Exercici 1.- Escaneig de ports. (0.5p)

a) > nmap ip

També serveix > nmap --open ip o > nmap -sS ip.

b1) Basicament envia cert paquets i evalua la resposta d'aquest.

b2) La máquina ha trobat 7 ports oberts.

PORT STATE SERVICE

135/tcp open msrpc

139/tcp open netbios-ssn

445/tcp open microsoft-ds

903/tcp open iss-console-mgr

1042/tcp open afrog

1043/tcp open boinc

3306/tcp open mysql

Exercici 2.- Detecció del sistema operatiu (0.5p)

a) > nmap -O -v ip

b1) No ha tingut exit, segurament hi ha algun problema amb la maquina virtual.

Resultats: Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

b2) Fa diferents proves per verificar quin SO executem, com: medició de temps d'activitat, la dificultat de fer una conexió TCP falsa…

Exercici 3.- Opcions de l'escàner de ports. (0.5p)

a) > nmap -sT ip

> nmap -sS ip

> nmap -sN ip

b1)

Escaner -sT Aquest si que fa una connexio TCP, pot comportar sospites en una red.

Escaner -sS No arriba a obrir una conexio TCP completa, envia un SYN, rep SYN/ACK port obert ,un RST no hi ha ningú escoltant al port o no rep res.

Escaner -sN Aquest es basa en verificar sistemes que compleixen amb el RFC, si un packet no conte SYN, ACK o RST resultara en l'enviament de RST per lo tant esta tancat.

b2)

Amb -sT i -sS mateixos resultats, latencia diferent.

Amb -sN resultat diferent, no es mostra ningún port.

Exercici 4.- Detecció de la versió dels serveis. (0.5p)

a) > nmap -sV ip

b)

PORT STATE SERVICE VERSION

135/tcp open msrpc Microsoft Windows RPC

139/tcp open netbios-ssn Microsoft Windows netbios-ssn

445/tcp open microsoft-ds?

903/tcp open ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)

1042/tcp open afrog?

1043/tcp open ssl/boinc?

3306/tcp open mysql MySQL 8.0.27

Exercici 5.- Escaneig de port (0.5p)

a)

Per detectar i llistar els ports oberts des de la nostra màquina o per detectar els serveis associats amb aquests ports, nessus utilitza el programa netstat que ens pot proporcionar per exemple informació detallada d'activitats a la xarxa o, com en aquest cas, informació sobre els ports i direccions a tracés dels qual s'executen connexions TCP/UDP

b)

S'han trobat 25 ports oberts a la màquina metasploitable. Els 10 primers ports trobats (tots protocol TCP) juntament amb el servei que tenen associat cadascun d'ells són: 21 ftp ,22 ssh, 23 telnet , 25 smtp, 53 domain, 80 http, 111 rpcbind, 139 netbios-ssn, 445 microsoft-ds.

c)

Els passos que hem seguit per crear la Policy són els següents:

1-A la barra de navegació de l'esquerra, fem clic a Policies

2-A la cantonada superior dreta, fem clic a New Policy

3-Fem clic a la política Advanced Scan.

4-Li afegim un nom a la nostra política.

5-A les pestanyes superior, fem clic a Plugins.

6-Ens trobarem que tots els Plugins estan habilitats incialment. Els deshabilitem tots fent clic a la cantonada superior dreta, a la pestanya Disable All.

7-En el nostre cas, els plugins que hem utilitzat són tots els de la família Port scanners (que no cal activar manualment degut a que ja ho fa el Advanced Scan de forma automàtica) i tots els de la família Service detection. Per afegir tots els plugins de la família Service detection, busquem aquesta família la llista Plugin Family i fem clic a la pestanya que es trobarà de color gris que posa DISABLED per habilitar aquests plugins. Quan fem clic, aquesta pestanya pasarà a ser de color verd i posarà ENABLED.

8- Finalment, baixem fins a baix de tots de la pàgina i fem clic a Save per guarda la nostra Policy

Exercici 6.- Escaneig de vulnerabilitats (0.5p)

a)

El resultat d'aquests escaneig es molt més extens i ens proporciona molta més informació que amb la Policy del exercici anterior.

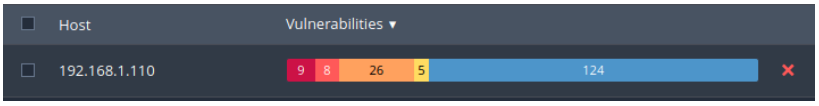
Ens mostra moltes més vulnerabilitats, fent un total de 63 vulnerabilitats quan amb la Policy del exercici anterior només ens mostrava 22 i molts més VPR Top Threats (10 en aquest cas, 2 en el exercici anterior), però realment, la diferencia més remarcable es que apareix una nova secció denominada "Remediations", és a dir, que ens realitza un escaneig de remediació. Aquesta nou escaneig consisteix en que ens dona remeis per resoldre problemes, és a dir, per resoldre algunes vulnerabilitats trobades, informació que no ens donava l'anterior escaneig utilitzant la Policy del exercici anterior.

Aquesta informació extra es aportada degut a que a que algunes de les vulnerabilitats es poden solucionar. En el escaneig anterior, al ser menys extens i trobar moltes menys vulnerabilitats, ninguna d'aquestes vulnerabilitats tenia solució i per tant no ens apareix cap informació sobre remeis per resoldre vulnerabilitats (escaneig de remediació), en canvi, en aquests nou escaneig, al trobar moltes més vulnerabilitats, algunes d'aquestes vulnerabilitats si que tenen solució i per tant el escaneig de remediació ens pot aportar remeis per aquestes. En conclusió,

aquesta informació es aportada degut a que al tenir tots els plugins habilitats el escaneig es molt més extens y detallat.

b)

S'han detectat 9 vulnerabilitats crítiques, 8 de nivell alt i 26 de nivell mig.



Exercici 7.- Analitzant una vulnerabilitat (1p)

a)

Description
The version of the Samba server installed on the remote host is affected by multiple heap overflow vulnerabilities, which can be exploited remotely to execute code with the privileges of the Samba daemon.

La versió del servidor Samba instal·lada al host remot es veu afectada per múltiples vulnerabilitats de desbordament de pila que es poden explotar de forma remota per executar codi amb els privilegis del Samba daemon.

b)

Es va descobrir el 14 de maig del 2007 i va ser informada per el investigador i reporter Brian Schafer als desenvolupadors de Samba. Va ser detectada utilitzant un plugin de la familia Misc amb ID 25216. Es tracta de diversos errors a la separació de l'NDR de Samba. La solució que ens proposa Nessus es que ens descarreguem la versió de Samba 3.0.25 o una posterior.

c)

Aquesta vulnerabilitat té el CVE -2007-2446 i afecta a les versions de Samba 3.0.0 fins a la versió 3.0.25rc3 (aquesta inclosa).

Exercici 8.- Puntuació d'una vulnerabilitat (1p)

a)

CVSS v2.0 Base Score: 10.0

CVSS v2.0 Vector Score: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

El vector de puntuacions, en primer lloc, ens indica las mètriques, és a dir, les condicions per explotar la màquina. Aquestes mètriques tractaran de, quin tipus d'accés es necessari per atacar la màquina que s'especificarà en el camp AV i pot ser del tipus L (accés local), A (accés des a una xarxa adjacent) o N (accés a la seva xarxa), de quin nivell de complexitat té atacar la màquina que s'especificarà al camp AC i pot ser del tipus H (complexitat alta), M (complexitat

mitjana) o L (complexitat baixa) i de quin tipus d'autenticació es requerida que s'especificarà al camp Au i pot ser del tipus M (múltiple), S (només una) o None (no es requereix l'autenticació).

En segon lloc, ens indica l'impacta que té en la màquina y tractarà de quin impacte de confidencialitat (camp C), integritat (camp I) i disponibilitat (camp A) té, i aquestes tres impacte poden ser del tipus del tipus N (No té impacte d'aquest tipus), P (Parcial) o C (complet).

En aquest cas com podem veure, es necessari tenir accés a la seva xarxa (AV:N), el nivell de complexitat que té accedir es baix (AC:L), no requereix autenticació (Au:N) i els impactes de confidencialitat, integritat i disponibilitat són complets (C:C/I:C/A:C).

b)

CVSS v2.0 Temporal Score: 7.8

CVSS v2.0 Temporal Vector: CVSS2#E:POC/RL:OF/RC:C

El vector temporal ens indica, al llarg del temps, el nivell d'explotació que s'especificarà en el camp E i pot ser del tipus ND (no definit), U (no existeix ningun codi per l'explotació), POC (explotació mitjançant un codi), F (existeix una explotació funcional) i H (nivell d'explotació alt), el nivell de remediació,és a dir, la facilitat per a buscar remeis per la vulnerabilitat que s'especificarà en el camp RL i pot ser del tipus ND (no definit), OF (correcció oficial), TF (arregla temporal), W (solució alternativa) i U (solució no disponible) i el nivell de detecció (informe de confiança) davant la vulnerabilitat que s'especificarà en el camp RC i pot ser del tipus ND (no definit), UC (sense confirmar), UR (sense corroborar) i C (confirmada).

En aquest cas com podem veure, la explotació al llarg del temps haurà de ser mitjançant un codi (E:POC), que els remeis es podrà utilitzar correccions oficials per la vulnerabilitat (RL:OF) i que la vulnerabilitat serà reconeguda per el proveïdor(RC:C)

c)

Si fos necessari l'accés local a la màquina per explotar-la el Base Score seria: AV:L/AC:L/Au:N/C:C/I:C/A:C.

Si la complexitat d'accés fos alta i no baixa el Base Score seria: AV:N/AC:H/Au:N/C:C/I:C/A:C.

De l'impacte de la complexitat de l'atac els impactes de confidencialitat, integritat i disponibilitat són complets (C:C/I:C/A:C).

Del nivell d'accés requerit ens diu que no és necessari tenir accés (Au:N).