou *wireless*) para acesso à Internet.
- Desejável 02 (dois) monitores para incremento na produtividade.
- Software de Virtualização: VMWare ou VirtualBox, preferencialmente, a versão mais atualizada.
- Será disponibilizado acesso a uma VM Kali Linux customizada para o treinamento (preparada com os desafios). O aluno está livre para utilizar qualquer outra distribuição ou mesmo um Kali próprio, contudo, é aconselhável utilizar a VM Kali oferecida no curso.

MATERIAL RECEBIDO

- Acesso ao Portal do Aluno – GoHacking Academy, que concentra o material do curso
- Apostila do Curso no formato PDF
- Gravações das sessões ao vivo
- Certificado de Conclusão do Curso no formato PDF (com a carga horária e ementa)

CAPACIDADES ALCANÇADAS

No final do curso, o aluno estará apto a:

- Manipular arquivos e diretórios em ambientes Linux
- Gerenciar permissões em ambientes Linux
- Utilizar redirecionamentos em ambientes Linux
- Automatizar as tarefas utilizando Shell Script
- Realizar tratamento de conteúdo utilizando Shell
- Utilizar ferramentas nativas para bind/reverse shell
- Utilizar falhas de configuração em Permissões especiais para escalar privilégio
- Utilizar falhas de configuração em Permissões avançadas para escalar privilégio
- Utilizar falhas de configuração em políticas de Sudo para escalar privilégio
- Utilizar falhas de configuração em tarefas agendadas para escalar privilégio
- Utilizar o protocolo SSH como ferramenta de gerenciamento de remoto e ferramenta de exploração
- Utilizar comandos quer permitem auditoria do sistema como lsof,fuser, find
- Acessar dados em imagens de disco utilizando os comandos mount/umount
- Aprender a criar e aplicar patches utilizando os comandos diff/patch
- Aprender a recuperar senha através da edição do Grub e como se proteger disso em sistemas Debian like, RedHat like e FreeBSD like
- Entender a estrutura de um pacote do Debian

MARCIO DE SOUZA OLIVEIRA