

# تال دېم ل او تاه جوم ل ا ى ل ع SSH ن ي و ك ت

## تاي و ت ح م ل ا

[ق م د ق م ل ا](#)

[ق ي س ا س ا ل ا ت ا ب ل ط ت م ل ا](#)

[ت ا ب ل ط ت م ل ا](#)

[ق م د خ ت س م ل ا ت ا ن و ك م ل ا](#)

[ت ا خ ا ل ط ص ا ل ا](#)

[2 ر ا د ص ا ل ا SSH ق ك ب ش ل ي ط ي ط خ ت ل ا م س ر ل ا](#)

[ق ق د ا ص م ل ا ر ا ب ت خ ا](#)

[SSH ن و د ق ق د ا ص م ل ا ر ا ب ت خ ا](#)

[SSH ع م ق ق د ا ص م ل ا ر ا ب ت خ ا](#)

[ق ي ر ا ي ت خ ا ل ا ن ي و ك ت ل ا ت ا ع و م ج م](#)

[SSH ف ا ل خ ب ت ا ل ا ص ت ا ل ا ع ن م](#)

[SSH ل ي م ع ك ل و ح م ل ا و ا IOS ق ج و م د ا د ع ا](#)

[RSA ى ل ا ق د ن ت س م ل ا م د خ ت س م ل ا ق ق د ا ص م ذ ي ف ن ت ب م و ق ي ي ذ ل ا SSH م د ا خ ك IOS ق ج و م د ا د ع ا](#)

[ي ف ر ط ل ا SSH ط خ ى ل ا ت م ا ل ا ل و ص و ل ا ق ف ا ض ا](#)

[ق ي ع ر ف ق ك ب ش ى ل ا SSH ل و ص و د ي ق ت](#)

[2 ر ا د ص ا ل ا SSH ن ي و ك ت](#)

[ب ا ع ش ل ا ر م ا ج ا ر خ ا ى ل ع ت ا ف ا ل ت خ ا ل ا](#)

[ب ا ع ش ل ا ر م ا ب ا ي خ](#)

[Telnet](#)

[SSH v2](#)

[LoginBanner ص ب ع ر ذ ع ت ي](#)

[show و debug ر م ا و ا](#)

[ق ن ي ع ل ل ا ع ا ط خ ا ل ا ج ي ح ص ت ج ا ر خ ا](#)

[ق ج و م ل ا ع ا ط خ ا ج ي ح ص ت](#)

[م د ا خ ل ا ع ا ط خ ا ج ي ح ص ت](#)

[ج ي ح ص ل ا ر ي غ ن ي و ك ت ل ا](#)

[\(DES\) ت ا ن ا ي ب ل ا ر ي ف ش ت ر ا ي ع م م ا د خ ت س ا ب SSH ل ي م ع ن م SSH ل ي و ح ت م ت ي م ل](#)

[ق ج ي ح ص ر ي غ ر و ر م ل ا ق م ل ك](#)

[ق ج و م ل ا ع ا ط خ ا ج ي ح ص ت](#)

[ق م و ع د م ر ي غ \(Blowfish\) ق ر ف ش SSH ل ي م ع ل س ر ي](#)

[ق ج و م ل ا ع ا ط خ ا ج ي ح ص ت](#)

[ا ط خ ل ا "ل ص ا خ ل ا RSA ج ا ت ف م د ا د ر ت س ا ر ذ ع ت ي: %SSH-3-PRIVATEKEY" ى ل ع ل و ص ح ل ا](#)

[ج ن ا ص ن ل ا](#)

[ق ل ص ت ا ذ ت ا م و ل ع م](#)

## ق م د ق م ل ا

و ا Cisco ت ا ه ج و م ى ل ع ه ا ط خ ا ج ي ح ص ت و (SSH) Secure Shell ن ي و ك ت ق ي ف ي ك د ن ت س م ل ا ا ذ ه ف ص ي

Cisco IOS® جمانرب ليغشتب موقت يتال تالدبملا

## ةيساسال تابلطتملا

### تابلطتملا

ليبس ىلع SSH معدل (ريفتت) k9 ةروص ةمدختسُملا Cisco IOS ةروص نوكت نأ بجي (ريفتت) k9 ةروص وه c3750e-universalk9-tar.122-35.SE5.tar، لاثملا

### ةمدختسُملا تانوكملا

Cisco IOS 3600 (C3640-IK9S-M) جمانرب ىل دننتسُملا اذه يف ةدراول تامولعمل دننتست، رادصإلا 12.2(2)T1.

