Ataque à senhas

Roberto Sadao Yokoyama

UTFPR-CP

Agosto, 2016

Prática de hoje[1]:

[1] Material baseado em [1]

Distribuição Linux para pentest

- Neste curso usaremos o Kali Linux como uma plataforma de teste vulnerabilidade
- Kali possui uma variedade de ferramentas de teste de invasão pré-instaladas

Download

https://www.kali.org/downloads/

Cenário

Objetivo

Verificar a segurança da senha de Bob no sistema Windows 7 utilizando um ataque de dicionário de senhas *off-line*.

Exemplos de como obter o(s) arquivo(s) de senhas:

- Atacante pode usar um boot pelo CD/DVD/pen-drive (falha na segurança física)
- Atacante consegue acesso remoto (falha de software)
- Bob deixa logado o computador (descuido do usuário)
- Atacante consegue o backup do sistema
- etc.

Ataque de dicionário *off-line*

Ferramentas:

- *samdum2*: extraí os valores de *hashing* dos aquivos de senha
- *John the Ripper*: utiliza a força bruta para descobrir a senha
  - dicionário disponível: /usr/share/john/password.lst
  - alteração automática no dicionário: editar o aquivo /etc/john/john.conf e abaixo de List.Rules:Wordlist adicionar uma regra, ex: $[0-9]$[0-9]$[0-9]$ – adiciona três números no final de cada palavra da lista
- *sites on-line*: https://crackstation.net/ – cracking hashes
- *sites de wordlists*: https://packetstormsecurity.com/Crackers/wordlists/ http://www.openwall.com/wordlists/

Passos:

Baixar os arquivos:
https://nuvem.utfpr.edu.br/index.php/s/AKeCN4Ok3N49BC1

- Gerar o arquivo de *hashes* a partir dos arquivos de senha
- Aplicar o dicionário de senhas no arquivo de *hashes*
- Caso não consiga recuperar a senha, pode-se atualizar o dicionário

- *#samdump2 SYSTEM SAM -o hashes.txt*
- *#john hashes.txt -user:Bob -format:NT - -show*
- *#vim /usr/share/john/password.lst*

Geração de listas

- ceWL: criar listas personalizadas de palavras que pesquisará o site (por exemplo, da empresa) a procura de palavras para sua lista
- *#cewl -w bulbwords.txt -d 1 -m 5 www.bulbsecurity.com*
- Crunch: cria uma lista com todas as combinações possíveis.
- *#crunch 7 7 AB*

Referências

[1] G. Weidman. *Teste de Invasão: Uma Introdução prática ao hacking*. Novatec, 2014.