Quebra de senha: Ataques off-line

Os ataques off-line representam ainda outra forma de ataque que é muito eficaz e difícil de detectar em muitos casos. Tais ataques dependem do atacante ser capaz de aprender como as senhas são armazenadas e, em seguida, usando essas informações, realizar um ataque. Veja abaixo um ataque de senha que extrai hashes.

Extraindo Hashes de um sistema

Agora que você viu que é possível extrair os hashes, vamos usar o *pwdump* para fazer este processo:

1. Abra o prompt de comando;
2. Execute *pwdump7.exe* para exibir os hashes do sistema;
3. Depois execute o comando *pwdump7.exe > C:\hash.txt*
4. Aperte ENTER;
5. Usando o notepad, navegue pelo diretório C: e abra o arquivo hash.txt e veja os hashes que tem no arquivo.

Hashes pré-computados ou Rainbow Tables

Os hashes pré-computados são usados em um tipo de ataque conhecido como Rainbow Tables. As tabelas Rainbow calculam todas as combinações possíveis de caracteres antes de capturar uma senha. Uma vez que todas as senhas foram geradas, o atacante pode capturar o hash de senha da rede e compará-lo com os hashes que já foram gerados.

Com todos os hashes gerados antes do tempo, torna-se uma questão simples comparar o hash capturado com os gerados, revelando a senha em alguns momentos.

A desvantagem do Rainbow Table é que eles levam tempo. Demora um período substancial, às vezes dias, para calcular todas as combinações de hash antes do tempo. Outra desvantagem é que você não pode quebrar senhas de comprimento ilimitado, porque a geração de senhas com maior comprimento leva mais tempo.

Gerando tabelas Rainbow

Você pode gerar as tabelas Rainbow de muitas maneiras. Um dos utilitários que você pode usar para executar esta tarefa é *winrtgen*, um gerador baseado em GUI. Os formatos de hash suportados neste utilitário incluem todos os seguintes:

- Cisco PIX
- FastLM
- HalfLMChall
- LM
- LMCHALL
- MD2
- MD4
- MD5
- MSCACHE
- MySQL323
- MySQLSHAl
- NTLM
- NTLMCHALL
- ORÁCULO
- RIPEMD-160
- SHA1
- SHA-2 (256), SHA-2 (384), SHA-2 (512)

Exercício abaixo demonstra como criar uma tabela Rainbow para quebra uma senha.

Criando a tabela Rainbow

Vamos criar uma tabela Rainbow para ver o processo. Lembre-se de que esse processo pode demorar um pouco.

Para executar este exercício, você precisará baixar o aplicativo *winrtgen*. Para usar *winrtgen*, siga estes passos:

1. Inicie a ferramenta *winrtgen.exe*;
2. Uma vez iniciado o *winrtgen*, clique no botão Add Table;
3. Na janela de Propriedades da Tabela Rainbow, faça o seguinte:
    1. Selecione NTLM na lista drop-down Hash;
    2. Definir comprimento mínimo para 4 e comprimento máximo para 9, com uma contagem de Cadeia de 4000000.
    3. Selecione *Loweralpha* na lista suspensa Charset;
4. Clique em OK para criar a tabela Rainbow.

Observe que a criação do arquivo de tabela Rainbow levará uma quantidade significativa de tempo, dependendo da velocidade do seu computador e as configurações que você escolher.

Os exercícios demonstrado executam dois passos vitais do processo: O primeiro extrai hashes de senhas de um sistema alvo e o outro exercício cria uma tabela Rainbow de potenciais correspondências. Agora que você executou essas duas etapas, você deve recuperar a senha, fazendo o próximo exercício.

Trabalhando com RainbowCrack

Depois de ter criado a tabela Rainbow, você pode usá-la para recuperar uma senha usando as informações do *pwdump* e *winrtgen*:

1. Clique duas vezes em *rcrack_gui.exe*.
2. Clique em File, e em seguida, clique em Add Hash. A janela Add Hash é aberta.

3. Se você executou *pwdump,* agora você pode abrir o arquivo de texto que ele criou e copiar e colar os hashes.
4. Clique em OK.
5. Clique em Rainbow Table na barra de menus e clique em Search Rainbow Table. Se você executou o *winrtgen,* você pode usar essa tabela Rainbow aqui.
6. Clique em Abrir.

Rainbow Tables é um método eficaz de revelar senhas, mas a eficácia do método pode ser diminuída através do Salt. Salting é usado em Linux, Unix e BSD, mas não é usado em alguns dos mais antigos mecanismos de autenticação do Windows, como LM e NTLM.

Salting um hash é um meio de adicionar entropia ou aleatoriedade para tornar sequências ou padrões mais difíceis de detectar. As tabelas Rainbow executam uma forma de criptoanálise. Salting tenta frustrar esta análise, adicionando aleatoriedade (por vezes conhecido como indução de entropia). Embora você ainda pode ser capaz de quebrar o sistema, será mais difícil de fazer.