Cisco IOS نم ةيلاتلا ةيساسال ةمظنأل او روصلا يف SSH ميوقت مت

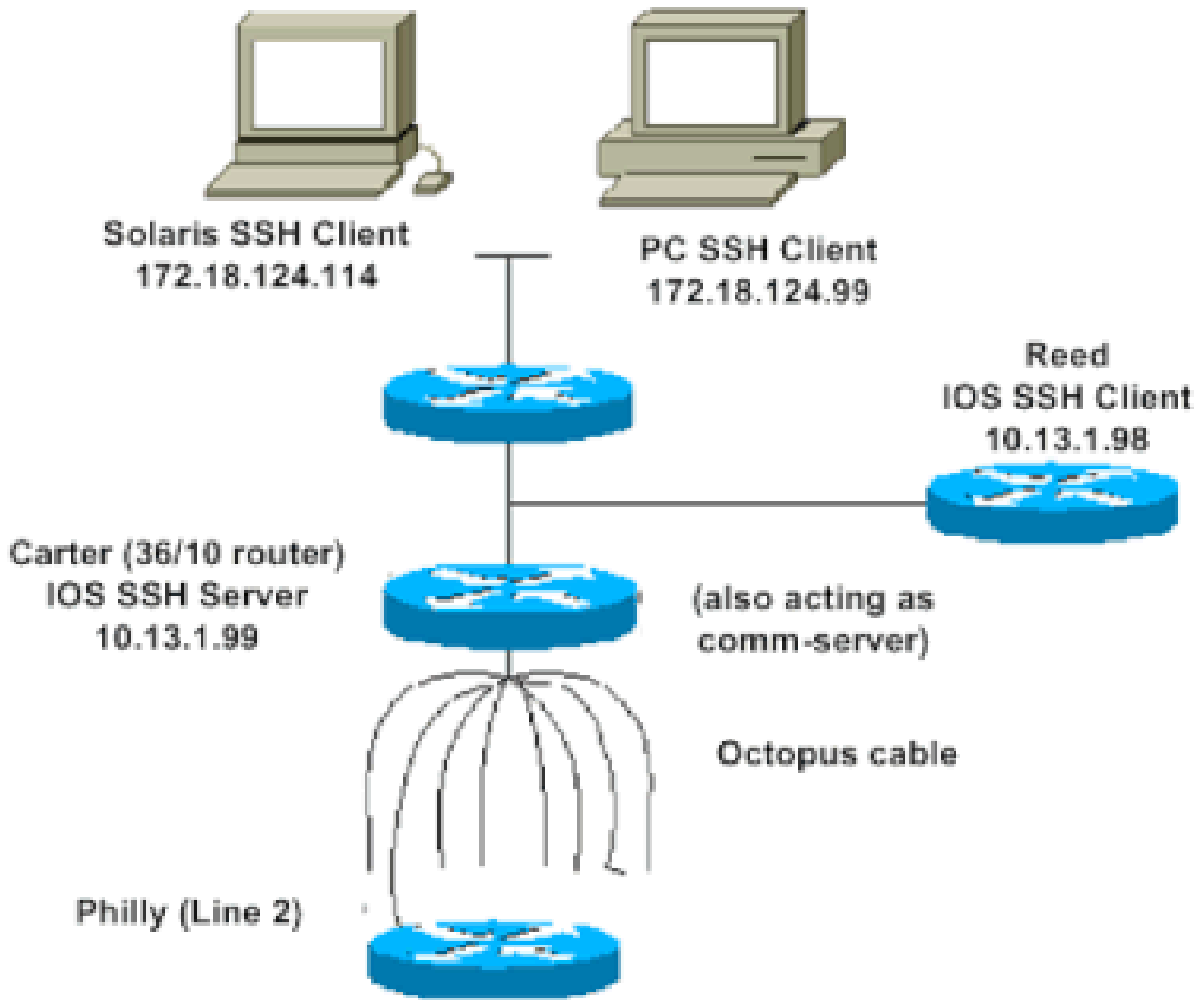
- يف (reverse-Telnet ب اضيأ فورعمل) يف رطلال SSH طخ ىل نملأل لوصول ميوقت مت رادصإلا Cisco IOS جمانرب يف أدبت يتال Cisco IOS نم ةيساسال ةمظنأل او روصلا 12.2.2.T.
- Cisco IOS نم ةيساسال ةمظنأل او روصلا يف (SSH v2) 2.0 رادصإلا SSH ميوقت مت رادصإلا Cisco IOS جمانرب يف أدبت يتال 12.1(19)E.

ةصاخ ةيلمعم ةئيب يف ةدوجوملا ةزهجال نم دننتسُملا اذه يف ةدراول تامولعمل عاشنإ مت تناك اذإ. (يضارتفا) حوسمم نيوكتب دننتسُملا اذه يف ةمدختسُملا ةزهجال عيمج تادب رمأ يأل لم تحملا ريثأتلل كمهف نم دكأتف، ليغشتلا ديقتك تكبش

### تاحالطصالا

تامولعمل نم ديزم ىلع لوصحلل [ةينقتلا Cisco تاحيملت تاحالطصا](#) عجار

## 2 رادصإلا SSH ةكبش ليطي طختلا مسرلا



## ةقداصملا رابتخا

### SSH نود ةقداصملا رابتخا

SSH ةفاضل لباق هجّوملل Carter عم ةقداصملا لمع نم دكأتلل آل وأ SSH نود ةقداصملا ربتخا لي وختلاو ةقداصملا مداخ ب وأ نيي لحم رورم ةملاك و مدختسم مساب ةقداصملا نوكت نأ نكمي لال نمةقداصملا مت نأ نكمي ال). RADIUS أو TACACS+ لّغشي يذلا (AAA) ةبساحملاو مادختسا كل حيتت يتلاو، ةي لحملا ةقداصملا لاثملا اذه حضوي (SSH عم رطسلا رورم ةملاك cisco رورملا ةملاك و cisco مدختسملا مساب هجّوملا يف Telnet.

✍ ةيفرطلا ةطحملا عون ىلإ ةراشلال vty مادختسا متي، دنتسملا اذه يف: ةظالم ةيرهاظلا.

!--- The aaa new-model command causes the local username and password on the router to be used in the a

```
aaa new-model
username cisco password 0 cisco
line vty 0 4
```

```
transport input telnet
```

!--- Instead of aaa new-model, you can use the login local command.

## SSH عم ةقداصملا رابتخا

ىلع SSH نيكمتل ةقباصولا تارابعلا ىلإ ةفاضلا كىلج بجي، SSH عم ةقداصملا رابتخا ل Carter، و UNIX و PC تاطحم نم SSH رابتخاو.

```
ip domain-name rtp.cisco.com
```

!--- Generate an SSH key to be used with SSH.

```
crypto key generate rsa  
ip ssh time-out 60  
ip ssh authentication-retries 2
```

هؤاشنإ مت يذلا حاتفملا show crypto key mypubkey rsa رمألا ضرعي نأ بجي، ةطقنلا هذه دن ع رتوي بمكلا زايج نم هجوملا ىلإ لوصولا ىلع كتردق ربتخا، SSH نيوكت ةفاضلا دعب UNIX ةطحم و يصخشلا.

## ةيراي تخال نيوكتلا تاعومجم

### SSH فالخب تالاصتالاع نم

لفسأ transport input ssh رمألا ةفاضلا مقف، SSH فالخب تالاصتالاع نم يف بغرت تنك اذا (SSH فالخب) Telnet جمارب ضفر متي. طقف SSH تالاصتالاع هجوملا ديدحتل رطسألا ةرشابملا.

```
line vty 0 4
```

!--- Prevent non-SSH Telnets.

```
transport input ssh
```

ىلإ Telnet مادختسا SSH فالخب جماربلا يمدختسمل نكمي ال هنأ نم دكأتلل رابتخا عارجا مق هجوملل Carter.

### SSH ليمعك لوحملا وأ IOS هجوم دادعإ

Cisco IOS هجوم ىلع SSH معد نيكمتل ةبولطم تاوطخ عبرا كانه:

1. hostname رمألا نيوكت مق .

2. DNS لاجم نيوكتب مق.

3. SSH حاتفم ئشنأ.

4. (vty) يضارتفالال عونلل ةيفرطالال ةدحولل SSH لقن معد نيكمتب مق.

زاهج لىل SSH ةفاضل كنكميف ، رخال لىل SSH ليمعك لمعي دحاو زاهج كي دل نوكي نأ تدراً اذإ ، مداخل Carter لمعي شيح ، مداخل-ال-ليمعل بيترت يفةزهجال هذه كلذ عضي و Reed يمسي ناث نيوكتل بولطمال هسفن وه Reed لىل Cisco IOS SSH ليمع نيوكت . ليمعك Reed لمعي و مداخل Carter لىل SSH مداخل

!--- Step 1: Configure the hostname if you have not previously done so.

```
hostname carter
```

!--- The aaa new-model command causes the local username and password on the router to be used in the a

```
aaa new-model
username cisco password 0 cisco
```

!--- Step 2: Configure the DNS domain of the router.

```
ip domain-name rtp.cisco.com
```

!--- Step 3: Generate an SSH key to be used with SSH.

```
crypto key generate rsa
ip ssh time-out 60
ip ssh authentication-retries 2
```

!--- Step 4: By default the vty transport is Telnet. In this case, Telnet is disabled and only SSH is s

```
line vty 0 4
transport input ssh
```

!--- Instead of aaa new-model, you can use the login local command.

مق Cisco IOS SSH (Carter) مداخل لىل Cisco IOS SSH (Reed) ليمع نم SSH لىل رمأال اذه رادصاب مق اذه رابتخال

```
ssh -v 2 -c aes256-cbc -m hmac-sha1-160 -l cisco 10.31.1.99
```

ةدنتسملال مدختسملال ةقداصم ذي فننتب موقوي يذال SSH مداخلك IOS ةجوم دادعإ لىل RSA

لىل RSA ةدنتسملال ةقداصم ذي فننتل SSH مداخل نيوكتل تاوطخال هذه لمكأ

1. فيضمال مسا ددح.

```
Router(config)#hostname <host name>
```

2. يضرارتفا لاجم مسا دي دحتب مق.

```
Router(config)#ip domain-name <Domain Name>
```

3. RSA حيتافم جاوزأ عاشنإب مق.

```
Router(config)#crypto key generate rsa
```

4. مداخل او مدختس مل اة قداصل مل SSH-RSA حيتافم ني وك ت ب مق.

```
Router(config)#ip ssh pubkey-chain
```

5. SSH مدختس م مسا ني وك ت ب مق.

```
Router(conf-ssh-pubkey)#username <user name>
```

6. دي عب ل ري ظن ل ل ماع ل RSA حات فم ددح.

```
Router(conf-ssh-pubkey-user)#key-string
```

7. (ة راي تخا ة و ط خ ل ا هذ ه). ه راد ص ا و SSH حات فم عون ددح.

```
Router(conf-ssh-pubkey-data)#key-hash ssh-rsa <key ID>
```

8. تازا ي ت م ا ل ا ي ذ EXEC عضو ل ا و و ج ر ل ا و ي ل ا ح ل ا عضو ل ا ن م ج و ر خ ل ا ب مق.

```
Router(conf-ssh-pubkey-data)#end
```

## يفرطال SSH طخ ىلإ نمآال لوصول ةفاضإ

جماربل هرابتخاو SSH نيوكت كنكمي ف، رداصلال يفرطال SSH طخ رطس ةقداصلم ىلإ تجتخا اذا  
ايفلداليف ىلإ تالاصتا مداخلك لمعي يذلاو، Carter لال خ نم ةرداصلال ةيسكعل Telnet.

```
ip ssh port 2001 rotary 1
line 1 16
  no exec
  rotary 1
  transport input ssh
  exec-timeout 0 0
  modem InOut
  stopbits 1
```

ىلإ SSH نيوكت كنكمي ف، Carter- ب صاخلا 2 ذفنم لابل ةلصتم ايفلداليف تناك اذا  
رمأل اذه مداخلتساب Reed نم Carter لال خ نم ايفلداليف:

```
ssh -v 2 -c aes256-cbc -m hmac-sha1-160 -p 2002 10.31.1.99
```

Solaris: نم رمال اذه مداخلتسا كنكمي:

```
ssh -c 3des -p 2002 -x -v 10.13.1.99
```

## ةيعرف ةكبش ىلإ SSH لوصول دييقت

تالواحم عيمج طاقسا متي شيح ةنيعم ةيعرف ةكبش SSH لاصلتا دييقت ىلإ جاتحتس  
ةيعرفال ةكبشال جراخ IP تالوكوتورب نم ىرخأل SSH.


هسفن رمالابل مايقلل تاوطخال هذه مداخلتسا كنكمي:

1. ةنيعملال ةيعرفال ةكبشال هذه نم رورمالا ةكحبحمست لوصول ةمئاق ديحت.
2. لوصول ةئف مداخلتساب VTY رطس ةهجاو ىلإ لوصول دييقت.

ةيعرفال ةكبشال ىلإ طقف SSH لوصول حومسم، لاثملا اذه في. نيوكتال ىلع لاثم اذه  
10.10.10.0 255.255.255.0، رخأ لوصول اضر متيو.

```
Router(config)#access-list 23 permit 10.10.10.0 0.0.0.255
Router(config)#line vty 5 15
Router(config-line)#transport input ssh
Router(config-line)#access-class 23 in
```

Router(config-line)#exit

 ةيساسألأ ةمظنألل SSH لوصو ني مأتل اضيأ هس فن ءارجإلأ مادختسا متي: ةظحال م لوجملل.

## 2 رادصلإلأ، SSH ني وكت

```
carter(config)#ip ssh version 2
```

## راعشللأ رمأ جارجإلأ يلع تافالخال

اذه حضوي SSH تالاصتتا نم ةفلتخملأ تارادصلإلأ او Telnet ني ب banner رمأ جارجإلأ فلتخي تالاصتالآ نم ةفلتخم ءاونأ عم banner رمأ تاراخي لمع فالتخا دم لودجال

راعشللأ رمأ رايخ	Telnet	SSH v2
راعشللأ لجس	يلإ لوخدلا ليجست لبق ضرع زاهجال	يلإ لوخدلا ليجست لبق ضرع زاهجال
banner motd	يلإ لوخدلا ليجست لبق ضرع زاهجال	يلإ لوخدلا ليجست دعب ضرع زاهج
banner exec	يلإ لوخدلا ليجست دعب ضرع زاهج	يلإ لوخدلا ليجست دعب ضرع زاهج

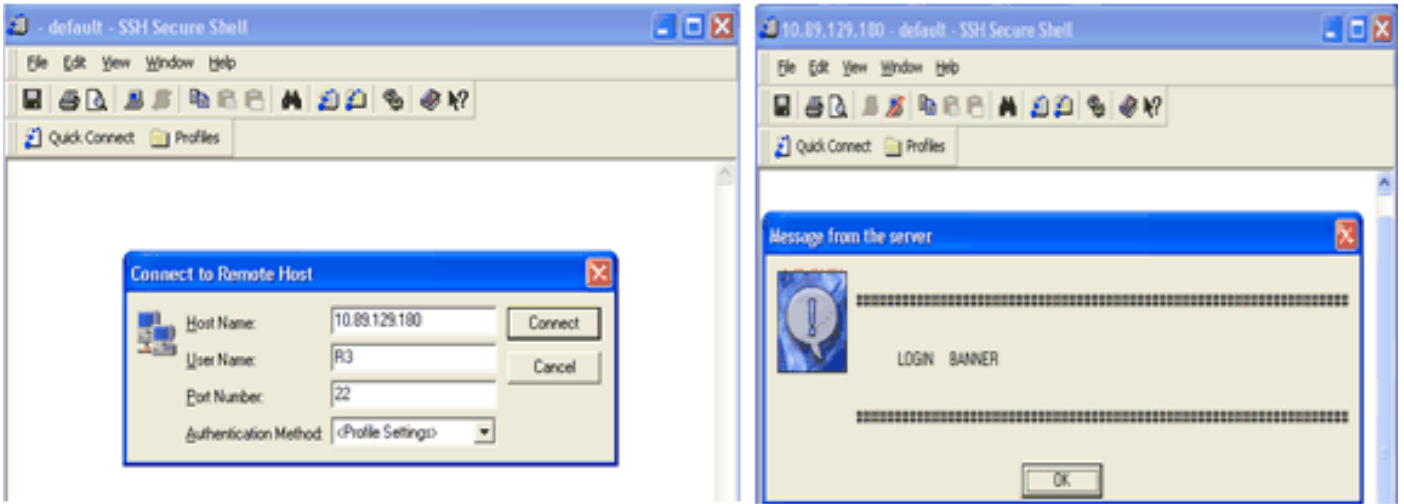
 ن.سحتسم SSH نم 1 رادصلإلأ دعي مل: ةظحال م.

## لوخدلا ليجست راعش ضرع رذعتي

ضرع متي Cisco هجوم عم SSH ةسلج أدبې ام دنع . لوخدلا ليجست راعش 2 رادصلإلأ SSH معدي مادختسا دنع ، لاثلما ليلبس يلع . مدختسمال مسا SSH ليمع لسرا اذا لوخدلا ليجست راعش ال ، PuTTY ssh ليمع مادختسا دنع . لوخدلا ليجست راعش ضرع متي ، Secure Shell ssh ليمع الوي ضارتفا لكشب مدختسمال مسا لسري SSH نأل كلذو . لوخدلا ليجست راعش ضرع متي ي.ضارتفا لكشب مدختسمال مسا لاسراب PuTTY موقوي .

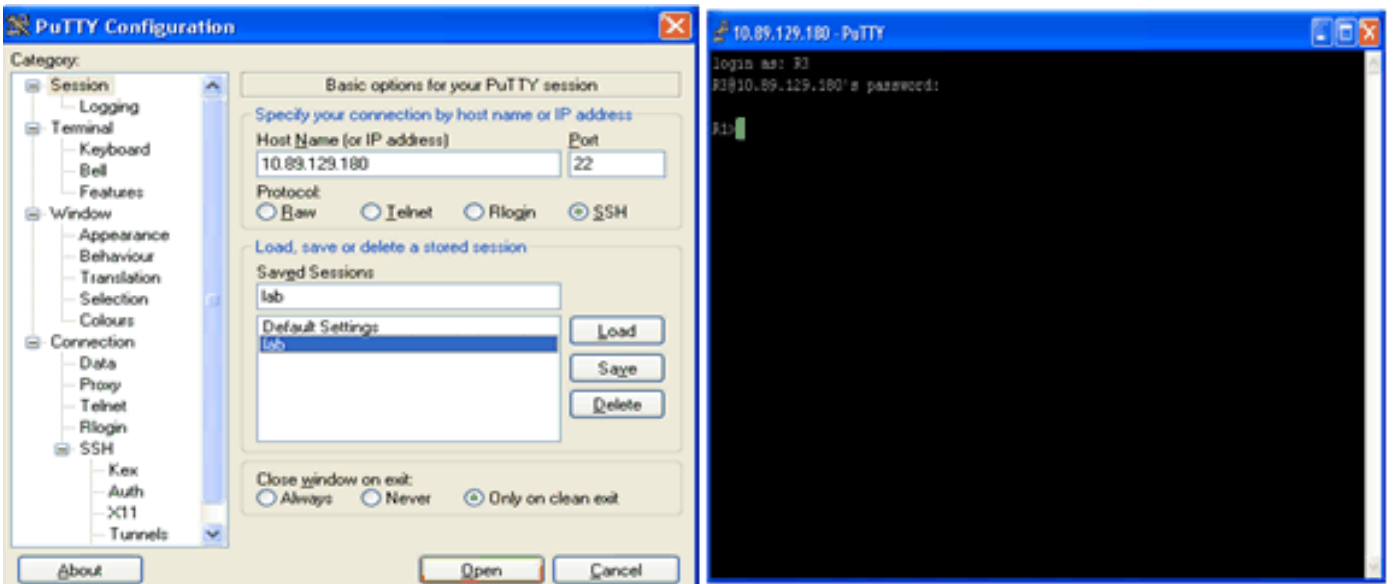
رز ني كمت متي ال SSH معدي يذلا زاهجال لاصتالآ ءدبل مدختسمال مسا SSH ليمع جاتحي هنا هذه ةشاشلأ ةروص حضوت . مدختسمال مسا او فيضمال مسا لاخداب مقت مل اذا لاصتالآ رورم ةم لكب راعشللأ بلاطي . هجوملاب SSH لاصتالآ دنع لوخدلا ليجست راعش ضرع متي





