Su infraestructura puede estar comprometida…

Guía de Estudio - (HSCP)
Hardened Systems Certified Professional
Laboratorio 4

Integrantes

ANDRES FELIPE RAMIREZ MACKENZIE
KEINER ZUÑIGA ROMERO

Remote Desktop

Hardened Systems
Colombia, Sur América
Tel: 318 706 88 67
Email: training@hardenedsystems.co
Web: www.hardenedsystems.co

Laboratorio 4 – RDP (remote desktop protocol)

Los laboratorios son procesos guiados en un 90%, algunos pasos tendrás que desarrollarlos por ti mismo utilizando algo de intuición y sagacidad. En azul encontraras rutas, y en verde encontraras

comandos específicos. Si tienes dudas no dudes en consultar con tu profesor, él te guiará hasta donde esté permitido en cada ejercicio.

Este laboratorio pertenece a la categoría **HACKING-TIME**, se realizan en parejas compitiendo uno contra otro para demostrar quien tiene de momento mejores capacidades para desenvolverse en el mundo de la seguridad informática. Si resultas ser el vencedor te felicitamos de antemano, sino recuerda, la práctica hace al maestro y seguir entrenando y estudiando te harán cada vez mejor.

OBJETIVOS

a. Habilitar el servicio de escritorio remoto en Windows. RDP.
b. Utilizar el cliente de RDP para ingresar a un equipo.
c. Conocer en qué puerto trabaja RDP.
d. Obtener un archivo en nuestra computadora.
e. Modificar por seguridad el puerto donde normalmente escucha RDP.
f. Identificar en que puerto está trabajando el servicio.
g. Verificar que ventajas tiene este ataque en el caso de ser exitoso y que desventajas.
h. Desarrollar el espíritu del hacker Ético.

PREPARACIÓN

1. Cree un archivo llamado usuarios.txt y guárdelo en una carpeta en la unidad C:/minombre/usuarios.txt. El contenido del archivo deben ser 5 nombres de usuario. Los nombres de usuario pueden ser del tipo, admin, administrador, manuel, estrella, etc. Deben ser textos que la gente común colocaría.
2. Cree un archivo llamado contraseñas.txt y guárdelo en una carpeta en la unidad C:/minombre/contraseñas.txt. El contenido del archivo deben ser 30 contraseñas. Deben ser contraseñas que la gente común colocaría, como rafa3450, pollitosuperestrella.
3. Cree un archivo llamado carta.txt en C:/minombre/carta/carta.txt. y escriba brevemente una carta sobre lo que Ud. piensa de su compañer@, qué sensación le produce y que cosas buenas cree que tiene. NO ENTREGUE ESTE ARCHIVO AL COMPAÑERO.
4. Entregue a su compañero el archivo usuarios.txt y contraseñas.txt.
5. Cree un usuario en Windows eligiendo alguno de los nombres de usuario del archivo usuarios.txt, y eligiendo una contraseña del archivo contraseñas.txt.
6. Ingrese a inicio > imágenes y coloque en esta carpeta 5 fotos descargadas de su Facebook.
7. Apague el Firewall de su sistema operativo. Inicio > Panel de control > Sistema y seguridad > Firewall de Windows > Activar o Desactivar Firewall de Windows. Valide que la opción “Desactivar firewall de Windows” está marcada en ambos escudos rojos.
8. Valide cual es el nombre de su equipo. Inicio > clic derecho en equipo > propiedades. Valide la etiqueta “nombre de equipo”. **R:/ Andres Laptop-k**
9. Modifique el nombre del equipo y coloque en su lugar, su nombre seguido de su apellido. Ej: erikagalindo.
10. Reinicie el equipo.

COMANDOS BASICOS

1. Ingrese a la consola de comandos inicio > cmd.exe
2. Ingrese el comando netstat –a y presione Enter. Ingrese todos los respectivos puertos donde está escuchando el equipo por conexiones. Podrá darse cuenta cuales son ya que el estado de la conexión es LISTENING.

Protocolo	Dirección Local	Dirección Remota	Estado
TCP	0.0.0.0:135	Andres:0	LISTENING
TCP	0.0.0.0:445	Andres:0	LISTENING
TCP	0.0.0.0:125	Andres:0	LISTENING
TCP	0.0.0.0:5040	Andres:0	LISTENING
TCP	0.0.0.0:49664	Andres:0	LISTENING
TCP	0.0.0.0:49665	Andres:0	LISTENING
TCP	0.0.0.0:49666	Andres:0	LISTENING
TCP	0.0.0.0:49667	Andres:0	LISTENING

3. Habilite el servicio de escritorio remoto. Inicio > Panel de Control > Sistema y seguridad > Permitir Acceso Remoto. Verifique que la casilla “Permitir conexiones de asistencia remota a este equipo” está marcada. Verifique que la opción “Permitir las conexiónes desde equipos que ejecuten cualquier versión de escritorio remoto (Menos seguro)” este seleccionada.
4. Repita una vez más el punto 2. Determine cuál es el nuevo puerto que está en escucha, después de habilitar el servicio de escritorio remoto. **R:/ 3989**
5. Utilice nmap para obtener más información acerca del servicio RDP (puerto Acceso Remoto). Utilice el comando nmap –sT -sV –PN –p puertordp localhost. Ingrese toda la información obtenida en este documento.

   R:/

   Starting Nmap 7.97 (https://nmap.org) at 2025-05-16 20:08 -0500
   Nmap scan report for 192.168.69.115
   Host is up (0.043s latency).

   PORT STATE SERVICE VERSION
   3389/tcp open ms-wbt-server
   1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
   SF-Port3389-TCP:V=7.97%I=7%D=5/16%Time=6827E199%P=i686-pc-windows-windows%
   SF:r(TerminalServerCookie,13,"\x03\0\0\x13\x0e\xd0\0\0\x124\0\x02/\x08\0\x
   SF:02\0\0\0");

   Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
   Nmap done: 1 IP address (1 host up) scanned in 12.12 seconds

6. Regrese al cmd.exe e ingrese el comando whoami. El resultado es el nombre de usuario con el que tenemos abierta la sesión de Windows actual. Por favor escriba el resultado. **R:/ andres/felipe**
   keiner/gomez
7. Ingrese el comando ipconfig. ¿Cuál es su dirección IP?.

Direccion IP IPv4	**192.168.69.115**	**192.168.68.75**

8. Investigue para qué sirve el comando nbtstat. Escriba sus conclusiones.

   nbtstat nos permite ver los nombres de netbios mostrando el nombre del equipo asociado a la ip en la red local, ver tabla de nombres o el listado de los nombres netbios registrados por el equipo, ver conexiones las conexiones activas por netbios y tambien para diagnosticar la red local para resolver problemas de red y descubrimientos de host.

LET'S HACK

1. Con el nombre y apellido del compañero, **determine cuál es la dirección ip del equipo de su compañero**. Recuerde los comandos vistos anteriormente en clase (nbtstat). No utilice software de terceros por favor ya que en un ambiente real no será fácil ejecutarlos.
   R:/

   Conociendo el nombre del compañero se probo hacer ping usando diversas variantes o posibles combinaciones del nombre del compañero para poder obtener su dirección ip.

   el comando usado fue: ping -4 andres/keiner

   Nota: importante usar el -4 para forzar el uso de ipv4 y no recibir la ipv6

2. Modifique el archivo hosts ubicado en C:\Windows\System32\drivers\etc. Y creamos un registro de DNS llamado "nombreDelCompañero.com" apuntando a la ip encontrada. Abra el archivo con el bloc de notas, he ingrese una entrada de este tipo:

   andres.com 192.168.69.115
   keiner.com 192.168.69.75

   Guarde y cierre el documento.