Ataques de rede distribuídos

Uma das abordagens modernas para quebrar senhas é o Distributed Network Attack (DNA). Aproveita o poder de processamento não utilizado de vários computadores e tenta executar uma ação, neste caso, quebra de senha.

Para fazer esse ataque funcionar, você instala um gerenciador em um sistema escolhido, que é usado para gerenciar vários clientes. O gerente é responsável pela divisão e atribuição de trabalho aos vários sistemas envolvidos no processamento dos dados. No lado do cliente, o software recebe a unidade de trabalho atribuída, processa-a e devolve os resultados ao gestor.

O benefício deste tipo de ataque é o poder de computação bruta disponível. Este ataque combina pequenas quantidades de poder de computação de sistemas individuais em uma grande quantidade de poder de computação. O poder de processamento de cada computador é semelhante a uma única gota de água: individualmente eles são pequenos, mas juntos eles se tornam muito mais. As gotas formam corpos de água maiores e pequenos pedaços de poder de processamento se reúnem para formar um enorme pool de poder de processamento.

Senhas Padrão

Uma das maiores vulnerabilidades em potencial é também uma das mais fáceis de resolver: senhas padrão. As senhas padrão são definidas pelo fabricante quando o dispositivo ou sistema é construído. Eles são documentados e fornecidos ao consumidor final do produto e são destinados a serem alterados. No entanto, nem todos os usuários ou empresas fazem esta etapa, e, portanto, deixam-se vulneráveis. A realidade é que com um pouco de varredura e investigação, um atacante pode fazer algumas suposições educadas sobre o equipamento ou sistemas que você pode estar executando. Se eles podem determinar que você não alterou os padrões, eles podem procurar sua senha padrão em qualquer um dos seguintes sites:

- http://cirt.net
- http://default-password.info
- www.defaultpassword.us
- www.passwordsdatabase.com
- https://w3dt.net
- www.virus.org
- http://open-sez.me
- http://securityoverride.org
- www.routerpasswords.com
- www.fortypoundhead.com

Adivinhando

Embora seja um método velho, adivinhar senhas manualmente pode potencialmente produzir resultados interessantes, especialmente em ambientes onde boas práticas de senha não são seguidas. Simplificando, um invasor pode fazer o seguinte:

1. Localize um usuário válido;
2. Determine uma lista de senhas potenciais;
3. Classifique senhas possíveis de menos para mais provável;
4. Experimente senhas até que o acesso seja obtido ou as opções sejam esgotadas;

Este processo pode ser automatizado através do uso de scripts criados pelo atacante, mas ainda qualifica como um ataque manual.

Roubo de senhas USB

Em contraste com os métodos manuais, existem alguns mecanismos automatizados para obter senhas, como por meio de unidades USB. Este método implica a incorporação de um aplicativo de roubo de senha em uma unidade USB e, em seguida, fisicamente conectar a unidade em um sistema de destino.

Como muitos usuários armazenam suas senhas para aplicativos e sites on-line em sua máquina local, as senhas podem ser facilmente extraídas.

PSPV

Para realizar este ataque, você pode usar as seguintes etapas genéricas:

1. Obtenha um utilitário de hacking de senhas, como *pspv.exe*;
2. Copie o utilitário para uma unidade USB;

3. Crie um arquivo de bloco de notas chamado *launch.bat* contendo as seguintes linhas:
   [Autorun]
   En = launch.bat
   Start pspv.exe / s passwords.txt
   4. Salve *launch.bat* na unidade USB.

Neste ponto, você pode inserir a unidade USB em um computador de destino. Quando o fizer, pspv.exe será executado, extrairá as senhas e colocara-los no arquivo *passwords.txt*, que você pode abrir no Bloco de Notas.

Vale a pena notar que esse ataque pode ser evitado com bastante facilidade ao desativar a reprodução automática de dispositivos USB, que é ativado por padrão no Windows.

A ferramenta *pspv.exe* é um visualizador de senha que exibe senhas armazenadas em um sistema Windows, se elas estiverem contidas no Internet Explorer e em outros aplicativos.

No que diz respeito aos ataques USB, há muitas outras maneiras de roubar senhas e outros dados valiosos através deste mecanismo. Um dos métodos mais recentes está usando algo conhecido como o USB Rubber Ducky da Hak5. Este dispositivo parece uma unidade flash USB normal, mas na realidade é muito mais do que isso. Dentro do dispositivo há um slot MicroSD e um processador para fazer o dispositivo realizar sua magia. Essencialmente, esta magia é que o dispositivo não só pode executar scripts no sistema conectado, mas também tem a capacidade de mascarar como algo diferente de uma unidade flash, neste caso, um dispositivo de interface humana (HID), como um teclado. O valor deste último ponto não deve ser subestimado porque muitos sistemas podem ser configurados para bloquear dispositivos USB. Eles não estão configurados para bloquear hardware HID porque isso significaria que coisas como teclados podem não funcionar.

Sugestões de livros: