Entendendo a autenticação na plataforma Microsoft

Vimos nas postagens anteriores os diferentes mecanismos através dos quais podemos obter credenciais, bem como como podemos ataca-los, vamos olhar alguns mecanismos de autenticação. Vamos nos concentrar nos mecanismos da plataforma Microsoft: SAM, NTLM, LM e Kerberos.

Security Account Manager (SAM)

Dentro do sistema operacional Windows, tem um banco de dados que armazena as entidades de segurança (contas ou qualquer entidade que pode ser autenticada). No mundo Microsoft, esses princípios podem ser armazenados localmente em um banco de dados conhecido como Security Account Manager (SAM). Credenciais, senhas e outras informações de conta são armazenadas neste banco de dados em um formato hash. Quando o sistema está em execução, o Windows mantém um bloqueio de arquivo no SAM para impedir que ele seja acessado por outros aplicativos ou processos. O sistema só desativará o acesso exclusivo ao SAM quando desligado ou quando o sistema tiver uma tela azul da morte.

A fim de melhorar a segurança, a Microsoft adicionou alguns recursos projetados para preservar a integridade das informações armazenadas no banco de dados. Por exemplo, um recurso conhecido como SYSKEY foi adicionado a partir do Windows NT 4.0 para melhorar a segurança existente do SAM. SYSKEY não é nada mais do que um nome de fantasia para um utilitário que é usado para criptografar parcialmente o SAM e proteger as informações armazenadas dentro dele. Por padrão, esse recurso é habilitado em todos os sistemas posterior ao NT

4.0. Embora possa ser desativado, é altamente recomendável que você não o faça. Com o SYSKEY no lugar, as credenciais são seguras contra muitos ataques off-line.

Como as senhas são armazenadas dentro do SAM

No Windows XP e plataformas mais recentes, as senhas são armazenadas em um formato hash usando os mecanismos de hash LM / NTLM. Os hashes são armazenados em *c:\windows\system32\config\SAM*.

Uma conta no SAM tem esta aparência:
*Link:1010:**624AAC413795CDC14E835F1CD90F4C76:6F585FF8FF6280B59CCE252FDB500EB8:::***

A parte em negrito antes dos dois-pontos é o hash LM e a parte em negrito após representa o hash NTLM – ambas para uma senha de uma conta de usuário padrão. Os crackers de senhas como Ophcrack e L0phtCrack tentam decifrar esses hashes, assim como aplicativos como pwdump.

As versões do Windows após o XP não armazenam o hash LM por padrão. Eles armazenam um valor em branco ou um valor fictício que não tem correlação direta com a senha real de qualquer usuário, portanto, extrair esse valor e usar um ataque de força bruta para decifrá-lo é inútil. Esse valor fictício também é usado quando a senha excede 14 caracteres, que é maior do que o mecanismo hash LM pode suportar.

No Windows, como em outros sistemas, o hash de senha pode ser reforçado usando salt. Esta técnica é projetada para adicionar uma camada adicional de aleatoriedade a um hash durante o processo de geração. Com o sal adicionado a um hash offline e pré-computado, os ataques se tornam muito mais difíceis de executar com sucesso.

Autenticação NTLM

NT LAN Manager (NTLM) é um protocolo exclusivo (proprietário) para produtos Microsoft. NTLM versões 1 e 2 ainda são muito utilizados em ambientes e aplicações onde outros protocolos como Kerberos não estão disponíveis, mas a Microsoft recomenda que seja evitado ou eliminado.

NTLM vem em duas versões: NTLMv1 e NTLMv2. NTLMv1 tem sido usado por muitos anos e ainda tem algum suporte em produtos mais recentes, mas tem sido amplamente substituído em aplicações e ambientes com pelo menos NTLMv2 se não outros mecanismos. NTLMv2 é uma versão melhorada do protocolo NTLM. Possui melhor segurança do que a versão 1, mas ainda é visto como relativamente inseguro e como tal deve ser evitado também. Existe outro mecanismo em camadas em cima do NTLM conhecido como Security Support Provider (SSP). Este protocolo é combinado com NTLM para fornecer uma camada adicional de proteção em cima do processo de autenticação existente.

Em geral, o processo de autenticação com o protocolo NTLM usa as seguintes etapas:

1. O cliente insere seu nome de usuário e senha no prompt de login.
2. O Windows executa a senha através de um algoritmo hash para gerar um hash para a senha específica.
3. O cliente transmite o nome de usuário e hash para um controlador de domínio.
4. O controlador de domínio gera uma cadeia de caracteres aleatórios de 16 bytes conhecida como um nonce e transmite-lo novamente para o cliente.
5. O cliente criptografa o nonce com o hash da senha de usuário e envia-lo novamente para o controlador de domínio.
6. O controlador de domínio recupera o hash de seu SAM e usa-lo para criptografar o nonce enviou para o cliente.

Neste ponto, se os hashes coincidirem, o pedido de login será aceito. Se não, o pedido é negado.

Sugestões de livros:

Kerberos

Na plataforma Microsoft, a versão 5 do protocolo de autenticação Kerberos está em uso desde o Windows 2000. O protocolo oferece uma estrutura de autenticação robusta através do uso de mecanismos criptográficos fortes, como criptografia de chave simétrica. Ele fornece autenticação mútua de cliente e servidor.

O protocolo Kerberos utiliza os seguintes grupos de componentes:

- Centro de distribuição de chaves (Key distribution center – KDC)
- Servidor de autenticação (Authentication server – AS)
- Servidor de admissão de tíquetes (Ticket-granting server – TGS)

O processo de utilização do Kerberos funciona da seguinte forma:

1. Você deseja acessar outro sistema, como um servidor ou cliente. Como o Kerberos está em uso neste ambiente, um ticket é necessário.
2. Para obter esse ticket, primeiro você é autenticado no AS, que cria uma chave de sessão com base em sua senha juntamente com um valor que representa o serviço ao qual deseja se conectar. Esta solicitação serve como seu ticket de concessão de bilhete (TGT).

3. Seu TGT é apresentado a um TGS, que gera um ticket que lhe permite acessar o serviço.
4. Com base na situação, o serviço aceita ou rejeita o bilhete. Nesse caso, suponha que você está autorizado e tem acesso.

O TGT é válido apenas por um período finito antes de ser regenerado. Isso atua como uma salvaguarda contra ela sendo comprometida.

Quebrando a senha do Kerberos

Neste passo a passo abaixo, vamos dar uma olhada em como quebrar uma senha capturada do Kerberos. Para executar este exercício, você deve baixar o utilitário Cain de oxid.it:

1. No software Cain, inicie o sniffer clicando no ícone sniffer na barra de ferramentas.
2. Quando solicitado, escolha a interface para usar no sniffer.
3. Selecione a guia Sniffer.
4. Clique no sinal azul +.
5. Quando apresentado com a caixa de diálogo, clique em OK.
6. Na caixa de diálogo que aparece, digite os endereços de dois hosts a terem ARP envenenados, o que significa que você está colocando informações nas tabelas ARP dos sistemas alvos. Escolha dois hosts diferentes daquele em que você está executando o ataque.
7. Clique em OK.
8. Na barra de ferramentas, selecione o ícone de envenenamento ARP e observe que o status mudará para o estado de “poisoning”.
9. Após um ou dois minutos, clique na guia Sniffer.
10. Clique na aba Password.
11. Selecione MSKerb5-PreAuth Hashes.
12. Clique com o botão direito do mouse e selecione Send To Cracker.

13. Clique na aba Cracker.
14. Selecione Kerb5 PreAuth Hashes.
15. Clique com o botão direito do mouse em uma senha e selecione um crack.

Neste ponto, se tudo correu bem você deve ser capaz de quebrar uma senha Kerberos. É importante notar que você pode ter que esperar um pouco em redes que não são ativas.

Sugestões de livros: