Cobrindo seus rastros em um pentest

Depois de ter invadido um sistema e ter um software instalado ou executado alguns scripts, o próximo passo é a limpeza de seus rastros ou esconde-los. O objetivo desta fase é evitar que seu ataque seja facilmente descoberto usando várias técnicas para esconder os sinais. Durante esta fase, você procura eliminar mensagens de erro, arquivos de log e outros itens que podem ter sido alterados durante o processo de ataque.

Desabilitando a auditoria

Uma das melhores maneiras de evitar ser descoberto é não deixar trilhas em tudo. E uma das melhores maneiras de fazer isso é evitar que qualquer trilha seja criada ou, pelo menos, minimizar a quantidade de provas. Quando você está tentando não deixar trilhas, um bom ponto de partida é alterando a forma como os eventos são registrados no sistema alvo.

Desativar a auditoria em um sistema evita que certos eventos apareçam e, portanto, retarda a detecção. Lembre-se que a auditoria é projetada para permitir a detecção e rastreamento de eventos selecionados em um sistema. Uma vez que a auditoria é desativada, você efetivamente privou o defensor de uma grande fonte de informações e forçou-os a procurar outros métodos de detecção.

No ambiente Windows, você pode desabilitar a auditoria com o comando *auditpol*. Usando a técnica de sessão NULL durante suas atividades de enumeração, você pode se conectar a um sistema remotamente e executar o comando da seguinte maneira:

auditpol \\<endereço IP do destino> /clear

Você também pode executar o que equivale à remoção cirúrgica

de entradas no Log de Segurança do Windows, usando ferramentas como as seguintes:

- Dump Event Log
- ELSave
- WinZapper
- CCleaner
- Wipe
- MRU-Blaster
- Tracks Eraser Pro
- Clear My History

Esconder dados

Existem outras maneiras de ocultar evidências de um ataque, incluindo ocultar os arquivos colocados no sistema, como arquivos EXE, scripts e outros dados. Sistemas operacionais como o Windows fornecem muitos métodos que você pode usar para ocultar arquivos, incluindo atributos de arquivo e fluxos de dados alternativos.

Os atributos de arquivo são uma característica dos sistemas operacionais que permite que os arquivos sejam marcados como tendo certas propriedades, como marcar para somente leitura e oculto. Os arquivos podem ser sinalizados como ocultos, o que é uma forma conveniente de ocultar dados e impedir a detecção através de meios simples, como listagens de diretório ou navegação no Windows Explorer. Ocultar arquivos desta forma não fornece proteção completa, pois, técnicas mais avançadas podem descobrir arquivos escondidos desta forma.

Fluxos de dados alternativos

Um método muito eficaz de ocultar dados em um sistema Windows também é um dos menos conhecidos: Fluxos de dados alternativos (Alternate Data Stream – ADS). Este recurso é parte do NTFS desde a década de 1990, mas desde a sua introdução tem

recebido pouco reconhecimento; Isso faz com que seja útil para um atacante experiente e perigoso para um defensor que sabe pouco sobre isso.

Originalmente, esse recurso foi projetado para garantir a interoperabilidade com o sistema de arquivos hierárquicos do Macintosh (HFS), mas desde então tem sido usado para outros fins. O ADS fornece a habilidade de fork ou de esconder dados do arquivo dentro dos arquivos existentes sem alterar a aparência ou o comportamento de um arquivo de qualquer maneira. Na verdade, quando você usa ADS, você pode ocultar um arquivo de todas as técnicas de detecção tradicionais, assim como *dir* e Windows Explorer.

Na prática, o uso de ADS é uma grande questão de segurança porque é quase um mecanismo perfeito para ocultar dados. Uma vez que um pedaço de dados é incorporado e oculto usando ADS, ele pode ficar em espera até que o atacante decide executá-lo mais tarde.

O processo de criação de um ADS é simples, como exemplo vamos esconder um arquivo chamado triforce em um arquivo chamado smoke.doc:

Type triforce.exe> ??smoke.doc:triforce.exe

Executando este comando, ocultaremos o arquivo triforce.exe atrás do arquivo smoke.doc. Neste ponto, o arquivo é transmitido. O próximo passo é excluir o arquivo original que você acabou de ocultar, triforce.exe.

Como um invasor, recuperar o arquivo é tão simples quanto:

start smoke.doc:triforce.exe

Este comando tem o efeito de abrir o arquivo oculto e executá-lo.

Como um defensor, isso soa como uma má notícia, porque os arquivos escondidos desta forma são impossíveis de detectar

usando a maioria dos meios. Mas usando alguns métodos avançados, eles podem ser detectados. Ferramentas que você pode usar para fazer isso incluem o seguinte:

- SFind – Uma ferramenta forense para encontrar arquivos streamed;
- LNS – Usado para encontrar arquivos ADS;
- Tripwire – Usado para detectar mudanças nos arquivos; Por natureza pode detectar ADS;

OBS.: ADS está disponível somente em volumes NTFS, não importa a versão do NTFS. Este recurso não funciona em outros sistemas de arquivos.

Sugestões de livros: