Enumeração Linux e Unix

Os sistemas linux e unix são similares ao Windows e podem ser enumerados. A diferença é nas ferramentas e na abordagem. Veremos como usar estas ferramentas e obter algumas informações ao explorar estes sistemas.

É importante lembrar que os comandos são case-sensitive, ou seja, deve-se prestar atenção aos comandos.

finger

O comando finger foi feito para retornar informações sobre um usuário em um sistema. Quando executado, ele retorna informações sobre o usuário como o diretório home, hora do login, tempo ocioso, localização do escritório e a última vez que eles recebem ou leram e-mail.

O comando do finger é semelhante a esta estrutura:

finger <switches> usuário

Os switches que podem ser usados são:

- -b remove a exibição do diretório home e o shell do usuário;
- -f remove a exibição do cabeçalho;
- -w remove o nome completo da exibição;
- -l retorna a lista de usuários;

rpcinfo

Este comando enumera informações expostas sobre o protocolo Remote Procedure Call (RPC).

O comando é semelhante a esta estrutura:

rpcinfo <switches> hostname

Os switches que podem ser usados são:

- -m exibe a lista de estatísticas do RPC de um host;
- -s exibe a lista de aplicações RPC registradas de um host;

showmount

Este comando lista e identifica diretórios compartilhados presente em um sistema. showmount exibe a lista de todos os clientes que tem um sistema de arquivos montados remotamente.

O comando é semelhante a esta estrutura:

/usr/share/showmount [- ade] [hostname]

Os switches que podem ser usados são:

- -a imprime todas as montagens remotas;
- -d lista os diretórios que foram montadas remotamente pelos clientes;
- -e imprime a lista de sistemas de arquivos compartilhados;

enum4linux

Uma ferramenta que faz este tipo de enumeração é o enum4linux, o qual permite extrair informações do Windows ou Samba. Mas o que é o Samba?

De acordo com o site samba.org, o software é descrito como:

> *…software that can be run on a platform other than Microsoft Windows, for example,*
> *UNIX, Linux, IBM System 390, OpenVMS, and other operating systems. Samba uses*
> *the TCP/IP protocol that is installed on the host server. When correctly configured, it*

allows that host to interact with a Microsoft Windows client or server as if it is a
Windows file and print server.

Enum4linux permite a extração de informações onde o Samba está sendo usado. Informações que podem ser retornadas incluem as seguintes:

- Informações de grupos de membros;
- Informações compartilhadas;
- Membros do grupo de trabalho ou domínio;
- Identificação do SO;
- Obter a política de senha;

Sugestões de livros: