Relatório Técnico – TargetRecon

Disciplina: TecHacker
Professor: Rodolfo Avelino
Aluno: Raphael Cavalcanti Banov

---

1. Pesquisa e definição de ferramentas

1. Além do PortScan, quais são as 5 ferramentas mais úteis para reconhecimento em um pentest?

- **Nmap**: Ferramenta para enumeração e mapeamento de hosts, escaneamento de portas e detecção de serviços. Útil para reconhecimento em qualquer rede.
- **theHarvester**: Busca e coleta e-mails e nomes associados a domínios usando fontes públicas como Google, LinkedIn, etc. Ideal para engenharia social.
- **Shodan**: Uma engine de busca para dispositivos conectados à internet. Útil, principalmente, para descobrir sistemas expostos e vulneráveis, especialmente para dispositivos IoT.
- **Amass**: Especializado em enumeração de subdomínios e estrutura de DNS. Auxilia na visualização da superfície de ataque de grandes domínios.
- **Wappalyzer CLI**: Identifica tecnologias utilizadas por websites (servidores, frameworks, CMS), útil para reconhecimento passivo e planejamento de exploração.

2. Qual a diferença entre um scanner de portas SYN e um TCP Connect Scan?

- **SYN Scan**: é um tipo de escaneamento de porta usado para determinar quais portas de um host estão abertas, fechadas ou filtradas. Envia pacotes SYN e interpreta a resposta sem completar o handshake. Mais rápido e menos detectável, usado com root/admin (Ex: `nmap -sS`).
- **TCP Connect Scan**: Usa do próprio sistema operacional para realizar o handshake completo de três vias (SYN, SYN-ACK e ACK). Mais visível, mas funciona sem privilégios elevados (Ex: `nmap -sT`).

Cenário de uso:

- SYN scan é ideal para varreduras rápidas onde procura-se priorizar a baixa vizibilidade.
- TCP Connect é útil quando não há permissão de root.

3. Como um pentester pode evitar ser detectado por sistemas de prevenção deintrusão (IPS) durante o reconhecimento?

Técnicas:

- **Uso de VPNs**: Dificulta rastreamento da origem.
- **Evitar fingerprinting explícito**: Desativar banners e coletas excessivas que pode acionar alertas.
- **Foco em reconhecimento passivo**: Usa fontes públicas ao invés de interações diretas (ex: `whois`, `Shodan`, `theHarvester`).

---

2. Arquitetura e Decisões de Design

- Estrutura modular em Python.
- CLI interativa baseada em menus.
- Ferramentas integradas via `subprocess` com controle de erros.
- Uso de `ThreadPoolExecutor` para varredura paralela de portas e subdomínios.
- Arquivos externos simples como `subdomains.txt` permitem personalização sem alterar o código.

---

3. Ferramentas Integradas

Ferramenta	Finalidade	Modo de Integração
PortScan	Escaneamento TCP/UDP	Implementado nativamente
whois	Consulta de informações de domínio	subprocess (whois)
wafw00f	Detecção de firewalls de aplicação web	subprocess (wafw00f)
dirb	Fuzzing de diretórios e arquivos em servidores	subprocess (dirb)
nikto	Varredura de vulnerabilidades web	subprocess (nikto)

---

4. Resultados de Testes

Para fins de testes não invasivos, foram realizados com domínio `http://testphp.vulnweb.com`, que é um ambiente de testes público para ferramentas de segurança web, disponibilizado pela empresa Acunetix:

- **PortScan TCP/UDP**: Detectou portas 80 (HTTP) e 443 (HTTPS) abertas.
- **whois**: Retornou dados do registrante via ARIN.
- **wafw00f**: Detectou ausência de WAF.
- **dirb**: Encontrou diretórios `/admin`, `/images`, `/uploads`.
- **nikto**: Indicou headers mal configurados e arquivos `.bak` expostos.
