Ferramentas adicionais para reconhecimento (além do PortScan)

nslookup / dig

Estas ferramentas de linha de comando permitem fazer consultas DNS dos tipos A, NS, MX, PTR, entre outros. No laboratório de DNS, utilizamos o comando:

```
nslookup -type=NS brasil.gov.br
```

para descobrir quais servidores de nomes têm autoridade sobre o domínio “brasil.gov.br”. Esse procedimento é essencial para entender a hierarquia DNS do alvo e direcionar consultas posteriores aos servidores corretos.

dnsenum

O dnsenum é um script Perl multithread que automatiza a enumeração DNS, incluindo tentativa de transferência de zona e brute-force de subdomínios a partir de listas de palavras. No exercício de força-bruta com o domínio avelinux.com.br, executamos:

```
dnsenum –f /usr/share/dnsenum/dns.txt avelinux.com.br
```

e identificamos vários subdomínios internos que não estavam documentados em buscas públicas, revelando hosts utilizados para serviços internos.

theHarvester

Ferramenta em Python que coleta informações públicas (e-mails, subdomínios, nomes de host e usuários) a partir de motores de busca e repositórios online. Durante o pentest na Ekkopark, rodei:

```
theHarvester –d ekkopark.com.br –b google
```

para extrair endereços de e-mail de funcionários e subdomínios expostos. Esses dados foram cruciais para montar um inventário inicial e planejar testes de engenharia social.

Shodan CLI

O Shodan é um motor de busca especializado em dispositivos conectados à Internet (IoT, SCADA, webcams, gateways industriais). Na Ekkopark, usei:

```
shodan host:203.0.113.10
```

para descobrir que um gateway industrial estava exposto, indicando uma falha de configuração que não seria visível em um simples port scan genérico.

whois

Ferramenta padrão para consulta de registros de domínio (registrante, datas de expiração, servidores de nomes autoritativos). Antes de qualquer varredura profunda na Ekkopark, executei:

```
whois ekkopark.com.br
```

para obter dados de contato administrativo e prazos de renovação. Essas informações são fundamentais para planejar notificações formais e entender o ciclo de vida do domínio usado pelo cliente.

Diferença entre SYN Scan e TCP Connect Scan

No **SYN Scan** (Nmap `-sS`), o scanner envia apenas o pacote SYN inicial e aguarda a resposta SYN-ACK (porta aberta) ou RST (porta fechada), sem concluir o handshake TCP. Isso gera menos entradas de log no alvo e torna o scan mais furtivo, mas exige privilégios de root ou administrador. É ideal em cenários onde se deseja evitar detecção por IDS/IPS em redes internas ou externas controladas.

No **TCP Connect Scan** (Nmap `-sT`), a ferramenta utiliza a chamada padrão do sistema operacional (`connect()`), completa todo o handshake TCP (SYN, SYN-ACK, ACK) e funciona sem privilégios elevados, mas deixa rastros completos de conexão nos logs do alvo, sendo mais fácil de detectar. Em geral, escolhe-se SYN Scan quando se tem acesso root e se busca furtividade, e TCP Connect Scan quando não se dispõe de privilégios de administrador ou quando half-open scans são bloqueados por firewalls.

Técnicas para evitar detecção por IPS durante o reconhecimento

Fragmentação de pacotes (-f)

Divide cada pacote TCP/UDP em fragmentos menores, o que dificulta que o IPS reconstrua o tráfego e reconheça assinaturas conhecidas. Essa técnica reduz alertas, mas aumenta o número de pacotes e o tempo total do scan.

Controle de taxa de envio (--scan-delay, --max-rate)

Insere atrasos entre os probes ou limita o throughput de pacotes por segundo, evitando picos de tráfego característicos de scans e reduzindo a chance de disparar alarmes no IPS.

Uso de decoys (-D)

Mistura IPs falsos junto com o IP real nos probes enviados, confundindo o IPS/IDS sobre qual máquina é a origem do scan e diluindo o tráfego malicioso.

Randomização de portas de origem e ordem de varredura (--source-port, --randomize-hosts)

Varia a porta de origem e embaralha a sequência de IPs e portas testadas, quebrando padrões previsíveis que assinaturas estáticas do IPS poderiam detectar.

Roteamento via VPN, proxies ou Tor

Encaminha o tráfego por múltiplos nós ou túneis, mascarando a origem real do scan e distribuindo o tráfego entre diferentes endpoints. Embora aumente latência e possa limitar a largura de banda, essa abordagem dificulta o bloqueio simples de um único endereço IP.