

Enumeração

Cassiano Peres

DIO Tech Education Analyst



cassiano-dio



peres-cassiano

Objetivo Geral

Neste curso vamos aprender a enumerar portas e serviços vulneráveis.

Pré-requisitos

Conhecimento prévio em linhas de comando Linux facilita o aprendizado.

Percorso

- Etapa 1** O que é enumeração?
- Etapa 2** Enumeração com NMap
- Etapa 3** Utilizando Scripts no NMap

Etapa 1

O que é enumeração?

Introdução

Nesta aula vamos explorar o conceito de *enumeração* e como explorar vulnerabilidades com essa técnica.

Enumeração

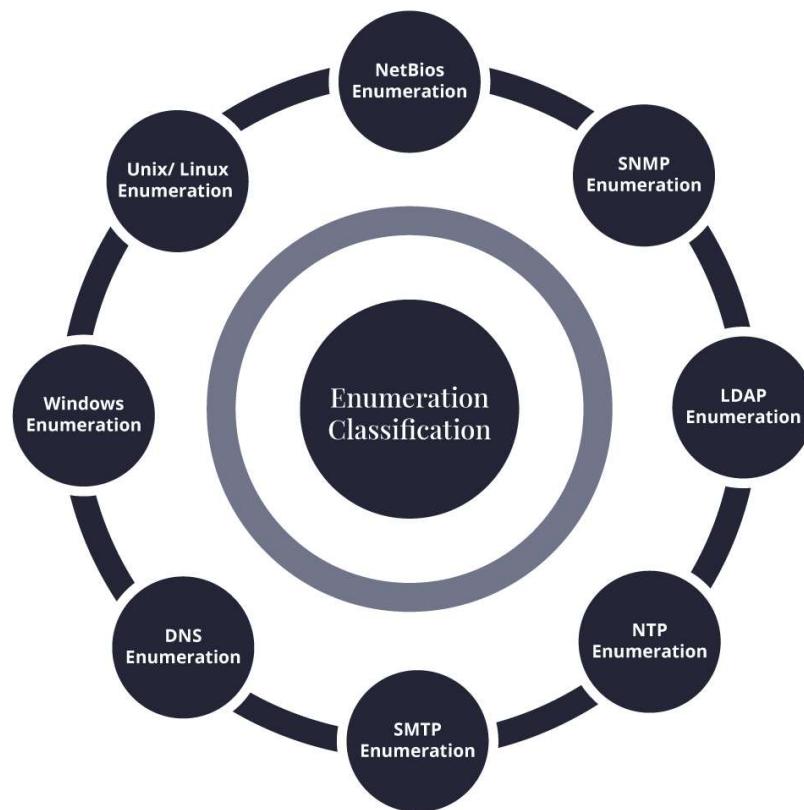
A enumeração é um processo que estabelece uma conexão ativa com os hosts de destino para descobrir possíveis vetores de ataque, podendo ser usado para exploração do sistema.



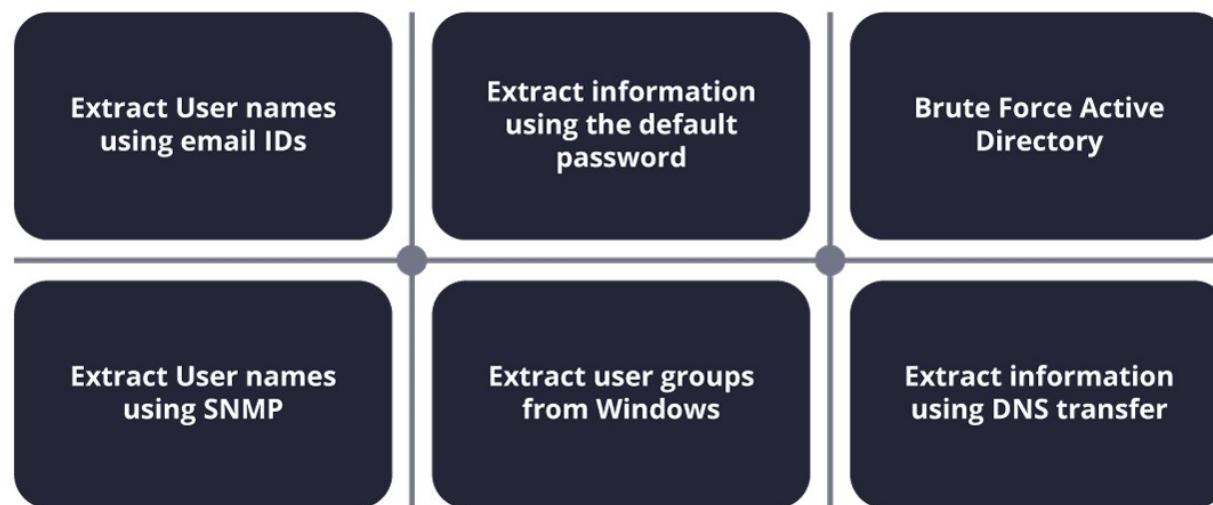
Varredura e enumeração

A etapa de **varredura** busca encontrar as vulnerabilidades, sem maiores detalhes, enquanto a etapa de **enumeração** traz mais detalhes a respeito do sistema invadido.

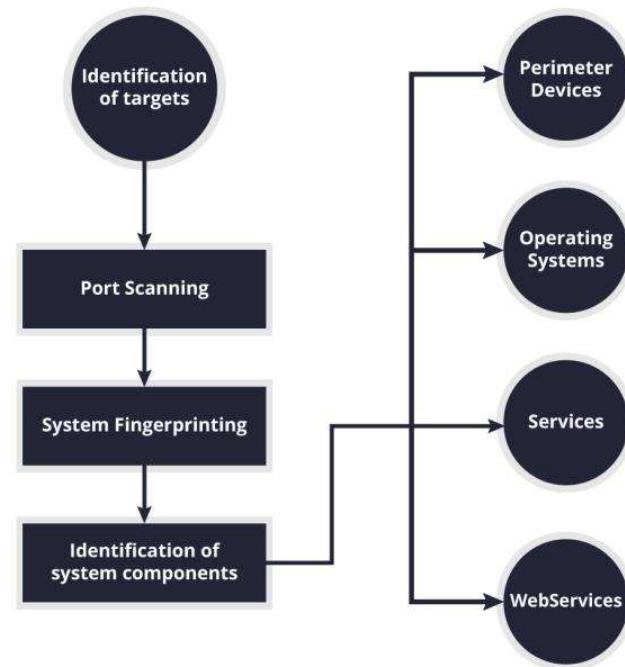
Tipos de enumeração



Técnicas de enumeração



Enumeração



Portas e serviços enumerados

TCP 53 - DNS Zone Transfer
TCP 135 - Microsoft RPC Endpoint Mapper
TCP 137 - NetBIOS Name Service
TCP 139 - SMB Over NetBIOS
TCP 445 - SMB OverTCP
UDP 161: SNMP
TCP/UDP 389 – LDAP
TCP/UDP 3368 - Global Catalog Service
TCP 25 - Simple Mail Transfer Protocol (SMTP)

Informações enumeradas

- Rede de origem;
- Usuários e grupos;
- Tabelas de roteamento;
- Configurações de auditoria;
- Configurações de serviços;

Informações enumeradas

- Nomes de máquinas;
- Aplicações;
- Banners ;
- Detalhes de SNMP;
- Detalhes de DNS.

Ferramentas

- NBTScan;
- DumpSec;
- SMBScanner;
- NMap
- NetCat.

Conclusão

Nesta aula exploramos a teoria por trás da varredura e enumeração em redes de computadores.

Etapa 2

Enumeração com NMap

Introdução

Nas etapas anteriores aprendemos a utilizar o Nmap para varredura de rede, agora vamos novamente utilizá-lo para detalhar as informações varridas.



Enumeração com Nmap

Vamos realizar a enumeração de serviços com o Nmap.

Etapa 3

Utilizando Scripts no Nmap (NSE)

Introdução

Nesta aula vamos utilizar o Nmap com scripts para automatizar as tarefas.

Nmap NSE

O Nmap Scripting Engine (NSE) é um dos recursos mais poderosos e flexíveis do Nmap, permitindo que os usuários utilizem scripts para automatizar uma ampla variedade de tarefas de rede.

Nmap NSE

```
root@kali:~# nmap -n -p80 --script http-grep \
> --script-args 'http-grep.url="login.html",http-grep.match="[a-zA-Z0-9]*pass[a-
zA-Z0-9]*"' 192.168.56.102
Starting Nmap 7.70 ( https://nmap.org ) at 2018-04-11 08:24 EDT
Nmap scan report for 192.168.56.102
Host is up (0.00033s latency).

PORT      STATE SERVICE
80/tcp    open  http
| http-grep:
|   (3) http://192.168.56.102:80/login.html:
|     (3) User Pattern 1:
|       + pass
|       + password
|       + teStdBpassw0rD123
MAC Address: 08:00:27:6E:A2:39 (Oracle VirtualBox virtual NIC)
```

Dúvidas?

- > Fórum/Artigos
- > Comunidade Online (Discord)

