Insper

Tecnologias Hacker

Aula – Ataques de credenciais

Objetivos da aula

- Conhecer os tipos de ataques a senhas;
- Explorar as características do armazenamento de senhas dos sistemas operacionais Windows e gnu/Linux;
- Criar e Utilizar lista de palavras;
- Explorar hashes de senhas.

Tipos de ataques a senhas

- ONLINE

Com uso de *scans* automatizados e scripts para tentar fazer login automaticamente em serviços para descobrir credenciais válidas.

- OFFLINE

Por meio de uma cópia das hashes de senha tentar revertê-las para seu formato texto claro.

Algumas técnicas para quebrar senhas

Ataque de dicionário

Por meio de uma lista de palavras conhecidas e possíveis senhas em um software que irá testar cada uma delas para tentar recuperar a senha. Sistemas

Força Bruta

Tentativa de várias combinações de caracteres até achar a senha correta.

Híbrida

Usa dicionário com alguns passos adicionais (ou modificações) como parte do processo. Ex: password por p@ss0rd

Rainbow Tables

São tabelas que calculam todas as combinações possíveis de caracteres antes de capturar uma senha.
Em posse desta tabela é possível por meio de uma hash de senha (capturada or diversas formas) compará-lo com os hashes geradas.

Senhas

Armazenamento de senhas de SO

Windows

Security Accounts Manager (SAM)

c:\windows\system32\config\SAM

c:\windows\system32\config\SYSTEM

Linux

/etc/passwd → armazena os UID e nome de users

/etc/shadow → armazena os hashes das senhas

Arquivo SAM

O Arquivo SAM, armazena hashes de senha do Windows. Este banco de dados é protegido pelo Utilitário Windows Syskey, que criptografa as hashes das senhas no arquivo SAM com o RC4 de 128 bits, provendo uma segurança adicional.

Recuperando hashes a partir do SAM

Mesmo de posse do arquivo SAM, será necessário da chave criptografica para reverter as hashes criptografadas.

A chave de criptografia do utilitário Syskey chama-se bootkey. A chave está armazenada no arquivo SYSTEM, no mesmo diretório config.

Shadow

Identificador 1 hash senha e algoritmo ($6)

$1 = Algoritmo de hash MD5.
$2 = Algoritmo de hash Blowfish.
$2a= Algoritmo de hash eksblowfish.
$5 = Algoritmo de hash SHA-256.
$6 = Algoritmo de hash SHA-512.

Identificador 2 > Última alteração de senha (última alteração) : dias desde 1º de janeiro de 1970 em que a senha foi alterada pela última vez.

Identificador 3 > Mínimo : O número mínimo de dias necessários entre as alterações de senha, ou seja, o número de dias restantes para que o usuário possa alterar sua senha.

Identificador 4 > Máximo : o número máximo de dias em que a senha é válida (depois que o usuário é forçado a alterar sua senha).

Identificador 5 > Aviso : o número de dias antes da senha expirar, o usuário é avisado de que sua senha deve ser alterada.

Criação de Listas de Palavras

- Lista de usuários
  - Procure usar o padrão de nomes do cliente (primeiro nome.sobrenome ; primeira letra do nome.sobrenome);
  - Existem diversas listas disponíveis na Internet, contudo, devemos levar em consideração que várias são de nomes estrangeiros.

Criação de Listas de Palavras

- Criação de listas personalizadas com ceWL

cewl -w minhawords.txt -d 1 -m 5 alvo

-w → arquivo que será criado
-d → especifica quantos links o cewl deverá seguir
-m → tamanho mínimo da senha
Alvo → ip ou domínio

Criação de Listas de Palavras

- Criação de listas personalizadas com crunch

crunch 3 4 qwerty > palavra.txt

3 → mínimo de caracteres da senha
4 → máximo de caracteres da senha
palavra.txt → nome do arquivo que será criado com a wordlist.

Criação de Listas de Palavras

- Cupp

Script em Python que cria a wordlist a partir de um reposório de perguntas interativas.
Obtendo o cupp (https://github.com/Mebus/cupp)

Listas de Palavras com Python

./cupp3 -i

Descobrindo user e pass com hydra

hydra -L listausuarios.txt -P palavra.txt 10.0.0.102 ftp

-L → indicar o arquivo com a lista de nomes
-P → indicar a lista com a lista de senhas
10.0.0.102 → alvo
ftp → protocolo

Descobrindo senha com hydra

hydra -l aluno -P password.txt 10.0.0.102 ssh

-l → indicar o nome do usuário que deseja testar
-P → indicar a lista com a lista de senhas
10.0.0.102 → alvo
ftp → protocolo

Recuperando hashes a partir do SAM com samdump2

samdump2 -o hashes SYSTEM SAM

-o → nome do novo arquivo que vai receber as hashes.
SYSTEM → arquivo SYSTEM recuperado do sistema alvo.
SAM → arquivo SAM recuperado do sistema alvo.

Ferramentas para decifrar hashes

https://hashkiller.co.uk/

https://hashes.com

https://www.onlinehashcrack.com/hash-cracking.php

John the Riper

#cp /etc/shadow pass.txt

#john pass.txt

Repositório de wordlists

https://packetstormsecurity.com/Crackers/wordlists

http://openwall.com/wordlists/

No Kali

/usr/share/wordlists

/usr/share/john/password.lst

Scripts Nmap (Brute Force)

DNS→ nmap -p 80 --script dns-brute.nse <host>

Samba → nmap --script smb-brute.nse -p445 <host>

Http → nmap --script http-brute -p 80 <host>

FTP → nmap --script ftp-brute -p 21 <host>

Wordpress → nmap -sV --script http-wordpress-brute<target>