Artigo – Utilizando Script NMAP para identificar hosts com a falha MS17-010

Procedimento homologado nos seguintes sistemas:

Debian 8.5
Linux Mint 18.2

Nota: Para execução desse script deve ser usada a versão 7.40 e LUA 5.3, pois há problemas com versões anteriores, caso a versão presente no sistema atenda os requisitos, desconsiderar a nota. Caso necessite a instalação da versão 7.40 muito provavelmente não terá êxito tentando instalar utilizando o comando "apt-get install nmap", pois dependendo das distros não trará a versão 7.40, caso esse impasse aconteça devemos instalar o mesmo compilando o pacote.

Caso já possua o NMAP presente em seu sistema verifique sua verão com o comando abaixo:

nmap --version

Instalar as ferramentas necessárias para compilação:

apt-get install build-essential

Baixando e instalando o NMAP versão 7.40

wget https://nmap.org/dist/nmap-7.40.tgz

tar -xvzf nmap-7.40.tgz

cd nmap-7.40

./configure

make

make install

Script:

https://github.com/cldrn/nmap-nse-scripts/blob/master/scripts/smb-vuln-ms17-010.nse

Salve o conteúdo do script em um arquivo chamado: smb-vuln-ms17-010.nse.

Ex:

vim smb-vuln-ms17-010.nse

Nota: O caminho completo do script deve ser passado durante a execução, como por exemplo: nmap -p445 --script /home/usuario/smb-vuln-ms17-010 192.168.16.0/24. Caso esteja executando o NMAP no mesmo diretório a qual o script esteja presente, não haverá problemas. Se preferir copie o mesmo para o diretório padrão que contem todos os scripts do NMAP "/usr/share/nmap/scripts".

nmap -p445 --script smb-vuln-ms17-010 192.168.16.0/24

Nota: Após execução do mesmo você terá uma saída semelhante ao exemplo abaixo, a qual devemos nos atentar a linha "State", pois a mesma informa o status sobre a vulnerabilidade. Caso não retorne o exemplo abaixo e sim a informação que a porta 445 está sendo filtrada tente desabilitar o Firewall do Windows SOMENTE DURANTE O ESCANEAMENTO, logo após o diagnostico o mesmo deve ser habilitado novamente.

Abaixo segue um exemplo de uma máquina vulnerável rodando o Windows 7 Professional SP1:

```
Starting Nmap 7.40 ( https://nmap.org ) at 2017-05-15 18:45 BRT
Nmap scan report for 192.168.16.6
Host is up (0.00041s latency).
PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|       servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://blogs.technet.microsoft.com/.../customer.../
|       https://technet.microsoft.com/.../security/ms17-010.aspx
|_ https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
```

Artigo por Lucas Cavalcanti
https://www.linkedin.com/in/lucas-cavalcanti-8a8347120/?trk=nav_responsive_tab_profile