3.3 - Quebra de Senha

prof. Fábio Engel

fabioe@utfpr.edu.br

Conteúdo

Ataques a senhas

Ataques a senhas

- Geralmente, as senhas representam o ponto que oferece a menor resistência em atividades de testes de invasão.
- Um cliente com um programa robusto de segurança pode corrigir a falta de patches do Windows e evitar a existência de softwares desatualizados, porém o usuários em si não podem ser corrigidos.

Ataques a senhas

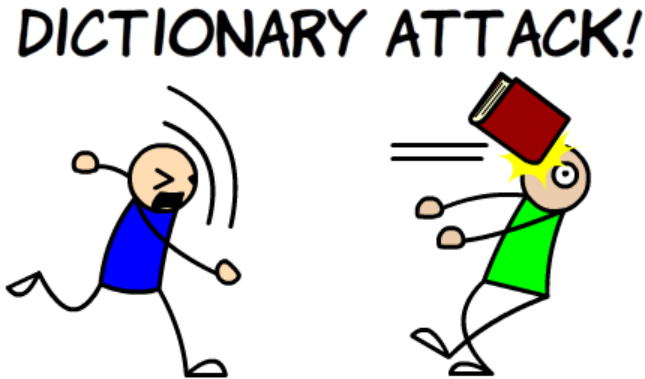
- Assim como usamos scans automatizado para descobrir vulnerabilidades, podemos usar scripts para tentar fazer login automaticamente em serviços e descobrir credenciais válidas.
- Utilizaremos ferramentas projetadas para automatizar ataques online a senhas ou para fornecer palpites para as senhas até o servidor responder com um login bem-sucedido. Essas ferramentas usam uma técnica chamada força bruta.

Ataques a senhas

- O problema da força bruta é que, à medida que senhas mais fortes são usadas, o tempo necessário para descobri-las por meio dessa técnica passa de horas para anos e até mesmo para um tempo maior que a duração natural de sua vida.
- Provavelmente, poderemos descobrir credenciais funcionais mais facilmente se fornecermos palpites embasados sobre as senhas corretas a uma ferramenta automatizada de login.

Ataques a senhas

- Listas de senhas disponíveis na Internet:
  - https://packetstormsecurity.com/Crackers/wordlists
  - http://www.openwall.com/wordlists/



Ataques a senhas

- Algumas listas de senha também estão incluídas no Kali Linux. Por exemplo, o diretório */usr/share/wordlists* contém um arquivos chamado *rockyou.txt.gz*. Esse arquivo contém uma lista de palavras compactada.
- Se o arquivo for descompactado com o utilitário gunzip do Linux, você terá cerca de 140 MB de senhas possíveis que poderão oferecer um bom ponto de partida.
- Além disso, algumas ferramentas para cracking de senhas no Kali vêm com amostras de listas de palavras.

Ataques a senhas

- Para obter melhores resultados, personalize suas listas de palavras para um alvo em particular por meio da inclusão de palavras adicionais.
- Palpites embasado podem ser fornecidos de acordo com informações obtidas online sobre os funcionários. As informações a respeito de cônjuges, filhos, animais de estimação e hobbies podem colocar você no caminho certo.

Ataques a senhas

- Além de dar palpites embasados em informações coletadas ao executar o reconhecimento, uma ferramenta com o o ceWL, que é um gerador de lista de palavras personalizadas, pesquisará o site de uma empresa à procura de palavras a serem adicionadas à sua lista.
- Você pode utilizar o *help* da ferramenta: **cewl –help**
- Exemplo para criar uma lista de palavras baseado no conteúdo de www.utfpr.edu.br
  - **cewl -w wordListUTFPR.txt -d 1 -m 5 www.utfpr.edu.br**
- A opção -d especifica quantos links o ceWL deve seguir no site-alvo. A opção -m define um tamanho mínimo de palavra, sendo 3 o valor padrão. A opção -w envia o resultado para o arquivo indicado.

Ataques a senhas

- O exemplo anterior, em um ambiente com proxy:
  - **cewl -w wordListTest.txt -d 1 -m 5 www.utfpr.edu.br −−proxy_host 10.1.5.250 −−proxy_port 3128 −−proxy_username nomeUsuario −−proxy_password senhaUsuario**

Ataques a senhas

- Outro método para criar listas de palavras consiste em gerar uma lista com todas as combinações possíveis de um dado conjunto de caracteres, ou uma lista com todas as combinações para uma quantidade especificada de caracteres.
- A ferramenta Crunch no Kali irá gerar esses conjuntos de caracteres para você. É claro que, quanto mais possibilidades houver, mais espaço em disco será necessário para o armazenamento.

Ataques a senhas

- Exemplo:
  - **crunch 2 3 ab -o dicionario.txt**
- No exemplo acima, uma lista é gerada com todas as combinações possíveis de 2 a 3 caracteres somente dos caracteres a e b. O conteúdo desta lista é armazenado no arquivo dicionario.txt.

Ataques a senhas

- crunch exemplo:
  - **crunch 9 9 1234567890 -t maria@@@@ -o dicionario.txt**
    Gera uma wordlist de palavras começando com "maria" seguidas de 4 números. O "@" marca os lugares que serão substituídos pelos caracteres indicados na linha de comando. Portanto, você pode colocá-los em qualquer lugar da string. Por exemplo, @@ maria modificaria apenas os dois primeiros caracteres e adicionaria "maria" ao final.

Ataques a senhas

- Dicas:
  - Limitar tamanho das palavras:
    grep -E '^.{,6}$' arquivo1.txt > arquivo2.txt
  - Converter para minúsculo:
    tr A-Z a-z < arquivo1.txt > arquivo2.txt

Ataques a senhas

- Se você tiver um conjunto de credenciais que gostaria de experimentar em um serviço em execução que exija login, elas poderão ser inseridas manualmente, uma por uma, ou você poderá usar uma ferramenta para automatizar o processo.
- O Hydra é uma ferramenta online para adivinhar senhas que pode ser usada para testar nomes de usuários e senhas em serviços que estejam executando.

Ataques a senhas

- Hydra Sintaxe:
  - **hydra -l username -p password -t threads IP protocol**
  - **hydra -L lista -P lista -t threads IP protocol**
- Argumentos:
  - -l Nome/login da vítima;
  - -L Carrega uma lista contendo nomes/logins de vítimas (1 por linha);
  - -p Especifica senha única;
  - -P Carrega uma lista com senhas (1 por linha);
  - -e Adiciona 'n', testa senha em branco ou adicional 's' testa user como pass;
  - -C Usado para carregar um arquivo contendo usuário:senha. Formato usuário:senha equivale a - L/-P;
  - -M Carrega lista de servidores alvos (1 por linha);
  - -o Salva as senhas encontradas dentro do arquivo que você especificar;
  - -f Faz o programa parar de trabalhar quando a senha ou usuário for encontrada[o];
  - -t Limita o numero de solicitações por vez (default: 16);
  - -w Define o tempo máximo em segundos para esperar resposta do servidor (default: 30s);
  - -v / -V Modo verbose do programa. 'V' mostra todas tentativas.

Ataques a senhas

- Hydra.
  - Exemplo para servidor ftp:
    - hydra -l usuario -P senhas.txt 192.168.0.33 ftp
  - Para autenticação via formulário web é necessário definir os parâmetros corretamente.
    - Utilizamos o burpsuite para obter estes parâmetros.
    - `https://portswigger.net/burp/communitydownload`

Ataques a senhas

- Outra maneira de quebrar senhas (sem ser descoberto) é obter uma cópia das hashes de senha e tentar revertê-las para o seu formato texto simples.
- As funções hashes são conhecidas por serem unidirecionais. Entretanto, podemos fornecer um palpite para uma senha, gerar seu hash usando a função unidirecional de hash e comparar o resultado com a hash conhecida. Se as duas hashes forem iguais, é porque descobrimos a senha correta.

Ataques a senhas

- Recuperando hashes de senha de um arquivo SAM do Windows
  - o arquivo SAM (C:\Windows\System32\config\SAM)armazena hashes de senha do Windows.
  - Entretanto, ao tentarmos ler o arquivo SAM, não conseguimos visualizar nenhum hash de senha.
  - O arquivo SAM permanece oculto porque o utilitário Windows Syskey criptografa as hashes das senhas no arquivo SAM com o RC4 (River Cipher 4) de 128 bits para prover uma segurança adicional. Mesmo que um invasor consiga ter acesso ao arquivo SAM, um pouco mais de trabalho será necessário para podermos recuperar as hashes das senhas. Especificamente, precisamos de uma chave para reverter as hashes criptografadas.

