

Introdução

- Hacker
- Vulnerabilidade
- Exploit
- Payload

- Exploit Chain
- Zero-Day
- Target of Evaluation
- Dosing

- Confidencialidade
- Integridade
- Disponibilidade
- Autenticidade
- Não-Rejeição

- Segurança
- Funcionalidade
- Usabilidade

Motivação: perturbação; roubo de informações

Vulnerabilidade: algo que sera explorado

Método: forma de explorar a vulnerabilidade

Ativo: algo com valor para a organização e que pode motivar um ataque

Ameaça: origem possível de danos aos ativos

→ natural

→ à segurança física

humana

- à rede
- à máquina
- à aplicação

Análise de Risco: PROBABILIDADE × IMPACTO

Defesas em Profundidade:

1. Aplicação
2. Máquina
3. Rede Interna
4. Perímetro
5. Física
6. Políticas, Procedimentos e Conscientização

Mecanismos de Controlo:

1. Físicos
2. Técnicos
3. Administrativos
4. Preventivos/Corretivos

Gestão de Incidentes:

1. Preparação
2. Detecção e Análise
3. Clasificação e Priorização
4. Notificação
5. Capacidade de Resposta
6. Contenção
7. Investigação Forense
8. Erradicação e Recuperação
9. Atividades Pós-Incidente

Cracking: geralmente não autorizado, ilegal, com intenção de utilizar o sistema para fins não previstos e/ou causar dano.

(Ethical) Hacking: autorizado, com intenção de efetuar diagnóstico, encontrar vulnerabilidades (pode causar dano), para melhorar a proteção.

Fases do Hacking:

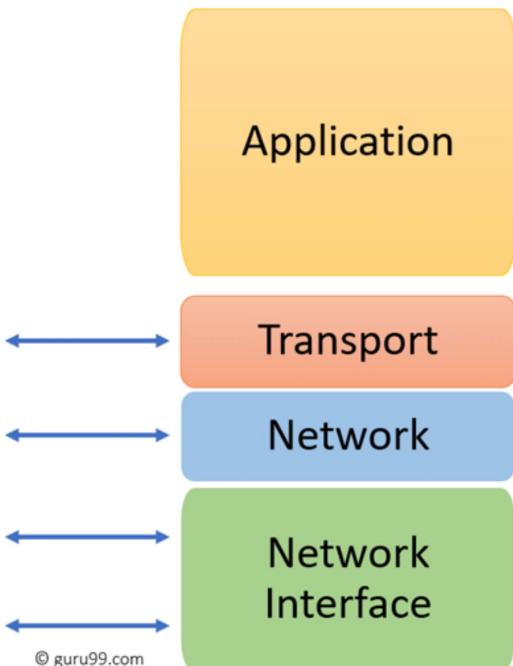
1. Reconhecimento Passivo/Ativo e Levantamento
2. Identificação de Vulnerabilidades
3. Exploração de Vulnerabilidades
4. Acesso
5. Manter Acesso

Redes & Reconhecimento

OSI Reference Model



TCP/IP Conceptual Layers



Reconhecimento: recolha de informação

Reconhecimento Passivo: fontes públicas – endereços IP, redes, servidores, SOs, serviços, arquiteturas, IDS, tecnologias, ...

Reconhecimento Ativo: enumeração de subdomínios, scan de portas, ferramentas de descoberta, força bruta, engenharia social, ...

Fontes: anónimos; aliases; organizações; internet

Informação Importante:

1. Rede: nomes de domínios, certificados SSL, intervalos de IP, redes internas, sites públicos, serviços expostos, protocolos, listas de controle de acessos e mecanismos de autenticação
2. Sistemas: utilizadores e grupos, banners, tabelas de rotas, arquitetura, sistemas operativos, software e versões
3. Organização: empregados, colaboradores, parceiros, telemóveis, sites, localizações, código "frontend", políticas de segurança, github,

Recon: processo de coletar toda a informação que permite a um atacante encontrar potenciais vetores de ataque dentro de um âmbito

↓ OBJETIVOS

1. Perceber a postura de segurança do alvo
2. Mapar a superfície de ataque
3. Construir uma base de conhecimento
4. Mapar os sistemas alvo, redes e serviços

Scan de URLs: um site, o código-fonte de frontend, os cookies e os cabeçalhos HTTP podem revelar o sistema operativo, tecnologias e versões, a estrutura do diretório e zones dos ficheiros, informação do editor de código e informações pessoais, ...

DNS:

1. A - endereço IP
2. AAAA - IP v6
3. MX - mail
4. NS - DNS
5. CNAME - nome alternativo
6. SOA - autoridade
7. TXT - texto
8. HINFO - informação sobre o anfitrião

Scan de Redes

Scan de Redes: mecanismos que permitem identificar máquinas, portas e serviços numa rede - obter informação a partir de respostas ou falta delas

Objetivo: identificar canais de comunicação que podem ser usados para lançar ataques

- Máquinas
- Portos Abertos
- Sistemas Operativos
- Anfitriões Ativos
- Serviços
- Versões e Erros de Configuração

Scans: 1. Redes 2. Portos 3. Tecnologias 4. Vulnerabilidades

Scan ICMP: 1. ECHO - ping 2. TIMESTAMP 3. NETMASK

Como usar NMAP?

1. Identificar sub-redes
2. Calcular número de anfitriões e intervalos de rede
3. Realizar varrimento ping

Scan de Portos: TCP - 1. SYN 2. SYN-ACK 3. ACK 4. SEQ 5. FIN/RST

"open": alcançável e aceita conexões - SYN/ACK

"closed": alcançável mas não aceita conexões - RST

"unfiltered": alcançável mas não se sabe se está aberto

"filtered": não se sabe se está aberto - nem resposta

"Banner Grabbing": técnica para perceber o SO e as versões dos serviços do host

Passivo: fazer "sniff" de pacotes na rede e "parse" de mensagens de erro

Ativo: enviar pacotes específicos

ENUMERAÇÃO

Enumeração: identificação de informações importantes que pode levar a múltiplos vetores de ataque

NetBIOS: serviço/API que permite listar recursos disponíveis na rede

SNMP: usado para gerir dispositivos de rede na rede

NTP: permite que "hosts" obtenham informação sobre o tempo de um dado "host"

LDAP: permite centralizar operações de autenticação de utilizadores

SMTP: protocolo para entrega de e-mails - VRFY; EXPN; RCPT TO

PALAVRAS-PASSE

Ataque Passivo: "man in the middle"; "sniffing"; ataques de repetição

Ataque Ativo: adquirir palavras-passe; trojans; spyware; keyloggers; phishing

Linux: /etc/shadow

Windows: SAM

MECANISMOS DE ANONIMIZAÇÃO

Proxy: para controlar, encaminhar e anonimizar tráfego de rede

VPN: torna uma conexão privada acessível a partir de uma rede pública

TOR: rede composta de nós voluntários

Túnel HTTP/SSH

Engenharia Reversa

Engenharia Reversa: descobrir o comportamento oculto/escondido de uma dada tecnologia, sistema, programa, protocolo ou dispositivo, ao analisar a estrutura e a operação dos seus componentes — extrai conhecimento sobre engenharia desconhecida

Engenharia Reversa Binária: processo de obter conhecimento sobre software compilado, de maneira a compreender como funciona e como foi originalmente implementado
→ tem o código fonte!

Formatos Compilados: ELF, PE, Class, PYC, Mach-O, DEX, ...

Desassemblier: traduz código máquina para assembly

Debugger: usado para testar outros programas

Decompilei: tenta traduzir software compilado no código fonte original

Patcher: altera o código máquina de maneira a modificar o comportamento original

Análise Estática: não executar o programa

Análise Dinâmica: executar o programa

→ Sintaxe Intel: operando, destino, origem

→ Registos

→ Operações

→ Flags

Sniffing & Malware

Wiretapping: escutar um canal de comunicação usado por entidades para trocar informação

Sniffing de Pacotes: capturar pacotes gerados por entidades legítimas numa rede ou canal de comunicação físico ou pelo ar

1. Inundação MAC: inundar um switch com novos endereços MAC de modo que a filtração não seja feita de maneira eficiente
2. "Rogue" DHCP: atuar como um servidor DHCP e fazer "broadcast" de um endereço de router/gateway malicioso
3. Envenenamento DNS: redirecionar máquinas para proxies maliciosos
4. Envenenamento ARP: fazer "spoof" do endereço IP da vítima e associá-lo com o endereço MAC do atacante
5. SSL Strip
6. MAC/IRDP "Spoofing"

