

->Ex1:

<https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?name=CVE-2021-36745&vector=AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H&version=3.1>

Temporal Score Metrics	
<b>Exploit Code Maturity (E)</b>	
Not Defined (E:X)	Unproven that exploit exists (E:U) <b>Proof of concept code (E:P)</b> Functional exploit exists (E:F) High (E:H)
<b>Remediation Level (RL)</b>	
Not Defined (RL:X)	<b>Official fix (RL:O)</b> Temporary fix (RL:T) Workaround (RL:W) Unavailable (RL:U)
<b>Report Confidence (RC)</b>	
Not Defined (RC:X)	Unknown (RC:U) Reasonable (RC:R) <b>Confirmed (RC:C)</b>

Environmental Score Metrics		
<b>Exploitability Metrics</b>		
<b>Attack Vector (MAV)</b>		
Not Defined (MAV:X)	<b>Network (MAV:N)</b>	Adjacent Network (MAV:A)
Local (MAV:L)	Physical (MAV:P)	
<b>Attack Complexity (MAC)</b>		
Not Defined (MAC:X)	<b>Low (MAC:L)</b>	High (MAC:H)
<b>Privileges Required (MPR)</b>		
Not Defined (MPR:X)	<b>None (MPR:N)</b>	Low (MPR:L) High (MPR:H)
<b>User Interaction (MUI)</b>		
Not Defined (MUI:X)	<b>None (MUI:N)</b>	Required (MUI:R)
<b>Scope (MS)</b>		
Not Defined (MS:X)	<b>Unchanged (MS:U)</b>	Changed (MS:C)

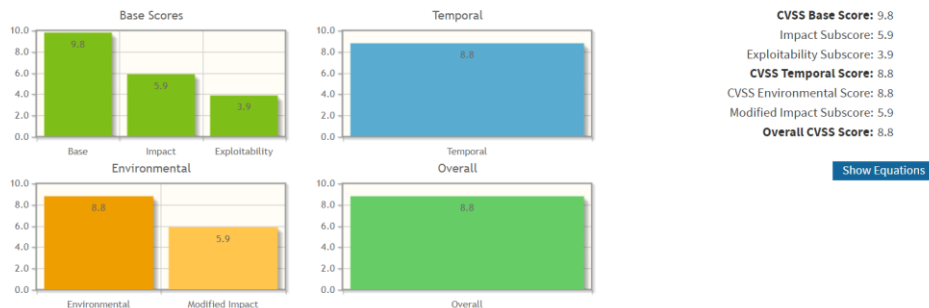
  

<b>Impact Metrics</b>	<b>Impact Subscore Modifiers</b>
<b>Confidentiality Impact (MC)</b>	<b>Confidentiality Requirement (CR)</b>
Not Defined (MC:X) None (MC:N) Low (MC:L)	Not Defined (CR:X) Low (CR:L)
<b>High (MC:H)</b>	Medium (CR:M) <b>High (CR:H)</b>
<b>Integrity Impact (MI)</b>	<b>Integrity Requirement (IR)</b>
Not Defined (MI:X) None (MI:N) Low (MI:L)	Not Defined (IR:X) Low (IR:L) Medium (IR:M)
<b>High (MI:H)</b>	<b>High (IR:H)</b>
<b>Availability Impact (MA)</b>	<b>Availability Requirement (AR)</b>
Not Defined (MA:X) None (MA:N) Low (MA:L)	Not Defined (AR:X) Low (AR:L)
<b>High (MA:H)</b>	Medium (AR:M) <b>High (AR:H)</b>

## Common Vulnerability Scoring System Calculator CVE-2021-36745

### Source: NIST

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.



->Ex3

### Breve parágrafo:

Durante a captura de tráfego à saída de A1 antes de arrancar os terminais e routers da topologia, foi possível observar um conjunto de PDUs. Inicialmente, foi realizada uma resolução de endereços (ARP) para determinar o endereço MAC correspondente ao endereço IP da interface Ethernet de R1. Após esta resolução, foi iniciado um three-way handshake, com a troca de mensagens SYN, SYN-ACK e ACK entre A1 e R1. Uma vez estabelecida a conexão, o servidor SSH de R1 apresentou a mensagem "Are you sure you want to continue connecting (yes/no)?" e aguardou pela resposta do utilizador. Como este não respondeu, não foi estabelecida a autenticação.

->Ex4:

Apos ter respondido yes, observei um aumento de trafego na captura. Foram trocados pacotes relacionados à autenticação e estabelecimento de uma conexão segura. Durante este processo, a chave publica de R1 foi enviada para A1 para garantir a autenticidade do servidor e prevenir ataques do tipo MITM.

->Ex5:

A primeira parte do output

"|1|hKuo4VzOQhSjkcJkwUTvnXSjBJ8=|zcYwk/3s2zIG2/bhb6ltyWp+YKk=" é um identificador de hash do host remoto e a segunda parte é a chave pública do host.

A terceira parte "ssh-rsa

AAAAB3NzaC1yc2EAAAADAQABAAQgQCUudc60E67n3NFulho3+muswV10p7N27ELE8w56F/Vj60DcrbxV6KOaMKHmb5zOJNJf0Omtu6Vu4ESqGN1XOop6Y09vDfjPRJpnb4QlzpDqtNrpgf/ta67qxXp81lkPcRJP25zT26dx3Z6MU8uTPBGxFzpCetcMoeQMwaVo/jLxw==" é a chave pública do host remoto em si, no formato "tipo-chave chave-pública".

Esse arquivo é utilizado para verificar a autenticidade dos hosts remotos, e é atualizado automaticamente toda vez que um novo host é acessado pela primeira vez via SSH.

->Ex6:

Pacote 64

->Ex7:

Inserindo a palavra "password" no campo find deve destacar a parte da stream onde a senha é enviada, porem isso só funciona se a senha for enviada em cleartext. Como estamos a usar uma SSH a password é cifrada e não poderá ser lida diretamente, logo, não resulta em destaque nenhum quando procurarmos a palavra "password".

->Ex8:

O melhor formato é um por linha, contendo um nome de host, numero de bits, expoente e módulo. No início da linha está o nome do host ou uma hash que representa o nome do host.

Após correr o comando:

```
ipterm-1 - PuTTY
[1]+  Stopped                  ssh admina110@192.168.100.240
root@ipterm-1:~# fg
ssh admina110@192.168.100.240
Password:

R1-4110>exit
Connection to 192.168.100.240 closed.
root@ipterm-1:~# ssh-keygen -F 192.168.100.240
# Host 192.168.100.240 found: line 1 type RSA
|1|hKuo4Vz0QhSjkcJkwUTvnXSjBj8=|zcYwk/3s2zIG2/bhb6ltyWp+YKk= ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQ=
root@ipterm-1:~# ls -l .ssh/known_hosts
-rw-r--r-- 1 root root 274 Apr 20 19:04 .ssh/known_hosts
root@ipterm-1:~# cat .ssh/known_hosts
bash: .ssh/known_hosts: Permission denied
root@ipterm-1:~# ls -l .ssh/known_hosts
-rw-r--r-- 1 root root 274 Apr 20 19:04 .ssh/known_hosts
root@ipterm-1:~# date
Thu Apr 20 21:50:52 UTC 2023
root@ipterm-1:~# ls -l .ssh/known_hosts
-rw-r--r-- 1 root root 274 Apr 20 19:04 .ssh/known_hosts
root@ipterm-1:~# cat .ssh/known_hosts
|1|hKuo4Vz0QhSjkcJkwUTvnXSjBj8=|zcYwk/3s2zIG2/bhb6ltyWp+YKk= ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQ=
root@ipterm-1:~# bash: .ssh/known_hosts: Permission denied
bash: bash:: command not found
root@ipterm-1:~#
```

Significa que o host foi encontrado na linha 1 do arquivo known\_hosts e a chave publica RSA associada a ele é a segunda linha.

No ficheiro .ssh/known\_hosts o endereço IP é legível? Em que formato estará guardado? Encontra algum motivo para não surgir em clear text?

Resposta: Não se encontra legível. Está guardado em formato hash.

A principal razão para armazenar os IP's em formato hash é para impedir que alguém possa ver facilmente a lista de servidores aos quais o user entrou. É importante estar assim para que quando o arquivo known\_hosts é armazenado num sítio onde outros users podem entrar.

O arquivo não atualiza pois este só é atualizado quando um user se conecta com sucesso.

Ao executar o programa não aparece nada porque não existe nenhum host no arquivo known\_hosts.

->Ex9:

A mensagem é exibida pela primeira vez quando um user tenta se conectar por ssh pela primeira vez. Isto acontece pq o user não tem nenhuma informação sobre a identidade do servidor e precisa de confirmar com o user se ele deseja continuar com a ligação.

Como já tinha respondido anteriormente com yes, a chave pública é guardada no arquivo known\_hosts. Nas próximas ligações ao mesmo servidor SSH, o user verifica a identidade do servidor comparando a chave que existe no arquivo known\_hosts com a que há no servidor e caso sejam iguais a ligação continua sem exibir a mensagem.

->Ex10:

- parser view DiogoSoares-VIEWA
- secret PASSWORD
- commands exec include configure terminal
- commands configure include interface Ethernet 0/1
- commands configure interface Ethernet 0/1 include ip address
- commands configure interface Ethernet 0/1 include description
- commands configure interface Ethernet 0/1 include shutdown

```
aaa new-model
aaa authentication login default
local
aaa authorization exec default
local
```

```
R1-4110#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1-4110(config)#username admina110 view DiogoSoares-VIEWA
R1-4110(config)#
```

```

R1-4110#sh running | begin parser
*Apr 20 23:01:03.063: %SYS-5-CONFIG_I: Configured from console by admin on console
R1-4110#sh running | begin parser
parser view DiogoSoares-VIEWA
secret 5 $1$uGrl$qPtF/6xYpnKESgk65YyHM.
commands interface include ethernet
commands interface include ethernet-transit-oui
commands interface include shutdown
commands interface include ip address
commands interface include ip
commands interface include description
commands configure include interface
commands exec include configure terminal
commands exec include configure
commands configure include interface Ethernet0/1
!
!
line con 0
password 7 00071A150754080F1C2243
logging synchronous
line aux 0
line vty 0 4
password 7 070C285F4D061A0C041104
transport input ssh
!
!
--More--

```

->Ex11:

```

root@ipterm-1:~# ssh admina110@192.168.100.240
Password:
R1-4110#show users
      ^
% Invalid input detected at '^' marker.

R1-4110#show ?
  banner  Display banner information
  parser  Display parser information

R1-4110#show parser
% Incomplete command.

R1-4110#show parser ?
  csb     Show csb information
  view    Show view configuration

R1-4110#show parser view
Current view is 'DiogoSoares-VIEWA'
R1-4110#

```

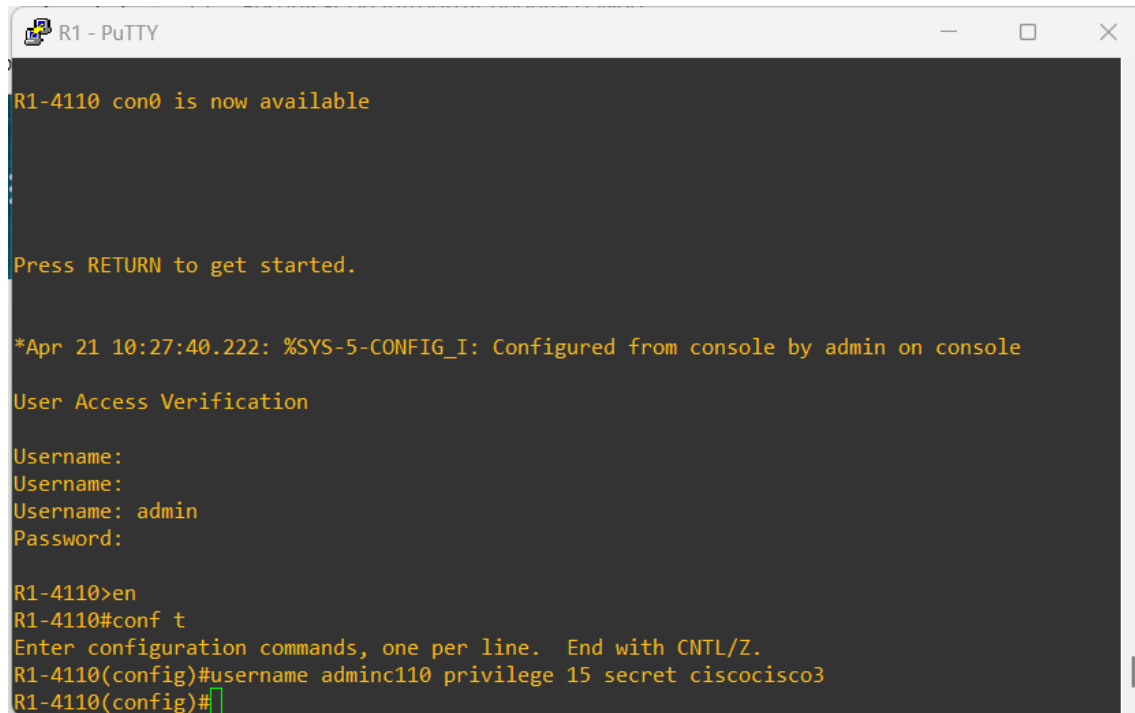
->Ex12:

Tem acesso a todos os comandos e recursos disponíveis em R1.

->Ex13:

Igual porem configura-se a ethernet 0/0

->Ex14:



```
R1-4110 con0 is now available

Press RETURN to get started.

*Apr 21 10:27:40.222: %SYS-5-CONFIG_I: Configured from console by admin on console

User Access Verification

Username:
Username:
Username: admin
Password:

R1-4110>en
R1-4110#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1-4110(config)#username adminc110 privilege 15 secret ciscocisco3
R1-4110(config)#
```

quando logo por ssh [adminc110@192.168.200.240](ssh:adminc110@192.168.200.240) entro e faço ? e aparece todos os comandos.

->Ex15:

```
configure terminal
parser view admin superview
view view1
view view2
end
```

->Ex16:

192.168.100.100

..02

->Ex17:

A RFC 5424 define o formato das mensagens syslog, que contém várias partes:

PRI

HEADER

MSG

Ao expandir a camada syslog message na PDU capturada conseguimos então ver essas partes da mensagem e analisar o conteúdo. Conseguimos verificar o timestamp, o endereço IP de T1 que gerou a mensagem no header e ver o conteúdo da mensagem no MSG.

Ex17 e 18:

```
R1 - PuTTY

*Apr 21 11:40:49.426: %SYS-5-CONFIG_I: Configured from console by admin on console
le

User Access Verification

Username: admin
Password:

R1-4110>en
R1-4110#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1-4110(config)#login on
R1-4110(config)#logging host 192.168.100.100
R1-4110(config)#logging host 192.168.100.
*Apr 21 11:52:09.672: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 192.168.100.
100 port 514 started - CLI initiated
R1-4110(config)#logging trap 7
R1-4110(config)#do wr
Building configuration...
[OK]
R1-4110(config)#service timestamps log datetime
R1-4110(config)#
```

->Ex19:

Significa que não existirá mais tráfego Syslog entre o servidor Syslog e R1.

```
R1 - PuTTY


R1-4110(config)#service timestamps log datetime
R1-4110(config)#do wr
Building configuration...
[OK]
R1-4110(config)#logging trap informational
R1-4110(config)#do sh logging
Syslog logging: enabled (0 messages dropped, 13 messages rate-limited, 0 flushes
, 0 overruns, xml disabled, filtering disabled)

No Active Message Discriminator.

No Inactive Message Discriminator.

Console logging: level debugging, 33 messages logged, xml disabled,
filtering disabled
Monitor logging: level debugging, 0 messages logged, xml disabled,
filtering disabled
Buffer logging: level debugging, 44 messages logged, xml disabled,
filtering disabled
Exception Logging: size (4096 bytes)
Count and timestamp logging messages: disabled
```

->Ex20:

 você pode usar o recurso `archive` do roteador Cisco para realizar backups automáticos da configuração do roteador para um servidor TFTP. O comando `archive` permite especificar o caminho para o servidor TFTP e o formato do nome do arquivo de backup. Você também pode usar o comando `write-memory` para fazer backup da configuração sempre que ela for alterada e o comando `time-period` para especificar a frequência dos backups.

No seu caso, você pode usar os seguintes comandos para ativar o processo de backup de 5 em 5 minutos em T1:

```
configure terminal
archive
  path
  tftp://192.168.100.100/$h-$t
  write-memory
  time-period 5
end
```

->Ex21:

Archive: entra no modo de conf do recurso archive

Log config: entra no modo de conf do registo de alterações de config

Logging enable: ativa o registo de alterações de config.

Notify syslog: envia nots de alterações de conf para o servidor syslog

Hidekeys: oculta informações confidenciais como pass's no registo de alterações de conf.



->Ex22:

```
R1 - PuTTY
R1-4110(config)#copy ri
R1-4110(config)#copy ru
R1-4110(config)#copy runn
R1-4110(config)#exit
R1-4110#copyt
*Apr 21 13:07:42: %SYS-5-CONFIG_I: Configured from console by admin on console
R1-4110#copy ru
R1-4110#copy running-config tftp
Address or name of remote host []? T1
Translating "T1"...domain server (255.255.255.255)

?Invalid host address or name
%Error parsing filename (Invalid IP address or hostname)
R1-4110#copy running-config tftp
Address or name of remote host []? name of remote host
?Invalid host address or name
%Error parsing filename (Invalid IP address or hostname)
R1-4110#copy running-config tftp
Address or name of remote host []? 192.168.100.100
Destination filename [r1-4110-config]? backup
!!
3436 bytes copied in 0.084 secs (40905 bytes/sec)

R1-4110#
```

->Ex22:

Para adicionar um novo usuário chamado `webadmin` com privilégios 15 em R1, você pode usar os seguintes comandos no modo de configuração global do roteador:

```
configure terminal
username webadmin privilege 15
password senha
end
```

Para ativar o serviço HTTP em R1 e configurar a autenticação de acesso com base na base de dados local, você pode usar os seguintes comandos:

```
configure terminal
ip http server
ip http authentication local
end
```

Depois de executar esses comandos, você poderá acessar a interface Web do roteador R1 usando o navegador Firefox no terminal BRW-1. Basta digitar o endereço IP do roteador na barra de endereço do navegador e fazer login com o nome de usuário e senha que você criou anteriormente.

Quanto à sua pergunta sobre a captura de tráfego de autenticação, se você estiver usando o protocolo HTTP (em vez de HTTPS), as informações de autenticação, incluindo a senha, serão transmitidas em texto claro e poderão ser vistas em uma captura de tráfego. É recomendável usar o protocolo HTTPS para criptografar as informações de autenticação e aumentar a segurança.

## Pacote 19

