ETHICAL HACKING ENUMERATION OF WEB ATTACK SURFACE (EHEWAS)

DESCRIÇÃO

(Nível Básico/Intermediário)

Carga Horária: 21 hrs

Neste curso você irá realizar exercícios práticos de enumeração em um "alvo real" (aplicações reais que estão disponíveis na Internet), utilizando técnicas e ferramentas que *hackers* profissionais usam (inclusive assistentes baseados em Inteligência Artificial – IA), enquanto aprende a mapear a superfície de ataque web de uma organização, que é o conjunto das aplicações que está visível na Internet.

O **conteúdo não é voltado a ensinar como utilizar um *scan* de vulnerabilidades**, mas vai apresentar técnicas e ferramentas que, isoladas ou em conjunto, permitem que os *hackers* possam reconhecer os ativos externos de uma organização, tanto ou mais que ela própria.

A crescente demanda por sistemas de informação, combinada com uma gestão de ativos deficiente, em especial das aplicações web, leva à negligência na manutenção dos ativos (por exemplo, aplicação de *patches*), abrindo caminho para o sucesso de ataques de fácil execução, porém com grande impacto nas organizações.

Quando uma organização "esquece" de uma aplicação web na Internet, por exemplo, ao remover de uma página o link que leva a ela, mas não realiza o seu *takedown*, a aplicação continua "viva" e provavelmente sem manutenção. Ela não pode ser acessada por meio da navegação pelo site principal da organização, mas se alguém encontrar essa URL, pode conseguir acessá-la.

A manutenção também pode se negligenciada por falhas no processo de CI/CD se as aplicações que entraram em produção não ficam documentadas. Então aplicações inteiras, em especial acessadas por subdomínios ou painéis de administração de soluções integradas (Jenkins, etc.) que foram disponibilizadas para testes e usavam credenciais *default* nestes ambientes continuam disponíveis e, com as constantes alterações das configurações e rede e segurança, podem ficar expostas e se tornarem vetores de ataque poderosos para os *hackers*.

A seguir temos um exemplo, ainda que não tão impactante, que trata de um caso real (e público) que evidencia que as afirmações acima não se trata de suposições teóricas.

Em 2018, um pesquisador de segurança relatou que uma instância de teste da Heroku (*Cloud Application Platform*) da empresa de entregas de produtos Shipt (shipt.com) estava "perdida", e que ele conseguia acessar e explorar aquela instância, obtendo um acesso inicial na organização. Esse pesquisador foi remunerado com um prêmio de US$ 750.

Mas como essas aplicações "esquecidas" impactam a vida de alguns dos papéis envolvidos no ecossistema de segurança?

a) Do ponto de vista de quem defende (gestores das aplicações e as equipes de segurança da informação), a etapa gestão de incidentes pode ficar comprometida, pois não é possível

instrumentalizar sensores para a deteção de ativo cuja existência é desconhecida da organização;

b) Do ponto de vista de *pentesters e red teams*, descobrir esses "pontos cegos" permitem às organizações clientes removerem os "frutos baixos" (do inglês, *low hang fruits*) das mãos dos *hackers*; e
c) Já para os *bug hunters*, pode representar a oportunidade de obter uma relação custo/benefício muito boa. Um bom reconhecimento/enumeração adiciona chances de encontrar vulnerabilidades. Um excelente reconhecimento/enumeração, multiplica essas chances.

No curso será proposto um **processo sistemático de reconhecimento e enumeração da superfície de ataque web de uma organização**, que tem como objetivo identificar o maior número possível de aplicações expostas na Internet, de propriedade de uma organização. Também é possível identificar integrações com terceiros, conhecidas ou esquecidas, e, de forma incidental, outras informações sensíveis (por exemplo, credenciais), que também podem enfraquecer as defesas das organizações.

O processo é implementado com dezenas de técnicas e ferramentas utilizadas por profissionais de segurança ofensiva ("do bem" e "do mal"), e incluem o uso de assistentes baseados em IA.

Ao longo do curso, também discutiremos técnicas de defesa, como uso de CDNs e WAFs, para "dificultar" as atividades de reconhecimento e enumeração, assim como as técnicas de *bypass* que podem ser utilizadas (serão explicados os conceitos com alguns exemplos, mas não aprofundaremos na configuração de cada produto).

A combinação de abordagens de segurança ofensiva e defensiva faz desse curso um instrumento para o desenvolvimento de um importante *mindset*: **quem quer defender bem, precisa saber como são feitos os ataques; e quem quer atacar bem, precisa saber como as defesas funcionam**.

Um grande diferencial do curso são as atividades práticas, que serão executadas em "alvos reais". Você receberá orientação para escolher uma aplicação que está disponível na Internet podendo, inclusive, ser da sua própria organização. Com os devidos cuidados legais, milhares de aplicações reais estão disponíveis, em produção e poderão ser testadas pelos participantes.