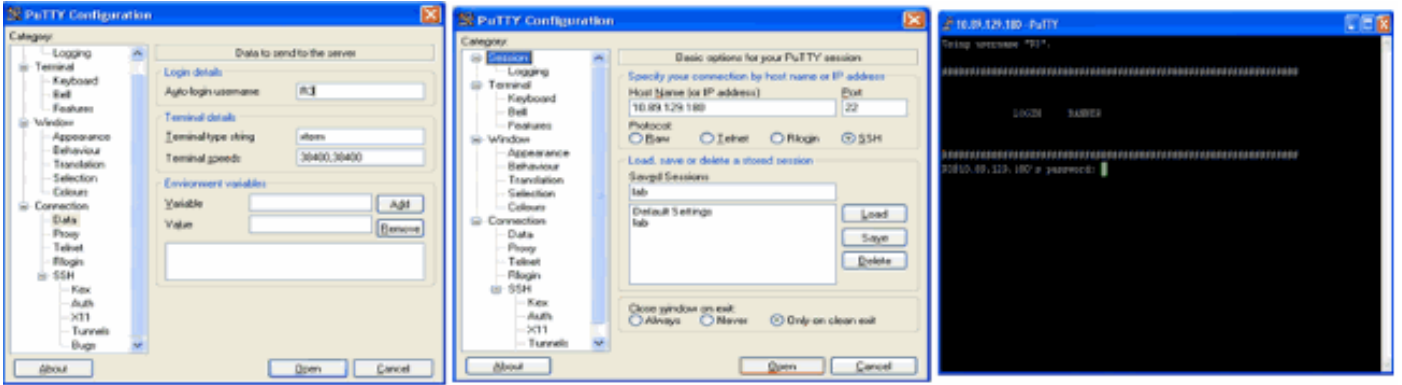
رورم ٲم لك ب راعش لا بالاطي

ٲشاشلا ٲروص حضورت . ٲجوم لاپ SSH لاصتا ءءبل مءءتسم لال مسال PuTTY ليل مع بللط تي ال راعش ضرعي الو . رورم لال ٲم لك و مءءتسم لال مسال بلطيو هجوم لاپ لصلتي PuTTY ليل مع نأ هءه لوءءلا ليل ءست



ٲجوم لاپ SSH لاصتا

لالسرال PuTTY نيوكت ءن ع هضرع م تي لوءءلا ليل ءست راعش نأ هءه ٲشاشلا ٲطق ل حضورت هجوم لال ال مءءتسم لال مسال .



Category → Connection → Data

هجوم ال اى ل مدخ تس الما مس لاس را

## أرم او debug و show

م تي . [عاطخ ال اى حصت رماو اى ف ةمه م ل ا تامول عمل ا](#) ع جار ، انه ةح وضوم ال debug رماو اى رادص ا ل بق كل اى حصت اى ت ل او ، (طوق ة ال م عمل ة ل ج س م ل) [جارخ ال اى م ج ر ت م ة ا د ا](#) ة ط س او ب show رماو اى ض ع ب م عد show رماو اى جارخ ا ل ل حصت ض رع

- debug ip ssh ل SSH. عاطخ ال اى حصت لئ اسر ضرع اى
- show ssh م داخ ت ال اصت ا ة ل ا ح ضرع اى

```
carter#show ssh
Connection      Version Encryption      State                Username
0                2.0          DES                 Session started     cisco
```

- show ip ssh ل SSH. نى و ك ت ل ا ت ا ن اى ب و رادص ال اى ضرع اى

```
carter#show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 120 secs; Authentication retries: 3
```


## ة نى عمل ل عاطخ ال اى حصت جارخ ا

هجوم ال اى ل اى حصت

```
00:23:20: SSH0: starting SSH control process
00:23:20: SSH0: sent protocol version id SSH-2.0-Cisco-1.25
00:23:20: SSH0: protocol version id is - SSH-2.0-1.2.26
00:23:20: SSH0: SSH_SMSG_PUBLIC_KEY msg
00:23:21: SSH0: SSH_CMSG_SESSION_KEY msg - length 112, type 0x03
00:23:21: SSH: RSA decrypt started
```

```
00:23:21: SSH: RSA decrypt finished
00:23:21: SSH: RSA decrypt started
00:23:21: SSH: RSA decrypt finished
00:23:21: SSH0: sending encryption confirmation
00:23:21: SSH0: keys exchanged and encryption on
00:23:21: SSH0: SSH_CMSG_USER message received
00:23:21: SSH0: authentication request for userid cisco
00:23:21: SSH0: SSH_SMSG_FAILURE message sent
00:23:23: SSH0: SSH_CMSG_AUTH_PASSWORD message received
00:23:23: SSH0: authentication successful for cisco
00:23:23: SSH0: requesting TTY
00:23:23: SSH0: setting TTY - requested: length 24, width 80; set:
    length 24, width 80
00:23:23: SSH0: invalid request - 0x22
00:23:23: SSH0: SSH_CMSG_EXEC_SHELL message received
00:23:23: SSH0: starting shell for vty
```

## مداخل اءاطخأ حىحصت

 Solaris زاهج جارخا وه اذه :ةظحالم

```
rtp-evergreen.rtp.cisco.com#ssh -c 3des -l cisco -v 10.31.1.99
rtp-evergreen#/opt/CISssh/bin/ssh -c 3des -l cisco -v 10.13.1.99
SSH Version 1.2.26 [sparc-sun-solaris2.5.1], protocol version 1.5.
Compiled with RSAREF.
rtp-evergreen: Reading configuration data /opt/CISssh/etc/ssh_config
rtp-evergreen: ssh_connect: getuid 0 geteuid 0 anon 0
rtp-evergreen: Allocated local port 1023.
rtp-evergreen: Connecting to 10.13.1.99 port 22.
rtp-evergreen: Connection established.
rtp-evergreen: Remote protocol version 2.0,
    remote software version Cisco-1.25
rtp-evergreen: Waiting for server public key.
rtp-evergreen: Received server public key (768 bits)
    and host key (512 bits).
rtp-evergreen: Host '10.13.1.99' is known and matches the host key.
rtp-evergreen: Initializing random; seed file //.ssh/random_seed
rtp-evergreen: Encryption type: 3des
rtp-evergreen: Sent encrypted session key.
rtp-evergreen: Installing crc compensation attack detector.
rtp-evergreen: Received encrypted confirmation.
rtp-evergreen: Doing password authentication.
cisco@10.13.1.99's password:
rtp-evergreen: Requesting pty.
rtp-evergreen: Failed to get local xauth data.
rtp-evergreen: Requesting X11 forwarding with authentication spoofing.
Warning: Remote host denied X11 forwarding, perhaps xauth program
    could not be run on the server side.
rtp-evergreen: Requesting shell.
rtp-evergreen: Entering interactive session.
```

## حىحصلا ريغ نيوكتلا

ريغ تانويوكتال نم ديدعال نم ةنيعلل ااطخال احيحصت جارخا لعل ماسقالا هذه يوتحت احيصلال.

(DES) تانايبال ريفشت راي عم مادختساب SSH ليمع نم SSH ليوتحت متي مل

ةحيص ريغ رورمال ةملك

ةومال ااطخال احيصت

```
00:26:51: SSH0: starting SSH control process
00:26:51: SSH0: sent protocol version id SSH-2.0-Cisco-1.25
00:26:52: SSH0: protocol version id is - SSH-2.0-1.2.26
00:26:52: SSH0: SSH_MSG_PUBLIC_KEY msg
00:26:52: SSH0: SSH_CMSG_SESSION_KEY msg - length 112, type 0x03
00:26:52: SSH: RSA decrypt started
00:26:52: SSH: RSA decrypt finished
00:26:52: SSH: RSA decrypt started
00:26:52: SSH: RSA decrypt finished
00:26:52: SSH0: sending encryption confirmation
00:26:52: SSH0: keys exchanged and encryption on
00:26:52: SSH0: SSH_CMSG_USER message received
00:26:52: SSH0: authentication request for userid cisco
00:26:52: SSH0: SSH_MSG_FAILURE message sent
00:26:54: SSH0: SSH_CMSG_AUTH_PASSWORD message received
00:26:54: SSH0: password authentication failed for cisco
00:26:54: SSH0: SSH_MSG_FAILURE message sent
00:26:54: SSH0: authentication failed for cisco (code=7)
00:26:54: SSH0: Session disconnected - error 0x07
```

ةومو دم ريغ (Blowfish) ةرفش SSH ليمع لسري

ةومال ااطخال احيصت

```
00:39:26: SSH0: starting SSH control process
00:39:26: SSH0: sent protocol version id SSH-2.0-Cisco-1.25
00:39:26: SSH0: protocol version id is - SSH-2.0-W1.0
00:39:26: SSH0: SSH_MSG_PUBLIC_KEY msg
00:39:26: SSH0: SSH_CMSG_SESSION_KEY msg - length 112, type 0x03
00:39:26: SSH0: Session disconnected - error 0x20
```

"ل صخال RSA حاتفم دادرتسا رذعتي %SSH-3-PRIVATEKEY: لعل لوصحال ااطخال

هذه ااطخال لاسر لريغشت ل افيضمال مسا و ااجمال مسا ي ريغتلل ديوي نأ نكمي ةلديبال لولحال هذه مدختسا:

- حيتافم لءاشنإ ءعأو رافصألأب RSA حيتافم ألما .

```
crypto key zeroize rsa label key_name
crypto key generate rsa label key_name modulus key_size
```

- ءةللل ءاوطخلل بّرف ،قبا سلال لحلل حجنل مل اءل :
  1. رافصألأب RSA حيتافم علمل ألما .
  2. زاهلل للمحت ءعأ .
  3. SSH- ل ءامسم ءءءل حيتافم ءاشنإب مل .