   Nota: Es posible que el sistema no le permita guardar porque hacen falta algunos privilegios de administrador.

3. Sobre el archivo hosts, clic derecho > propiedades > seguridad, observara varios grupos (System, Administradores, Usuarios), identifique el grupo que no posee **control total**, marque el grupo y de clic en el botón editar, marque nuevamente el grupo y habilite la casilla **control total**. Clic en aceptar en ambas ventanas.
4. Revise si la configuración del archivo hosts tuvo efecto. Abra una consola de comandos cmd.exe e ingrese el siguiente comando, ping nombredelcompañero.com. Si todo ha salido bien, debería obtener la respuesta con la respectiva dirección ip.

INTENTANDO HACKIAR EL EQUIPO DEL COMPAÑERO

9. Cambie de usuario al usuario creado. Inicio > al lado derecho del botón apagar seleccione el triángulo > cambiar de usuario.
10. Abra el cliente RDP para realizar una conexión remota al equipo de su compañero. Inicio > Todos los programas > Accesorios > Conexión a escritorio remoto. Ingrese en el campo "equipo" **nombredelcompañero.com** y de clic en el botón conectar.
11. Valide los archivos usuarios.txt y contraseñas.txt entregados por su compañero, intente hackear el computador probando la combinación que ud cree tendrá éxito.
12. Una vez adentro. Busque el archivo carta.txt y cópiela en su computadora. Realice un Drag & Drop (arrastre el archivo hasta el escritorio de su computadora). Si no funciona utilice copiar y pegar.

LA REVANCHA

1. En su equipo, Cambie el puerto en el que escucha el servicio de RDP del 3389 a cualquier otro entre el 1024 – 65535. Abra una consola de comandos cmd.exe e ingrese el comando regedit.

2. Ingrese a la ruta **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\TerminalServer\WinStations\RDP-Tcp** busque el valor **PortNumber** y de doble clic. Seleccione Decimal y cambie el valor por el puerto seleccionado, de clic en aceptar.

3. Reinicie el servicio de RDP. (Clave servicios > Remote Desktop Services)

4. Valide con el comando netstat -a que en su equipo se encuentre abierto el nuevo puerto para el servicio de RDP.

5. Utilice nmap para investigar como luce el nuevo puerto en el que se encuentra el servicio de escritorio remoto. Nmap –sT -sV –Pn –p puertnuevordp localhost.

6. Utilice nmap para investigar en que puerto se encuentra el servicio de escritorio remoto en la máquina del compañero. Nmap –sT -sV –Pn –p 1024-65535 ipdelcompañero.

   R:/ el nuevo puerto que asigno mi compañero fue el puerto 3000 el servicio es el ms-wbt-server

7. Intente loguearse con el nuevo puerto de la siguiente manera. IP:Puerto, o nombredelcompañero:puerto.Ver la figura a continuación.

8. Una vez más intente realizar una conexión por escritorio remoto utilizando el nombre de usuario y contraseña.
   R:/

   direccion: ip del usuario o el dns creado en este caso podia ser: andres.com o keiner.com
   usuario: andres o keine
   contraseña: alejandra o goku242115

Trucos y Comandos

Para los nombres de equipo

Nbtstat –R > (Volver a cargar) purga y vuelve a cargar la tabla de nombres de la cache remota
Nbtstat –RR > Liberar y Actualizar
Nbtstat –c > Realiza una lista con los nombres y sus respectivas direcciones IP.

Crear un usuario en Windows

Panel de control\Cuentas de usuario y protección infantil\Cuentas de usuario\Administrar otra cuenta
Clic en crear nueva cuenta. Ingrese el nombre de la nueva cuenta (nombre de usuario). Marque la opción administrador. Clic en el botón crear cuenta.

Pasar los archivos del Target a nuestro equipo con escritorio remoto

Abrir el cliente de escritorio remoto > opciones > Recursos Locales
Marque la casilla Unidades y de clic en Aceptar y luego en conectar