MALWARE

→ Ambiente Seguro

Análise Estática: não executar o malware

Análise Dinâmica: observar e controlar malware em tempo de execução

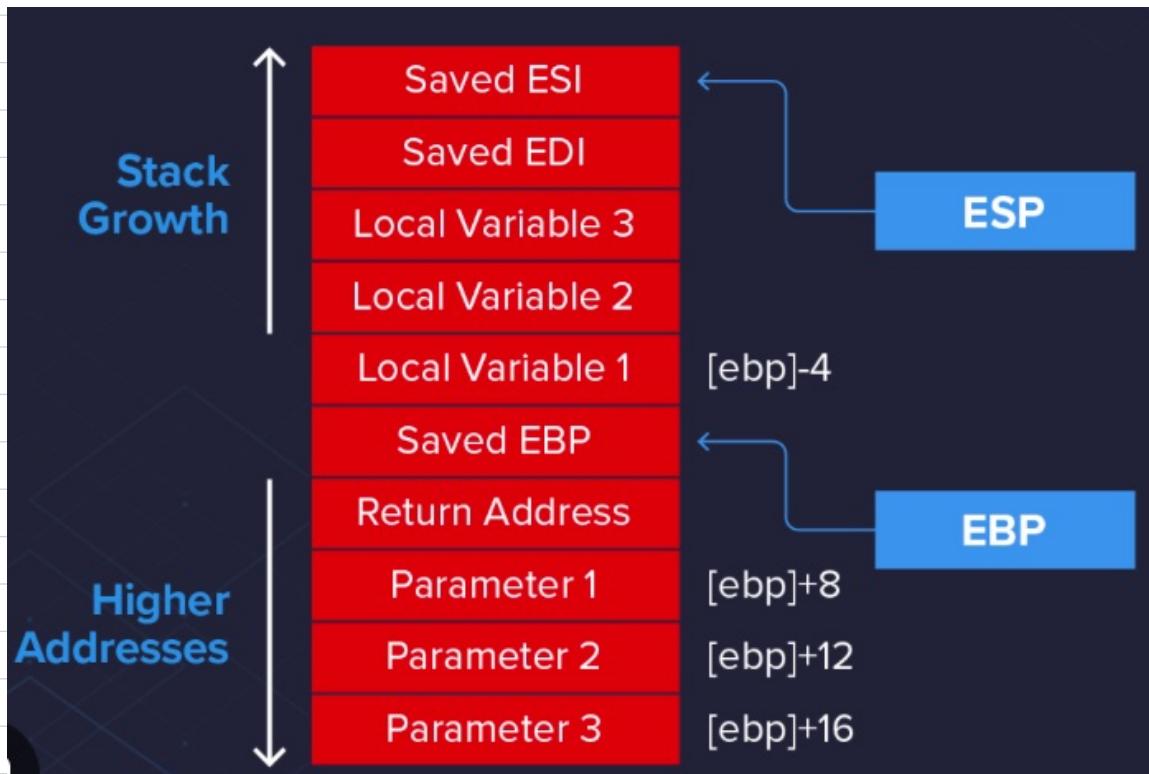
1. Packers: uso de compressão
2. Cryptors: uso de criptografia para obfuscar segmentos de código
3. Protectors: packers + cryptors + técnicas anti-debugging/manipulação

Binários

Binário: executável (.EXE ou .ELF) que corre numa máquina
PWN: pesquisa de vulnerabilidades e desenvolvimento de exploits

Binary Exploitation: alterar os dados que o programa de forma não impõe
→ Tamanhos dos Arrays!

"**Endianess**": como os dados são armazenados em memória
"**Little Endian**": $0x1234 \rightarrow 0x34\ 0x12$



Web

Um endereço IP pode ter múltiplas aplicações web — pode ser possível aceder a "virtual hosts" não sujeitos às contornos restrições e mecanismos de autenticação

Cookie: par de dados chave-valor enviado pelo servidor que reside no cliente por um período fixo de tempo

- Cookies adicionados para um subdomínio só podem ser lidos nesse subdomínio e nos seus subdomínios
- Um subdomínio pode definir cookies para os seus próprios subdomínios e pai, mas não pode definir cookies para domínios irmãos

Set-Cookie: Secure: não acessível por HTTPS **HTTP Only:** não acessível por JavaScript

Value	Cross-Site Cookies Sent?	Safe Methods Only?	Requires HTTPS?
Strict	No	N/A	No
Lax	Limited (safe methods only)	Yes	No
None	Yes	No	Yes

Cross-Site Request Forgery (CSRF): quando um atacante engana uma vítima a ir a uma página controlada pelo atacante, que depois submete dados ao site alvo como a vítima faz uma ação em nome da vítima, fazendo uso do comportamento dos cookies do navegador

↓ SOLUÇÃO

TOKENS CSRF

Cross Site Scripting (XSS): fazer TUDO em JavaScript no navegador da vítima no domínio afetado

1. Refletido: no URL
2. Armazenado: permanece de forma persistente no site cliente
3. DOM: o JavaScript não é enviado para o servidor, mas permanece do lado do cliente
4. Cego: o XSS ocorre noutro sitio

Local File Inclusion (LFI): permite ao atacante incluir um ficheiro local no servidor

Remote File Inclusion (RFI): inclusão de ficheiros remotos

Insecure Direct Object Reference (IDOR): aceder a um objeto ao qual não se devia ter acesso

SQL Injection

XML External Entity (XEE):

- XML permite definir novas entidades que podem ler ficheiros externos &...;
- Ataques aproveitam a capacidade de ler ficheiros e URI arbitrários
- Pode ser usado como um oráculo para saber se um ficheiro ou URI existe

Server Side Request Forgery (SSRF): um atacante faz com que uma aplicação faça a um pedido a uma localização indesejada

→ Segurança "Wireless"