<**Hacking**

**ético**

# 

[**Objetivo 2**](#_qh2lm4w331k0)

[Host Discovery: para descubrir todas las máquinas de la red. 2](#_lmr1h790pguk)

[Escaneo básico de todos los puertos: en el target solo se especifican las tres máquinas del laboratorio. 2](#_3yvqb1bmt62w)

[Generar un informe en formato pdf/html de las máquinas. 3](#_mbtdqbll04si)

[Realizar un escaneo a las dos máquinas, añadir credenciales para ambas máquinas, y generar un informe en formato html del resultado de los dos equipos. 3](#_knu8ybqa0e1o)

[Con credenciales: 3](#_hx6nfeu2c7ko)

[Sin credenciales: 4](#_tw8x62wcltjg)

[Añadir todos los plugins para sistemas Windows 7 (Windows : Microsoft Bulletin) y todos los que consideres adecuados. 5](#_yv06rk7ku6q7)

[Anexar al documento anterior una valoración de alguna vulnerabilidad crítica encontrada y el riesgo que suponen, comentarlas y para ello apoyarse en las páginas vistas en la teoría de CVEs. 5](#_74hr85ss0w56)

[**Bibliografía 7**](#_9yf7b482w37a)

| Objetivo |
| --- |
| Practicar tareas relacionadas con la intrusión a una máquina Windows 7, para ello haré haré uso de una máquina Kali Linux y principalmente las herramientas **nmap y Metasploit.** |
| Host Discovery: para descubrir todas las máquinas de la red. |
| 1. Arp -a ( si estas en el servidor) 2. Nmap -sn <nombre red local ej:192.168.44.0> 3. Herramientas con interfaz gráfica    1. Advanced IP Scanner (windows)    2. Angry Ip scanner (linux) |
| Escaneo básico de todos los puertos: en el target solo se especifican las tres máquinas del laboratorio. |
| Ejemplo desde nmap: |
| nmap -p- 192.168.69.ip1,ip2,ip3 -n |
| Generar un informe en formato pdf/html de las máquinas. |
| nmap -p- 192.168.69.ip1,ip2,ip3 -n -oX informe.xml  xsltproc informe.xml -o informe.html |
| Realizar un escaneo a las dos máquinas, añadir credenciales para ambas máquinas, y generar un informe en formato html del resultado de los dos equipos. |
| Nmap -p- -sV <ej:192.168.172.ip1,ip2> -n  Asumo un acceso por ssh. Con credenciales: nmap -p 22 --script ssh-auth-methods --script-args="ssh.user=<username>" <target1, target2> -oX <nombreXML>  xsltproc <nombreXML> -o <nombreHTML>  Descripción del script→   Sin credenciales: nmap -p 22 --script ssh-brute --script-args userdb=users.lst,passdb=pass.lst \  -- --script-args ssh-brute.timeout=4s <target1, target2> -oX <nombreXML>  xsltproc <nombreXML> -o <nombreHTML>  Descripción del script→ <https://nmap.org/nsedoc/scripts/ssh-brute.html> |
| Añadir todos los plugins para sistemas Windows 7 (Windows : Microsoft Bulletin) y todos los que consideres adecuados. |
| Msfconsole  search OS:Windows 7 |
| Anexar al documento anterior una valoración de alguna vulnerabilidad crítica encontrada y el riesgo que suponen, comentarlas y para ello apoyarse en las páginas vistas en la teoría de CVEs. |
| [Nombre del parche: MS17-010](https://learn.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010)  Descripción:  “La más grave de las vulnerabilidades podría permitir la ejecución remota de código si un atacante envía mensajes especialmente diseñados a un servidor de Bloque de mensajes de Microsoft Server 1.0 (SMBv1).”  [learn.microsoft](https://learn.microsoft.com/es-es/security-updates/securitybulletins/2017/ms17-010)  Gravedad: Crítica.  SO: <Windows 10 v1607,, <Windows Server 2016 x64  Exploits: ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE y ETERNALSYNERGY  Malware: Trickbot, WannaCry, CoinMinner, WannaMine.  [Códigos CVE](https://www.cvedetails.com/google-search-results.php?q=MS17-010#gsc.tab=0&gsc.q=MS17-010&gsc.page=1): |
| Puertos: |
| [TCP port 445](https://www.tenable.com/plugins/nessus/97833)  SMB sobreNetBIOS API,   * TCP 137 / 139 and UDP ports 137 / 138 |
|  |
| Bibliografía  * <https://www.ionos.es/digitalguide/servidores/know-how/arp-resolucion-de-direcciones-en-la-red/> * <https://academy.hackthebox.com/module/39/section/381> * <https://learn.microsoft.com/es-es/security-updates/securitybulletins/2017/ms17-010> * <https://www.cvedetails.com/google-search-results.php?q=MS17-010#gsc.tab=0&gsc.q=MS17-010&gsc.page=1> * <https://learn.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010> * <https://www.tenable.com/plugins/nessus/97833> |