Escalando privilégios e executando aplicações em um ataque

Quando você obtém uma senha e obtém acesso a uma conta, ainda há mais trabalho a fazer: escalar os privilégios. A realidade é que a conta que você está comprometendo pode acabar sendo privilegiada e menos defendida. Se este for o caso, você deve executar o escalonamento de privilégios antes de realizar a próxima fase. O objetivo deve ser ganhar um nível onde menos restrições existem na conta e você tem maior acesso ao sistema.

Cada sistema operacional vem com um número de contas de usuário e grupos já presentes. No Windows, os usuários pré-configurados incluem as contas de administrador e de convidado. Como é fácil para um invasor encontrar informações sobre as contas incluídas em um sistema operacional, você deve ter o cuidado de garantir que essas contas sejam protegidas adequadamente, mesmo que nunca sejam usadas. Um invasor que sabe que essas contas existem em um sistema é mais do que provável para tentar obter suas senhas.

Existem dois tipos definidos de escalonamento de privilégios. Cada um se aproxima do problema de obter maiores privilégios a partir de um ângulo diferente:

- **Escalação de Privilégio Horizontal** – Um invasor tenta assumir os direitos e privilégios de outro usuário que tem os mesmos privilégios que a conta atual;
- **Escalação de Privilégio Vertical** – O atacante ganha acesso a uma conta e tenta elevar os privilégios da conta. Também é possível realizar uma escalação vertical comprometendo uma conta e, em seguida, tentando obter acesso a uma conta de privilégios mais elevados.

Uma maneira de aumentar os privilégios é identificar uma conta que tenha o acesso desejado e, em seguida, alterar a senha. Várias ferramentas que oferecem esta capacidade, incluindo:

- Active@ Password Changer
- Trinity Rescue Kit
- ERD Commander
- Windows Recovery Environment (WinRE)
- Password Resetter

Vejamos um destes aplicativos um pouco mais perto: Trinity Rescue Kit (TRK). De acordo com os desenvolvedores da TRK:

> *Trinity Rescue Kit (TRK) é uma distribuição Linux especificamente projetada para ser executada a partir de um CD ou unidade flash. TRK foi projetado para recuperar e reparar sistemas Windows e Linux que eram de outra forma não inicializáveis ou irrecuperáveis. Embora o TRK tenha sido projetado para propósitos benevolentes, ele pode ser facilmente usado para aumentar os privilégios ao redefinir senhas de contas às quais você não teria acesso. TRK pode ser usado para alterar uma senha, inicializando o sistema de destino através de um CD ou flash drive e entrar no ambiente TRK. Uma vez no ambiente, uma sequência simples de comandos pode ser executada para redefinir a senha de uma conta.*

Os seguintes passos devem ser executados no Windows usando o TRK para mudar a senha do administrador:

1. Na linha de comando, use o seguinte: winpass -u Administrator
2. O comando winpass mostra uma mensagem similar ao seguinte:
   Searching and mounting all file system on local machine
   Windows NT/2K/XP installation(s) found in:
   1: /hda1/Windows
   Make your choice or “q” to quit [1]:
3. Pressione 1 ou o número do local onde o Windows está

instalado, caso tenha mais de uma instalação.
4. Pressione Enter;
5. Digite a nova senha ou aceite a sugestão do TRK para setar a nova senha.
6. Você verá a mensagem: “Do you really wish to change it?” Aperte Y e Enter.
7. Digite **init 0** para desligar o sistema TRK Linux
8. Reinicie.

Executando aplicações

Depois de ter acesso a um sistema e obter privilégios suficientes, é hora de comprometer o sistema e realizar o ataque. Quais aplicativos serão executados neste momento é uma decisão do invasor, mas podem ser aplicativos personalizados ou comerciais.

Em alguns casos, uma vez que um atacante obteve acesso a um sistema e está executando aplicativos nele, dizem que o sistema está *owned.*

Um invasor executa diferentes aplicativos em um sistema com objetivos específicos em mente:

- Backdoors – Aplicações deste tipo são projetadas para comprometer o sistema de tal forma que permita o acesso posterior. Um atacante pode usar essas portas para atacar o sistema. Backdoors podem vir na forma de rootkits, trojans e semelhantes. Eles podem até incluir software na forma de Trojans de acesso remoto (RATs).
- Crackers – Qualquer software que se encaixa nesta categoria é caracterizado pela capacidade de quebrar um código ou obter senhas.
- Keyloggers – Keyloggers são dispositivos de hardware ou software usados ??para obter informações inseridos através do teclado.
- Malware – Este é qualquer tipo de software projetado

para capturar informações, alterar ou comprometer o sistema.

Plantando um backdoor

Há muitas maneiras de plantar um backdoor em um sistema, mas vamos olhar para um fornecido através da suíte PsTools. Esta suíte inclui um conjunto misto de utilitários concebidos para facilitar a administração do sistema. Entre essas ferramentas está o PsExec, que é projetado para executar comandos de forma interativa ou não interativa em um sistema remoto. Inicialmente, a ferramenta pode parecer semelhante ao Telnet ou Remote Desktop, mas não requer instalação no sistema local ou remoto para funcionar. Para trabalhar, o PsExec só precisa ser copiado para uma pasta no sistema local e executado com as opções apropriadas.

Vejamos alguns dos comandos que você pode usar com o PsExec:

- O comando a seguir lança um prompt de comando interativo em um sistema chamado *zelda:psexec \\zelda cmd*
- Este comando executa ipconfig no sistema remoto com a opção /all e exibe a saída resultante localmente: *psexec \\zelda ipconfig /all*
- Este comando copia o programa rootkit.exe para o sistema remoto e executa-o interativamente: *psexec \\zelda -c rootkit.exe*
- Este comando copia o programa rootkit.exe para o sistema remoto e executa-o de forma interativa usando a conta de administrador no sistema remoto: *psexec \\zelda -u administrator -c rootkit.exe*

Como esses comandos ilustram, é possível para um invasor executar um aplicativo em um sistema remoto com bastante facilidade. O próximo passo é para o atacante decidir o que fazer ou o que executar no sistema remoto. Algumas das opções comuns são trojans, rootkits e backdoors.

Outros utilitários que podem ser úteis para se conectar a um sistema remotamente são os seguintes:

- **PDQ Deploy** – Este utilitário foi projetado para auxiliar na implantação de software em um único sistema ou em vários sistemas em uma rede. O utilitário foi projetado para integrar com o Active Directory (AD), bem como outros pacotes de software.
- **RemoteExec** – Este utilitário foi projetado para funcionar como o PsExec, mas também facilita a reinicialização, reinicialização e manipulação de pastas no sistema.
- **DameWare** – Este é um conjunto de utilitários usados ??para administrar e controlar remotamente um sistema. Bem como os outros utilitários nesta lista, ele está prontamente disponível e pode não ser detectado por antivírus. DameWare também tem a vantagem de trabalhar em plataformas como Windows, OS X e **Linux.**
- **Netcat** – Este utilitário é uma aplicação simples e eficaz que pode ser usada abrir backdoors em um sistema quando plantado eficazmente em um sistema.

Sugestões de livros: