53GUR4NC4 D4 INFORM4C40

474QU35

J1y4n y4R1

474QU35

71P05 D3 474QU35

474QU35

Footprinting

Tarefa de coletar informaçõES sobre um sistema alvo; - feita por vias tradicionais e públicas, como uso do finger, leitura de páginas do site para obter dados interessantes, etc.;

- ferramentas:
- engenharia social;
- port-scanner;
- analisadores de vulnerabilidades;
- ferramentas de redes e etc.

0000 0100

474QU35

SCANNING

- VERIFICA VULNERABILIDADES;
- SCANEIA PORTAS, SERVIÇOS, FIREWALL E ETC.
- PODE SER UM SCANNER DE SISTEMA, QUANDO CHECA VULNERABILIDADES NA MÁQUINA LOCAL (ERROS NO /ETC/PASSWD, PERMISSÃO INCORRETA DE ARQUIVOS, ETC.);
- PODE SER UM SCANNER DE REDE, QUANDO FAZ VARREDURA DE PORTAS DE REDES, VERIFICANDO QUAIS ESTÃO ABERTAS E, PRINCIPALMENTE, QUAIS ESTÃO MAIS VULNERÁVEIS;
- O OBJETIVO PRINCIPAL DESSE TIPO DE ATAQUE É DESCOBRIR FALHAS DE SEGURANÇA DEVIDO A BUGS EM SERVIÇOS DE REDE OU AUSÊNCIA DE PROTEÇÃO PARA SERVIÇOS INTERNOS.

474QU35

Sniffers

- usado geralmente dentro de uma rede quando física; - usada de fora quando uma rede Wireless;

- aplicativo que fica "escutando" todos os pacotes de dados que trafegam por uma dada interface de rede;

- objetiva principalmente a captura de senhas de usuários internos;

- ou a captura de outras informaçõES confidenciais em trânsito na rede

474QU35

Spoofing

- tarefa de fazer uma máquina se passar por outra, forjando, por exemplo, pacotes IP;

- o atacante tenta bloquear o envio de pacotes de dados de uma máquina, tentando se passar por ela (Man-In-TheMiddle)

474QU35

Denial of Service (DoS) e DDos

- ataque que busca "derrubar" um serviço ou mesmo um servidor inteiro;

- o mais típico é o DDoS (Distributed DoS);

- no DdoS o atacante utiliza várias máquinas "zumbis" para enviar inúmeras requisições, ao mesmo tempo e de forma sincronizada a um mesmo servidor;

- isso consome a maior parte da largura de banda de rede ou sobrecarregar um dado daemon (serviço) fazendo com que não atenda requisições.

0000 0100

474QU35

Cavalos de Tróia (trojan horse ou trojan)

- código malicioso com finalidades ilícitas;

- executa ações em um computador criando uma porta para uma possível invasão sem a autorização do usuário;

Exemplos:

- Keylogger
- Screenlogger
- Backdoor
- Mouselogger
- Hijacker

0000 0100

474QU35

Vírus

- efetua ação não desejada pelo usuário (malware);

- uma vez ativado, irá se replicar e infectar, danificar ou deletar arquivos; - por definição vírus não podem infectar máquinas externas sem o auxílio humano (?).

Exemplo:

- pendrive infectado;

- e-mails com anexos-vírus;

- envio de arquivos de outros computadores via rede e etc.

0000 0100

474QU35

Worm (verme)

- código que pode infectar tanto a máquina local, quanto máquinas remotas, geralmente utilizando falhas de protocolos, serviços ou aplicativos.

474QU35

Exploit

- programas criados para explorar falhas, geralmente de bugs nos daemons de serviços ou falhas no código do kernel ou de módulos.

474QU35

Ataques de Senhas

- consiste em tentar descobrir a senha de um ou mais usuários por força bruta ou usando técnicas de heurísticas;

- em geral o invasor tenta obter uma cópia das senhas e efetuar um ataque de dicionário.

474QU35

BUFFER-OVERFLOW (ESTOURO DE PILHA)

- A "PILHA" FORNECE UM ESPAÇO ONDE SÃO ARMAZENADOS DIVERSOS DADOS (MEMÓRIA);

- "ESTOURA" A PILHA PARA QUE OS DADOS QUE "VAZAREM" SEJAM EXECUTADOS COMO CÓDIGO PELO PROCESSADOR OU ARMAZENADO EM UM ARQUIVO;

- TÊM SIDO LARGAMENTE UTILIZADA PARA A PENETRAÇÃO REMOTA DE COMPUTADORES LIGADOS A UMA REDE.

474QU35

Defacer (desfiguração ou pichação)

- técnica de alterar a página principal do site;
- Pode ser seguido de roubo de informações também;
- ataque do tipo "hacker ativismo" na maioria das vezes, com palavrões e xingando ou palavras e frases de efeito contra alguém ou alguma coisa ou algum órgão ou empresa.

