ETHICAL HACKING
ENDPOINT PROTECTION EVASION – EHEPE

DESCRIÇÃO

(Nível Intermediário/Avançado)

Carga Horária: 40hrs

O curso Ethical Hacking Endpoint Protection Evasion (EHEPE) apresenta técnicas ofensivas de evasão, com a análise das etapas de desenvolvimento de códigos e ferramentas capazes de burlar sistemas de defesa, bem como realiza um estudo de mecanismos de execução de *shellcode* em ambientes corporativos *hardenizados*.

Milhões de dólares são gastos em empresas com soluções de Antivírus, *Endpoint Detection and Response* (EDR) e monitoramento, contudo a maioria desses controles é contornada por ameaças persistentes avançadas (*Advanced Persistent Threats* – APT) que, muitas vezes, utilizam técnicas, táticas e procedimentos (*Tactics, Techniques and Procedures* – TTP) customizados, fazendo com que toda a cadeia de proteção comprada e configurada seja burlada.

Como os atacantes conseguem executar código malicioso mesmo com proteções ativadas e atualizadas? Como eles se movimentam dentro de uma rede sem deixar alertas em sistemas de detecção? Como eles conseguem contornar proteções como *Applocker, Sysmon, ETW, LAPS, CLM* dentre outras e serem bem-sucedidos na propagação de malwares dentro de uma rede corporativa? Como eles fazem para utilizar outros canais para exfiltração de dados e não serem pegos? Essas e outras perguntas serão respondidas nesse treinamento, que possui uma abordagem 100% prática, conduzido por laboratórios e exercícios que farão com que o aluno compreenda em detalhes os tópicos mencionados.

O curso trabalha técnicas atuais de evasão de antivírus e *hardening* em ambientes atualizados. Serão apresentados TTP de ataques, bem como o desenvolvimento de outras ferramentas para execução de código malicioso, das mais simples até técnicas utilizadas por APT, pontos fundamentais tanto para atividades ofensivas (Pentesters, Red Team) quanto para as atividades de defesa (Blue Team, Threat Hunting, CSIRT, SOC).

Diversos temas serão abordados, tais como: entendimento de antivírus, evasão de detecções por assinatura, evasão de detecções por heurística, P/Invoke, D/Invoke, *Reflection*, desenvolvimento de shellcode runners/malwares, ofuscação, evasão de *Applocker*, evasão de *LAPS*, evasão de *Applocker*, movimentação lateral evasiva, evasão de AMSI, entre outros.

TÓPICOS

MÓDULO 1

Evasão de Antivírus

- Linguagens utilizadas: C/C++, C#, Python, Powershell e Rust
- Introdução à antivírus
- Portable Executable
- Estrutura de um PE
- Import Address Table (IAT)
- Windows Architecture
- Windows Aplication Programming Interface (API)
- Windows NTApi
- Userland Hooking
- System Service Descriptor Table (SSDT)
- Platform Invoke (P/Invoke)
- Dynamic Invoke (D/Invoke)
- System Call Obfuscation
- Assinatura e métodos de evasão
- Ofuscação
- Shellcode Runners, Crypters & Encoders
- Heurística e métodos de evasão
- Sandbox Evasion
- Offensive Reflection
- Evasão de antivírus no Linux

MÓDULO 2

Injeção (*Injection*)

- Linguagens utilizadas: C/C++ e C#
- Introdução à injeção de código
- Process Injection vanilla
- Process Injection via NtMapViewOfSection
- Process Injection via QueueUserAPC
- Process Hollowing
- DLL Injection
- Reflective DLL Injection
- Shellcode Reflective DLL Injection (sRDI)
- Backdooring

MÓDULO 3

Powershell & AMSI

- Introdução à *Antimalware Scan Interface* (AMSI)
- Hooking AMSI
- AMSI Bypass com reflection
- Engenharia reversa amsi.dll
- AMSI Bypass in initialization
- P/Invoke Powershell
- Dynamic Lookup Powershell
- Powershell Obfuscation
- Constrained Language Mode (CLM)
- Unmanaged Powershell

