ETHICAL HACKING COMMAND AND CONTROL
EHC2

DESCRIÇÃO

(Nível Básico/Intermediário)

As ameaças cibernéticas estão cada vez mais avançadas ao ponto de grandes empresas e nações serem vítimas constantes de ataques mais elaborados. Isso nos leva a dura realidade de que, mais cedo ou mais tarde, sua organização será atacada e comprometida em algum nível.

Esse minicurso descreve técnicas atuais de pós-exploração em um ambiente controlado e composto por aplicações reais e com sistemas operacionais modernos (Windows e Linux), com foco na Infraestrutura de Comando e Controle (C2). Ele é uma pequena parte de nosso curso mais completo, o Ethical Hacking Post Exploitation – EHPX.

Será abordado, de forma 100% prática, como os sistemas de C2 funcionam, quais são os protocolos de comunicação mais utilizados, quais técnicas são empregadas para camuflar o tráfego entre a vítima (alvo/agente) e o atacante (servidor de C2), quais ferramentas podem ser utilizadas e customizadas, quais as vantagens e desvantagens dos frameworks disponíveis (*open source* e gratuitos) e o que pode ser feito para detectar essas atividades.

AGENDA

(Duração de 5hs)

1. Visão Geral sobre Teste de Invasão (*Pentesting*), Exploração (*Exploitation*), Pós-Exploração (*Post-Exploitation*) e *Red Team Operation*

2. Cyber Kill Chain Framework
   - Análise das etapas de um ataque cibernético

3. Mitre ATT&CK Framework
   - Visão Geral
   - Análise de atividades de Pós-Exploração

4. C2 Frameworks
   - Visão Geral
   - Arquitetura e características de mecanismos de C2
   - Sistemas de C2 disponíveis

5. Empire
   - Estrutura, Módulos e Funcionalidades
   - Estabelecimento de um Canal de C2
   - Laboratório

6. Covenant
   - Estrutura, Módulos e Funcionalidades
   - Estabelecimento de um Canal de C2
   - Laboratório

7. SilentTrinity
   - Estrutura, Módulos e Funcionalidades
   - Estabelecimento de um Canal de C2
   - Laboratório

8. Merlin
   - Estrutura, Módulos e Funcionalidades
   - Estabelecimento de um Canal de C2
   - Laboratório

9. Sliver
   - Estrutura, Módulos e Funcionalidades
   - Estabelecimento de um Canal de C2
   - Laboratório

PRÉ-REQUISITOS

- Conhecimentos básicos em Sistema Operacional Windows
  - Estrutura de diretórios, comandos básicos do prompt, configuração de rede, verificação de serviços e processos, gerenciamento de usuários locais
- Conhecimentos básicos em Sistema Operacional Linux
  - Estrutura de diretórios, comandos básicos do shell, configuração de rede, verificação de serviços e processos, gerenciamento de usuários locais, permissão de arquivos
- Conhecimentos básicos de Rede de Computadores e Serviços de Rede
  - Protocolo TCP/IP, FTP, HTTP, HTTPS, SMB, SSH, DNS, ICMP
- Conhecimentos básicos de Penetration Testing – Metodologia e Procedimentos
- Familiaridade com a distribuição Kali Linux
- Familiaridade com ferramentas de Pentesting – Metasploit, Meterpreter
- Familiaridade com ferramentas de Virtualização – VMWare, Virtual Box
- Familiaridade com Powershell

MATERIAL NECESSÁRIO

- Os alunos precisam trazer seus próprios laptops (Windows, Linux ou Mac OS), com a capacidade de executar de 02 a 03 Máquinas Virtuais (VM) simultaneamente;
- Configuração mínima de 8GB de RAM, 40 GB de espaço livre em disco;
- Software de Virtualização: VMWare, versão mais atualizada, de preferência Workstation (para hosts Windows ou Linux) ou Fusion (para host Mac OS), pode ser a versão trial. O VMWare Player também é capaz de executar as VMs do curso; e

MATERIAL RECEBIDO

- 02 Máquinas Virtuais (Kali e Windows 10) com as aplicações utilizadas nos exercícios
- Apostila do Curso no formato PDF
- Certificado de Conclusão do Curso no formato PDF

LAIOS FELIPE BARBOSA

GoHacking
CYBER SECURITY TRAININGS