Ataques a senhas

- Recuperando hashes de senha de um arquivo SAM do Windows
  - A chave de criptografia do utilitário Syskey chama-se bootkey e está armazenada no arquivo SYSTEM do Windows, no mesmo local do arquivo SAM.
  - Podemos obter cópias dos arquivos SAM e SYSTEM por meio deste script de execução em lote. Crie um novo arquivo, insira o conteúdo abaixo e o salve com extensão .bat.
    - @echo off
      reg SAVE HKLM\SAM C:\SAM
      reg SAVE HKLM\SYSTEM C:\SYSTEM
      exit
  - Podemos utilizar uma ferramenta chamada samdump2 para extrair a bootkey do utilitário Syskey do arquivo SYSTEM para podermos descriptografar as hashes.
    - **samdump2 SYSTEM SAM -o hash.txt**

Ataques a senhas

- Alternativa:
  - http://www.onlinehashcrack.com/hash-generator.php

Ataques a senhas

- Exemplo de hash:
  Administrador❶:500❷:aad3b435b51404eeaad3b435b51404ee❸:31d63f20110a0901b73c59d7a0dc089c0❹
  Fabio❶:1000❷:aad3b435b51404eeaad3b435b51404ee❸:d5b4bc16fc43bc914c17dabae5579859a❹
- O primeiro campo nas hashes corresponde ao nome do usuário ❶; o segundo é o ID do usuário ❷; o terceiro é a hash no formato LM (LAN Manager) ❸ e o quarto é a hash NTLM (NT LAN Manager) ❹

Ataques a senhas

- A hash LM foi a primeira maneira de criar hashes de senha no Microsoft Windows e até o Windows NT, porém é um método de criptografia que não é robusto e possibilita a descoberta da senha correta em formato texto simples a partir de um hash LM, independente do tamanho e da complexidade da senha.
- A Microsoft introduziu a hashing NTLM para substituir a hash LM, porém, no Windows XP, as senhas são armazenadas tanto em formato LM quanto NTLM, por padrão. O Windows 7 opta exclusivamente pela hash NTLM, que é mais segura.

Ataques a senhas

- A utilização da entrada com a hash LM fará com que quebrar as hashes seja muito mais fácil.
- Com efeito, qualquer hash LM de senha pode ser quebrada por meio de força bruta em minutos ou horas.
- Em contrapartida, nossa capacidade de quebrar hashes NTLM dependerá tanto de nossa habilidade de adivinhar quanto do tamanho e da complexidade da senha.

Ataques a senhas

- Problema com hashes de senha LM
  - Hashes LM não são seguras, pois podemos recuperar o texto simples a partir da hash.
  - Uma matemática complexa é usada para desenvolver algoritmos que tornam impossível a descoberta do valor da senha original em formato texto simples submetida ao hashing. Porém, podemos submeter um palpite de senha em formato de texto simples ao algoritmo criptográfico de hashing e comparar o resultado com a hash que estamos tentando quebrar; se forem iguais, é porque descobrimos a senha correta.

Ataques a senhas

- Os problemas a seguir contribuem com a falta de segurança das hashes LM:
  - as senhas são truncadas em 14 caracteres;
  - as senhas são totalmente convertidas para letras maiúsculas;
  - as senhas com menos de 14 caracteres são preenchidas com nulo até terem 14 caracteres;
  - a senha de 14 caracteres é dividida em duas senhas de sete caracteres que geram hashes separadas.

Ataques a senhas

- Por que essas características são tão significativas? Suponha que tenhamos partido de uma senha complexa e robusta como esta:
  - T3LF23!+?sRty$J
- Essa senha tem 15 caracteres de quatro classes que incluem letras minúsculas, letras maiúsculas, números e símbolos, e não corresponde a uma palavra que possa ser encontrada em um dicionário. No entanto, no algoritmo de hash LM, a senha é truncada em 14 caracteres, desta maneira:
  - T3LF23!+?sRty$

Ataques a senhas

- Em seguida, as letras minúsculas são convertidas em letras maiúsculas:
  - T3LF23!+?SRTY$

Ataques a senhas

- A seguir, a senha é dividida em duas partes de sete caracteres cada. As duas partes são então usadas como chaves para criptografar a string estática KGS!@#$% usando o algoritmo de criptografia DES (*Data Encryption Standard*)
  - T3LF23! +?SRTY$
- Os textos cifrados de oito caracteres resultantes da criptografia são então concatenados para compor a hash LM.

Ataques a senhas

- Para quebrar uma hash LM, basta descobrirmos os sete caracteres, todos maiúsculos, talvez com alguns números e símbolos. O hardware moderno dos computadores pode tentar todas as combinações de um a sete caracteres, criptografar a string KGS!@#$% e comparar a hash resultante com um dado valor em questão de minutos a horas.

Ataques a senhas

- Uma das ferramentas mais populares para quebras de senha é o John the Ripper.
- O modo *default* do John the Ripper é aquele em que a força bruta é usada. Pelo fato de o conjunto das senhas possíveis em formato texto simples em hashes LM ser tão limitado, a força bruta é um método viável para quebrar qualquer hash LM em um intervalo de tempo razoável.

Ataques a senhas

- Em termos de facilidade, quebrar hashes NTLM do Windows não chega nem perto de quebrar hashes LM.
- Embora uma senha NTLM de cinco caracteres que use somente letras minúsculas e nenhum outro tipo de complexidade possa ser quebrada por meio de força bruta tão rapidamente quanto uma hash LM, uma senha NTLM de 30 caracteres com diversos tipos de complexidade pode exigir vários anos para ser quebrada.

Ataques a senhas

- Quebrando hashes LM e NT com o John the Ripper:
  - john –format=nt senhas.txt
  - john –format=nt senhas.txt ––show
- Onde senhas.txt é o arquivo com as hashes dos usuários do windows.

Ataques a senhas

- **Tabelas Rainbow**
  - Em vez de usar uma lista de palavras, gerar a hash de cada entrada com o algoritmo relevante e comparar a hash resultante com o valor a ser quebrado, podemos agilizar consideravelmente esse processo se tivermos uma lista de palavras com as hashes previamente geradas. Isso, é claro, exigirá espaço para armazenamento - mais espaço para listas mais longas de hashes e tendendo ao infinito à medida que tentarmos armazenar todos os valores de hashes de todas a senhas possíveis para serem usadas com a força bruta.
  - Um conjunto de hashes pré-calculados é conhecido como uma tabela rainbow (*rainbow table*). Normalmente armazenam todas as entradas possíveis de hash para um dado algoritmo, até um determinado tamanho, com um conjunto limitado de caracteres.

Ataques a senhas

- Por exemplo, você pode ter uma tabela rainbow para hashes MD5 que contenha todas as entradas somente com letras minúsculas e números, com tamanhos entre um e nove caracteres.
- Esta tabela ocupa cerca de 80 GB - nada mal considerando o preço atual de armazenamento, mas tenha em mente que isso corresponde a uma quantidade bastante limitada para o keyspace possível com o MD5.
- Dado o keyspace limitado, um hash LM parece ser um candidato ideal para usar as tabelas rainbow. Um conjunto completo de tabelas rainbow para hash LM tem cerca de 32 GB.

Ataques a senhas

- Você pode baixar conjuntos previamente gerados de hashes a partir de http://project-rainbowcrack.com/table.htm
- A ferramenta Rcrack no Kali pode ser usada para pesquisar as tabelas rainbow em busca do formato texto simples correto.

Ataques a senhas

- Há também serviços online para quebra de senhas. Por exemplo, o https://www.cloudcracker.com/ pode quebrar hashes NTLM do Windows, SHA-512 do Linux, handshakes WPA2 para wireless etc.
- Basta fazer o upload de ser arquivo de hashes de senha e o cracker fará o resto.

Referências

- Testes de Invasão: Uma introdução prática ao hacking. Georgia Weidman. Ed. Novatec, 2014.
- http://remote-execution.blogspot.com.br/2011/05/wordlist-lista-de-palavras-para-ataque.html