





SEGURANÇA DA INFORMAÇÃO

TÓPICOS ESPECIAIS EM ENGENHARIA

ETHICAL HACKING

Ferramentas para Varredura

PENTEST

Teste de Intrusão / Penetração

FASES DE UM PENTEST

- ✕ Etapa 0 : Negociação
- ✕ Etapa 1 : Levantamento de dados (FootPrinting)
- ✕ Etapa 2 : Varredura
- ✕ Etapa 3 : Ganhando Acesso
- ✕ Etapa 4 : Mantendo Acesso
- ✕ Etapa 5 : Limpando Rastros
- ✕ Etapa 6 : Escrita de Relatórios

ETAPA 1: IDENTIFICAÇÃO OU COLETA DE DADOS

- ✗ Fontes que possam trazer informações sobre a empresa
 - softwares
 - sites
 - pessoas
 - livros
 - jornais
- ✗ Ferramentas
 - Maltego
 - AnyWho
 - Google Maps

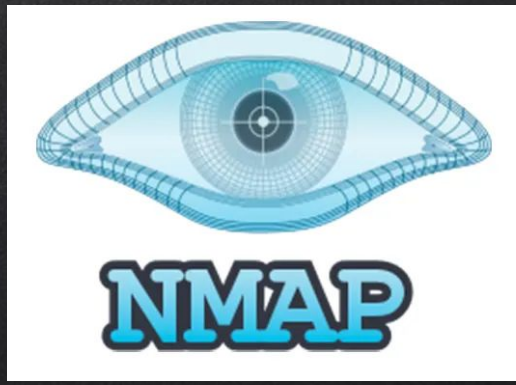


ETAPA 2: VARREDURA

X Softwares/sites que fazem varreduras buscando por vulnerabilidades:

- nmap
- nslookup
- Nessus
- ping
- nbtstat
- macof
- netdiscover
- smbclient
- SuperScan
- Pstools
- nikto
- owasp-zap
- Sqlmap
- Google Hacking





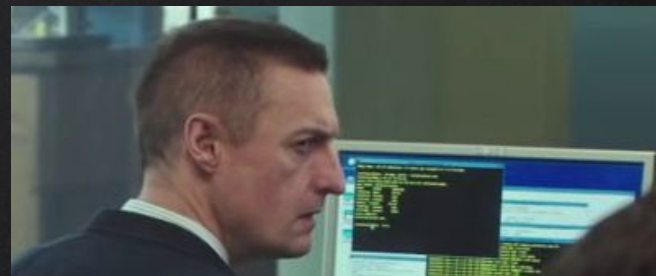
- ✗ Network Mapper
- ✗ Desenvolvido por Gordon “Fyodor” Lyon (1997)
- ✗ Possui modo gráfico (Zenmap)
- ✗ Permite escanear portas de rede
 - avaliar segurança de um dispositivo na rede
 - descobrir serviços e portas abertas



```
80/tcp    open      http
81/tcp    open      https
10.0.0.1   [mobile]
11 # nmap -u -sS -O 10.2.2.2
11
13 Starting nmap V. 2.54DETA25
13 Insufficient responses for TCP sequencing (3), OS detection i
13 accurate
14 Interesting ports on 10.2.2.2:
44 (The 1539 ports scanned but not shown below are in state: cl
51 Port      State       Service
51 22/tcp    open       ssh
58
68 No exact OS matches for host
68
74 Nmap run completed -- 1 IP address (1 host up) scanned
50 # sshnuke 10.2.2.2 -rootpw="Z10H0101"
Connecting to 10.2.2.2:ssh ... successful.
Re Attempting to exploit SSHv1 CRC32 ... successful.
IP Resetting root password to "Z10H0101".
System open: Access Level <9>
Na # ssh 10.2.2.2 -l root
root@10.2.2.2's password: [REDACTED]
```

ACCESS CONTROL
ACCESS GRANTED

```
calhost:~ # nmap -oP 10.14.0.0/24
calhost:~ # nmap -p1433 --script=ptast.nse
calhost:~ # tar cvfj sqlfiles.tar.tb2 /dbdump
calhost:~ # sudo nmap -oP 10.14.0.0/24
calhost:~ # tar --extract --file=sqlfiles.tar.br2 /dbdump
calhost:~ # bash #
```



NMAP – COMANDOS

- x -sT : varredura completa de portas TCP
- x -O : detecta SO
- x -sU : varredura UDP
- x -sO : varredura de IP
 - o quais protocolos IP são suportados
- x -sA: Varredura ACK: mapeia regras ativas no firewall

NESSUS

- ✕ Cliente / Servidor
- ✕ Verificação de falhas e vulnerabilidades
- ✕ <https://temp-mail.org/>
- ✕ Relatórios

OWASP ZAP

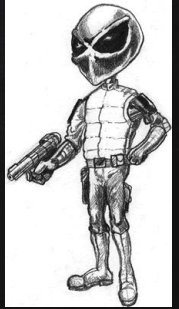


- ✘ OWASP (Open Web Application Security Project)
- ✘ ZAP (Zed Attack Proxy)
- ✘ Automatizar testes
 - <https://pypi.org/project/python-owasp-zap-v2.4/>
- ✘ Ataque Spider
 - <https://www.zaproxy.org/docs/desktop/start/features/spider/>
- ✘ Active Scan
 - requests e respostas resultantes de varredura ativa de um site

DIRBUSTER

- ✗ Também desenvolvida pela OWASP
- ✗ Dicionários
 - Dicionários pré-existent
 - `/opt/DirBuster/` ou `/usr/share/dirbuster/wordlists`
- ✗ Brute-force puro
 - Conjunto de caracteres deseja que sejam utilizados
 - Quantidade mínima e máxima de caracteres por tentativa.

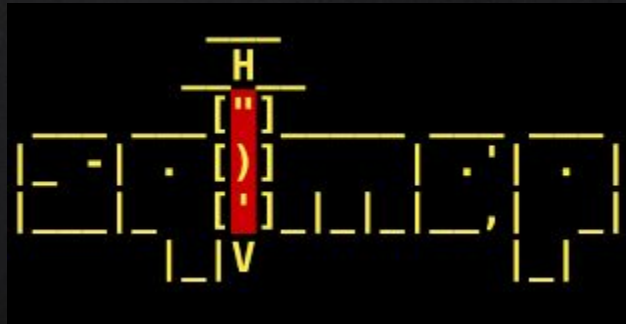
NIKTO



- ✗ Escrito em PERL
- ✗ Análise de vulnerabilidades comuns em servidores Web
- ✗ nikto -h <http://testphp.vulnweb.com>
- ✗ nikto -h <http://testphp.vulnweb.com> -evasion 1,2,3 -o relatorio.html

SQLMAP

- ✗ Open-source
- ✗ Python
- ✗ SQL Injection
- ✗ Procurar parâmetros via GET



SQL MAP – COMANDOS

- ✗ `sqlmap -u URL --dbs`
- ✗ `sqlmap -u URL -D NOME_BASE --tables`
- ✗ `sqlmap -u URL -D NOME_BASE -T NOME_TABELA --dump`

ATIVIDADE

- ✗ Utilizar uma das ferramentas apresentadas
 - se possível, via Kali Linux em VMWARE
 - <https://www.kali.org/downloads/>
 - Kali Linux 64-bit VMware
- ✗ Pesquisar vulnerabilidades no site <http://testphp.vulnweb.com>
 - ou em um dos sites do <http://www.vulnweb.com/>
- ✗ Escrever um breve relatório sobre uma vulnerabilidade encontrada
 - impactos
 - possíveis formas de correção
- ✗ 1 página



DÚVIDAS?

- ✗ Não esqueça de enviar sua maior dúvida pelo link que está no Classroom.
- ✗ Críticas/Sugestões: ezarpelao@unaerp.br

CREDITS

Special thanks to all the people who made and released these awesome resources for free:

- ✕ Presentation template by [SlidesCarnival](#)
- ✕ Photographs by [Unsplash](#)