474QU35

SQL-INJECTIONS

- TÉCNICA DE "INJETAR" COMANDOS SQL (CONSULTAS) VIA BARRA DE ENDEREÇOS DO NAVEGADOR OU VIA FORMULÁRIO WEB;

- O DB WEB RECEBE PARÂMETROS DO ATACANTE E RETORNA AS CONSULTAS BASEADO NAS FALHAS EM SEU CÓDIGO.

474QU35

HIJACK (SEQUESTRADOR)

- SEQUESTRAM A PÁGINA INICIAL DO NAVEGADOR;
- ALGUMAS VEZES TAMBÉM REDIRECIONAM TODA PÁGINA VISITADA PARA UMA OUTRA PÁGINA ESCOLHIDA PELO PROGRAMADOR DA PRAGA;
- INFECTAM O COMPUTADOR CLICANDO EM LINKS E OU VISITANDO PÁGINAS COM CÓDIGOS MALICIOSOS OU INSTALANDO PROGRAMAS COM ESSES TROJANS;

EXEMPLO:

- HAO123;
- BAIDU.

0000 0100

474QU35

KEYLOGGER (REGISTRADOR DE TECLADO)

- PROGRAMA CUJA FINALIDADE É MONITORAR E GRAVAR TODO O BUFFER DE TECLADO, GRAVANDO-O EM UM ARQUIVO E POSTERIORMENTE ENVIANDO A ELE;
- FINALIDADE DE ROUBAR SENHAS DE BANCO, NÚMEROS DE CARTÃO DE CRÉDITO E AFINS, ENFIM, TUDO QUE FOR INSERIDO VIA TECLADO;
- O USUÁRIO GERALMENTE NÃO PERCEBE SUA AÇÃO;
- PODE SER REMOVIDO COM FERRAMENTAS ESPECÍFICAS.

0000 0100

474QU35

Cross-site scripting (XSS)

- injeção de scripts por meio de campo de input do usuário;

- ativam ataques maliciosos ao injetarem client-side script dentro das páginas web vistas por outros usuários;

- Para evitar não se deve permitir input de usuários.

Exemplo:

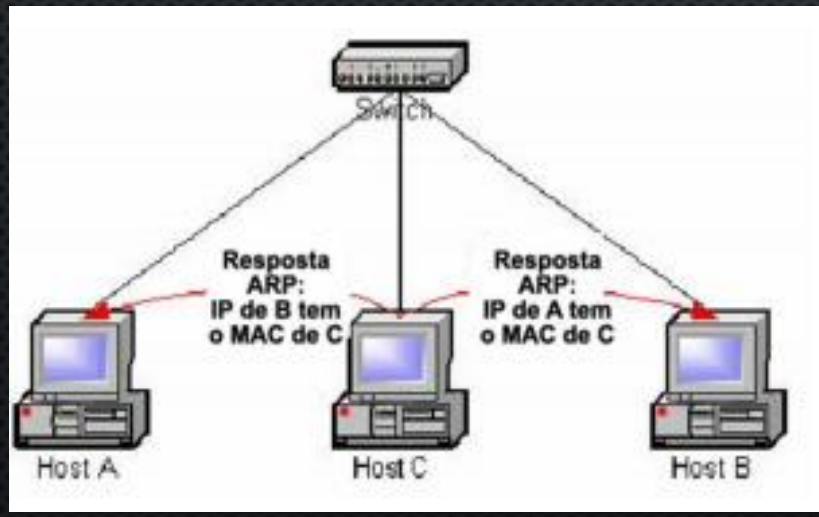
<script>malicious.js... = SYN

browser = ACK

474QU35

ARP Spoofing (ARP-Poisoning)

-meio mais eficiente de executar o ataque conhecido por Man-In-The-Middle: permite que o atacante intercepte informações confidenciais posicionando-se no meio de uma conexão entre dois ou mais hosts.



0000 0100

474QU35

DNS Spoofing (envenenamento de cache DNS)

- ataque no qual os dados são introduzidos em um Sistema de Nomes de Dominio (DNS) do banco de dados cache dos nomes do servidor, fazendo com que o nome do servidor redirecione para o endereço IP incorreto, desviando o tráfego para outro computador ou site (muitas vezes o do atacante).

Ferramentas:

- ettercap;
- nmap.

0000 0100

474QU35

DNS Spoofing (envenenamento de cache DNS)

Solução:

- DNS reverso;
- não utilizar os serviços rexec, rlogin e rsh;
- IDS (Intrusion Detection System);
- IPS (Intrusion Prevention System).

474QU35

Engenharia Social

- Ataque em que se faz uso da persuasão e convencimento;

- na maioria das vezes abusa da ingenuidade e ou confiança do usuário para obter informações que podem ser utilizadas para ter acesso não autorizado a computadores ou informações.