## حئل اصنل

- ءاشنإب مل ءنأف ،ءةنوناق رلرل رمأوك كب ءصاأل SSH نلوك ءرمأو أضفر مل اءل مء . لءم و فلضم مسا ءءءء نم ءكأء .كب صاأل ءءوملل لءنل RSA حيتافم ءوز SSH. مءاآ نل كمءو RSA حيتافم نم ءاوزأ ءاشنإل crypto key generate rsa رمال مءءءسا .
- هءه أءأل لءلسر لءل لوصلل كنكمل ،RSA حيتافم نم ءاوزأ نلوك ءنء :
  1. فلضم لءل مسا ءءءء مل مل .
  - ءءوملل فلضم مسا نلوكءل hostname مءل نلوكءل رمال مءءءءء نأ بءل .
  2. لءم ءءءء مل مل .
  - ءءوملل فلضم لءم نلوكءل ip domain-name مءل نلوكءل رمال مءءءءء نأ بءل .
- مل vty ءلل ءالاصءال ءءل صقأل ءلل لءل ءومسم ل SSH ءالاصءال ءءل رصءقل . اءوم vty SSH لاصءال لك مءءءسل .ءءوملل اءنلوكءل

•

ءنء .مءءءءسم لءق ءاصمل ءءوملل لءل AAA لءل نم هءنلوكءل مل ءل نامأل لوكوءورب وأ لءلم آنامل SSH مءءءسل ءضو فل ءة ساسأ ءم لك قل بءءب مل . AAA- ل أءو مءءءل ءءو لءل ءءءء مءء نم ءكأءل بءل ،AAA نلوكءل مءءءل ءءو لءل AAA لءل ءءءل مءل نلوكءل .

•


No SSH server connections running:


```
carter#show ssh %No SSHv2 server connections running.
```

عداعاب صوؤي ف ،لعفلال SSH نيوكتب تمق اذا .ححص لكشب هنيكمت متي مل وأ لّطعم SSH مداخ نأ جارخال اذه حرتقي زاهال لىل SSH مداخ نيوكت عداعال تاوطخال هذه لمكأ .زاهال ي SSH مداخ نيوكت

- أيئاقولل SSH مداخ ليطعت متي ، RSA حيتافم جاوزأ فذح دع . RSA حيتافم جاوزأ فذح

```
carter(config)#crypto key zeroize rsa
```

 SSH v2 نيكمت دن لقال لىل 768 مجحب حيتافم جاوزأ عاشن مهمل نم :تظالم

 مادختسا كنكمي ال ، RSA حيتافم فذح دع ، أضياو .كب صاخال نيوكتل لظفح دع رمأ اذه نع عجاتل نكمي ال :ريذحت عداعاب تمق اذا ال اىرأال (IPSec) IP نامأ رئاظن مادختساب تاداهشل لدابت تايلمع يف ةكراشمل وأ CA وأ تاداهشل كتداهش بلطو ، CA ةداهش لىل لوصحالو ، CA - لينيبل لىل غششال ةيناكم نيوكت عداعال RSA حيتافم عاشن اددجم ةصاخال

2. زاهال لاجمل مساو فيضمال مسا نيوكت دعأ .


```
carter(config)#hostname hostname
```

```
carter(config)#ip domain-name domainname
```

3. أيئاقولل SSH نيكمت لىل اذه يدؤي .كب صاخال هجوملل RSA حيتافم جاوزأ عاشن اب مق .

```
carter(config)#crypto key generate rsa
```

 مادختسا لوح تامولعمل نم ديزم لىل لوصحلل [12.3 رادصالا ، Cisco IOS نامأ رمأ عجرم - crypto key generate rsa](#) عجار :تظالم رمأ اذه

 ال ةمليتسم ةمزه دوجو ببسب همالتسا مت عقوتم ريغ ةلاسر عون : SSH2 أطلال ةلاسر يقلت كنكمي :تظالم هذه لحل ssh لوكوتوربل rsa حيتافم عاشن اب كمايق اناثأ حاتفملا لوط ةدايزب مق . هجومل ةطساوب اهمهف نكمي ةلكشمل .

4. SSH مداخ نيوكتب مق .

5. SSH تاملعمل نيوكتب مق مل اذا . SSH تاملعمل نيوكت كىلعل بجي ، SSH مداخل هنيوكتو Cisco تاهجوم/تالدم دأ نيكمتل . ةيضا رتفال ميقلل مادختسا متيس .

```
ip ssh {[timeout seconds] | [authentication-retries integer]}
```

```
carter(config)# ip ssh
```

ةلص تاذا تام ولعم

- [SSH جتنم معد ةحفص](#)

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا اذ ه Cisco ت مچرت  
م ل ا ل ا ا ن ا ع مچ م ف ن م دخت س م ل م عد و ت م م م دقت ل ة م ش ب ل و  
م ك ة ق م ق د ن و ك ت ن ل ة مچرت ل ض ف ا ن ا ة ظ ح ا ل م م چ ر م . ة ص ا خ ل م ه ت غ ل ب  
Cisco مچرت م ا م د ق م م ا ت ل ا ة م ف ا ر ت ح ا ل ا ة مچرت ل ا م ل ا ح ل ا و ه  
ل ا ا م ا د ا د ع و چ ر ل ا ب م ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت م ل و ئ س م  
Systems (ر ف و ت م ط ب ا ر ل ا) م ل ص ا ل ا م ز م ل چ ن ا ل ا دن ت س م ل ا