Ah! Não é necessário saber programar. Precisaremos usar alguns *scripts* simples em *bash*, mas não se preocupe: vamos aprender a pedir para nosso "amigo" ChatGPT nos ajudar nestas tarefas.

MÓDULO 1 – Importância do Reconhecimento e Enumeração

1. A vida como ela é ....
   - Demonstração

2. Recon & Enum nos *frameworks*
   - *Cyber Kill Chain Framework*
   - Mitre ATT&CK *Framework*

3. Definições
   - O que é superfície de ataque Web?
   - O que é Reconhecimento? E Enumeração?
   - Tipos: ativo x passivo

4. Superfície de ataque Web de uma organização?
   - Domínios, subdomínios, servidores web, hosts virtuais, aplicações
   - *Tracking*.

5. *Mindsets* complementares
   - Ataque & Defesa
   - Para que serve o produto de Recon&Enum para o *Red Team* & *Pentester*?
   - E para os *Bug Hunters*?
   - E para o *Blue Team*?
   - E para o gestor de aplicações?
   - Auditores?

6. Escolha de um alvo real para praticar no curso
   - *Rules of Engagement* (RoE) ou *Scope of Work* (SoW) e mitigação de riscos do trabalho
   - Entendendo as regras de programas de recompensas (*Bug Bounty*) e de Descoberta de Vulnerabilidades (VDP)

7. Preparar sua VM de ataque
   - Como preparar sua máquina de ataque
   - Listagem das ferramentas usadas no curso (há VM pronta para os alunos!)

8. Sugestões para revisão de conceitos básicos (gratuita e opcional)
   - THM
     - TryHackMe – HTTP in Detail (30 min)
     - TryHackMe – DNS in Details (45 min)
     - TryHackMe – Burp Suite: The basics (60min)
   - Hach-the-box
     - HTB - Web Requests (4h)
     - HTB - Introduction to Web Applications (3h)

MÓDULO 2 – Conhecendo as principais defesas (e como contorná-las)

1. A lógica da defesa em camadas
   - Existe defesa contra reconhecimento e enumeração?
   - Onde é bloqueado?
   - O que é bloqueado?
   - Quando é bloqueado?

2. Medidas de defesa
    - Detecção
    - Mitigação

3. Como contornar os bloqueios
    - Técnicas de *bypass*

MÓDULO 3 – Enumeração de domínios

1. Técnicas e ferramentas
    - Aquisições, fusões e incorporações – Parte 1 e 2
    - Uso de IA na enumeração de domínios
    - Microsoft Exchange APIs
    - DNS Reverso – Partes 1 e 2
        - ASN & IPRanges
        - Identificando CDN & Host de Origem
    - Mapeando TODOS os nomes na nuvem
    - WHOIS Reverso
    - IP Reverso
    - Shodan
    - Ferramentas holísticas de OSINT
    - Spidering
    - Mobile Apps
    - Técnicas "exóticas"

MÓDULO 4 – Enumeração de subdomínios

1. Zone transfer & DNSSEC

2. Técnicas e ferramentas passivas
    - Scrapping em várias fontes: Chaos, Shodan, Github, Gitlab, ...
    - Como obter o melhor de cada fonte?

3. Técnicas e ferramentas ativas
    - Força bruta
    - *wordlists*
    - Permutação
    - Uso de IA na enumeração de subdomínios

MÓDULO 5 – Identificação de sites ativos

1. Técnicas e ferramentas
    - Servidores DNS
    - Ferramentas

2. Identificando oportunidades ocultas de enumeração
    - Enumerar subdomínios de subdomínios

MÓDULO 6 – Enumeração de servidores Web

1. Técnicas e ferramentas
   - IPs de subdomínios ativos
   - ASN
   - Expansão da lista de IPs
   - Bônus: identificação de outros serviços, de regras de firewalls e de alguns *bypasses*

MÓDULO 7 – Enumeração de hosts virtuais

1. Técnicas e ferramentas
   - Subdomínios não ativos
   - Força bruta
   - Permutação
   - Escolha de *wordlists*
   - Uso de IA na enumeração de subdomínios

MÓDULO 8 – Priorização de aplicações para enumeração

1. Ferramentas e técnicas ativas
   - Uso de IA na identificação de aplicações
2. Ferramentas e técnicas passivas

MÓDULO 9 – Enumeração de uma aplicação

1. Técnicas e ferramentas passivas
2. Técnicas e ferramentas ativas
   - Não autenticado
   - Autenticado
3. Uso de IA na enumeração de aplicações

MÓDULO 10 – *What´s next?* (Bônus)