MÓDULO 4

Windows Controls & C2

- Linguagens utilizadas: C/C++, C# e Powershell
- Técnicas furtivas em estruturas de Comando e Controle (C2)
- Redirectors
- Network Profiles
- Covert Channels
- Bypass de Network Proxies & DNS filtering
- Introdução à Domain Fronting
- HTML Smuggling
- Introdução à App Locker
- Bypass de Applocker
- Introdução à JSCRIPT
- Técnicas de bypass com JSCRIPT
- Introdução à *Local Administrator Password Solution* (LAPS)
- Enumeração de LAPS e leitura de senha
- Introdução à *Protected Process Light* (PPL)
- Bypass de PPL
- Introdução à *Event Tracing for Windows* (ETW)
- ETW Patching
- Introdução à Sysmon
- Desabilitando Sysmon
- Binary Signing & Attributes for Evasion
- Mark of the Web (MOTW)
- MOTW Packing

MÓDULO 5

Macros

- Introdução à criação de macros
- Visual Basic for Applications (VBA) 101
- Métodos Auto Open e Document Open
- Pretexting
- Command Execution
- WMI Dechainning
- VBA Obfuscation
- Macro P/Invoke
- VBA Stomping

PRÉ-REQUISITOS

- Conhecimentos básicos em Sistema Operacional Windows
  - Estrutura de diretórios, comandos básicos do prompt (cmd.exe), 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 (bash), 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
- Conhecimentos básicos de programação
- Conhecimentos básicos nas linguagens: Powershell, C, C++, C#, Python e Rust

PÚBLICO ALVO

- Especialistas em Segurança da Informação
- Analista de Segurança da Informação
- Pentesters
- Membros de Red Team / Blue Team
- Membros de CSIRT
- Analista de SOC
- Profissionais de TI com interesse e afinidade na área 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 de 02 a 03 Máquinas Virtuais (VM) simultaneamente.
- Configuração mínima de 8GB de RAM, 60 GB de espaço livre em disco, porta USB e placa de rede (RJ45 ou *wireless*) para acesso à Internet.
- Desejável 02 monitores para incremento na produtividade
- Software de Virtualização: VMWare, versão mais atualizada, de preferência *Workstation* (para hosts Windows ou Linux) ou *Fusion* (para host Mac OS). É possível utilizar a versão de avaliação (*trial*). O VMWare *Player* também é capaz de executar as VMs do curso (não possui a capacidade de realizar *snapshots*, importante, mas não imprescindível para o curso).
- Será disponibilizado uma VM Kali Linux customizada para o treinamento (empregada como a máquina atacante). 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

- As Máquinas Virtuais com as aplicações utilizadas nos exercícios
- Apostila do Curso no formato PDF
- Gravações das sessões ao vivo, disponibilizadas no GoHacking Academy
- 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:

- Desenvolver e aperfeiçoar táticas, técnicas e procedimentos ofensivos para operações de Pentesting e Red Team
- Entender o funcionamento das principais soluções de proteção de *endpoints*
- Compreender a estrutura de binários Windows e suas características
- Entender a estrutura, as chamadas e a importância das API's do Windows
- Compreender o funcionamento de soluções de antivírus e EDR
- Dominar as técnicas básicas de evasão de antivírus e EDR
- Contornar mecanismos de detecção por assinatura, por heurística e por comportamento
- Manipular o Powershell para atividades ofensivas
- Realizar o bypass do AMSI
- Ter a capacidade de desenvolver seus próprios *malwares*
- Executar malware em disco e em memória
- Se movimentar dentro de uma rede sem ser detectado (*stealthy*)
- Configurar uma estrutura de Comando e Controle (C2) furtiva
- Criar ferramentas de injeção de código
- Criar mecanismos para contornar proteções do Applocker
- Contornar a proteção do LAPS
- Contornar a proteção do ETW
- Contornar a proteção do PPL
- Utilizar técnicas de bypass com JSCRIPT
- Criar e manipular macros para uso ofensivo

JOÃO PAULO DE ANDRADE FILHO