1. O que fazer com toda essa informação: opções de abordagem
   - Análise de vulnerabilidades (passiva e ativa)
   - Informações sensíveis vazadas

PRÉ-REQUISITOS

1. Conhecimentos básicos do funcionamento de aplicações web
2. Conhecimentos básicos de rede de computadores e serviços de rede
3. (Opcional) Fazer uma revisão dos conhecimentos básicos (recursos gratuitos)
   3.1. THM free roadmap: https://tryhackme.com/r/hacktivities

PÚBLICO-ALVO

1. Iniciantes na área de Segurança da Informação
2. Especialistas em Segurança da Informação
3. Analista de Segurança da Informação
4. *Pentesters*
5. Membros de *Red Team* / *Blue Team*
6. *Bug hunters*
7. Membros de CSIRT
8. Analista de SOC
9. Gestor de Segurança da Informação
10. Profissionais de TI com interesse e afinidade na área de Segurança da Informação

MATERIAL NECESSÁRIO

1. Os alunos devem utilizar suas próprias estações de trabalho (Windows, Linux ou Mac OS)
   1.1. Configuração mínima da estação de trabalho: 8GB de RAM (16GB é o recomendado), 80 GB de espaço livre em disco e placa de rede (RJ45 ou *wireless*) com acesso à Internet.
   1.2. Instalar software de virtualização VBox, versão mais atualizada (gratuito): link para download: https://www.virtualbox.org/wiki/Downloads
   1.3. Desejável 02 (dois) monitores para incremento na produtividade do curso.
2. Ter uma conta (gratuita) no ChatGPT.

MATERIAL RECEBIDO

1. Acesso ao Portal do Aluno, o GoHacking Academy, que concentra o material do curso
2. Imagem de uma VM VBox pré-configurada com todas as (dezenas) de ferramentas utilizadas no curso
3. Modelo de planilha para *tracking*
4. Modelo em X-Mind para tracking
5. Apostila do curso no formato PDF
6. Gravações das sessões ao vivo
7. Certificado de conclusão do curso no formato PDF (com a carga horária e ementa)

AUTORIZAÇÃO DO “ALVO”

O curso é quase 100% prático: os participantes farão a enumeração da superfície de ataque web de um “alvo real”, de forma que deve haver autorização da “organização alvo” para que o participante realize as atividades.

O “alvo” pode ser a organização do participante ou uma organização que esteja cadastrada em uma plataforma gerenciadora de programas de *Bug Bounty* e VDP (hackerone, bugcrowd, intigriti, bughunter, ...).

No caso de o participante escolher como “alvo” a sua própria organização, ele deve providenciar a devida autorização ANTES de iniciar as atividades práticas do curso, seguindo os trâmites internos e respeitando às normas e às políticas da organização. Este é um excelente argumento para autorização de participação no treinamento, pois permite que o participante preste um serviço à organização a um custo excepcionalmente baixo comparado ao valor que seria contratado.

No caso de a opção ser por uma organização que esteja em uma plataforma gerenciadora de programas BB ou VDP, é necessário que o participante se cadastre na plataforma ANTES de iniciar as atividades práticas do curso. Quem sabe após o curso você ainda sai com um *Bounty* no bolso? Esta não é uma promessa, mas uma possibilidade.

Observação 1: o fato de a organização estar numa plataforma de Bug Bounty por si só não autoriza qualquer pessoa a efetuar qualquer ação ofensiva. Essa autorização é concedida nos termos expressos na plataforma somente aqueles que estejam lá cadastrados e nas regras estabelecidas em cada programa.

Observação 2: o fato de você pertencer a uma organização, ainda que da equipe responsável pela segurança da informação, por si só não o autoriza a efetuar qualquer ação ofensiva. Verifique se isso está expresso nas suas atribuições e aconselhe-se com seu departamento jurídico.

CAPACIDADES ALCANÇADAS

No final do curso, o aluno estará apto a:

- Mapear a superfície de ataque web de uma organização.
- Entender os principais mecanismos de defesa para aplicações web.
- Entender os principais métodos para contornar os mecanismos de defesa para aplicações web.
- Realizar o reconhecimento de aplicações web de uma organização.
- Enumerar domínios e subdomínios de aplicações web.
- Enumerar hosts virtuais de aplicações web.
- Identificar aplicações web “perdidas” ou “esquecidas” por uma organização, que são portas de entrada para ataques cibernéticos.
- Utilizar ferramentas usadas por profissionais de segurança e “*hackers*” para realizar atividades de reconhecimento.
- Utilizar IA na enumeração e identificação de aplicações web.
- Priorizar aplicações web no processo de enumeração.
- Entender o funcionamento dos programas de Bug Bounty e VDP.
- Participar de um programa de Bug Bounty.
- Aumentar as chances de ser remunerado em um programa de Bug Bounty.

RENATO BRAGA