

أدبت. هجوم اللى على AAA ضيوفت نيوكت ةلاح في طرف ةمدخل أدبت، قيصدت اللى دنع: PASS. تقولا اذ في ليوخت اللى ةلحرم.

ةلواح ةداع اب كتب لاطم نكمي وأ لوصولو نم ديزم ضفر نكمي، ةقداصل لاشف دنع: لشف كنكمي، اذ فيفو. TACACS+ جم انرب اللى كلذ دمتعي. لسلست اللى في لوخذل ليجست لشف تيقلت اذ، TACACS م داخ في مدخت سملل اهنوكت مت يتل تاسايس اللى نم ققحت اللى م داخ اللى نم

في وأ في فخلل جم انرب اللى في اما اذ نوكتي نأ نكمي. ةقداصل اناثأ أطخ ثودح اللى ريشي: أطخ ةداع هجوم اللى لواحي، أطخ ةباجت سا يقلت مت اذ. هجوم لاولي مدخلل جم انرب اللى نيب ةكبش لاصلت ا مدخت سملل ةقداصل ةلديب ةقيرط مادخت سا

Cisco هجوم اللى على TACACS و AAA نم ياساس اللى نيوكت اللى وه اذ

```
aaa new-model
aaa authentication log in default group tacacs+ local
aaa authorization exec default group tacacs+ local
!
tacacs server prod
address ipv4 10.106.60.182
key cisco123
!
ip tacacs source-interface Gig 0/0
```

اه حالص او TACACS ءاطخأ فاش كتسا

1. ةوطخلل

هجوم اللى نم 49 ذفنم اللى على Telnet جم انرب مادخت سباب TACACS م داخ ب لاصلت اللى نم ققحت TACACS م داخ ب لاصلت اللى على هجوم اللى ةردق مدع ةلاح في. ةبسانم لاردصم لاهج او مادخت سباب ةكرح عنمت يتل لوصول ةمئاق وأ ةيامحلل رادج ضعب كانه نوكتي نأ نكمي، 49 ذفنم اللى على رورم ل.

```
Router#telnet 10.106.60.182 49
Trying 10.106.60.182, 49 ... Open
```

2. ةوطخلل

*Apr 6 13:32:50.462: TPLUS: Authentication start packet created for 84()
*Apr 6 13:32:50.462: TPLUS: Using server 10.106.60.182
*Apr 6 13:32:50.462: TPLUS(00000054)/0/NB_WAIT/2432818: Started 5 sec timeout
*Apr 6 13:32:50.466: TPLUS(00000054)/0/NB_WAIT: socket event 2
*Apr 6 13:32:50.466: TPLUS(00000054)/0/NB_WAIT: wrote entire 38 bytes request
*Apr 6 13:32:50.466: TPLUS(00000054)/0/READ: socket event 1
*Apr 6 13:32:50.466: TPLUS(00000054)/0/READ: Would block while reading
*Apr 6 13:32:50.466: TPLUS(00000054)/0/READ: socket event 1
*Apr 6 13:32:50.466: TPLUS(00000054)/0/READ: read entire 12 header bytes (expect 43 bytes data)
*Apr 6 13:32:50.466: TPLUS(00000054)/0/READ: socket event 1
*Apr 6 13:32:50.466: TPLUS(00000054)/0/READ: read entire 55 bytes response
*Apr 6 13:32:50.466: TPLUS(00000054)/0/2432818: Processing the reply packet
*Apr 6 13:32:50.466: TPLUS: Received authen response status GET_USER (7)
*Apr 6 13:32:53.242: TPLUS: Queuing AAA Authentication request 84 for processing
*Apr 6 13:32:53.242: TPLUS(00000054) log in timer started 1020 sec timeout
*Apr 6 13:32:53.242: TPLUS: processing authentication continue request id 84
*Apr 6 13:32:53.242: TPLUS: Authentication continue packet generated for 84
*Apr 6 13:32:53.242: TPLUS(00000054)/0/WRITE/10882BBC: Started 5 sec timeout
*Apr 6 13:32:53.242: TPLUS(00000054)/0/WRITE: wrote entire 22 bytes request
*Apr 6 13:32:53.246: TPLUS(00000054)/0/READ: socket event 1
*Apr 6 13:32:53.246: TPLUS(00000054)/0/READ: read entire 12 header bytes (expect 16 bytes data)
*Apr 6 13:32:53.246: TPLUS(00000054)/0/READ: socket event 1
*Apr 6 13:32:53.246: TPLUS(00000054)/0/READ: read entire 28 bytes response
*Apr 6 13:32:53.246: TPLUS(00000054)/0/10882BBC: Processing the reply packet
*Apr 6 13:32:53.246: TPLUS: Received authen response status GET_PASSWORD (8)
*Apr 6 13:32:54.454: TPLUS: Queuing AAA Authentication request 84 for processing
*Apr 6 13:32:54.454: TPLUS(00000054) log in timer started 1020 sec timeout
*Apr 6 13:32:54.454: TPLUS: processing authentication continue request id 84
*Apr 6 13:32:54.454: TPLUS: Authentication continue packet generated for 84
*Apr 6 13:32:54.454: TPLUS(00000054)/0/WRITE/2432818: Started 5 sec timeout
*Apr 6 13:32:54.454: TPLUS(00000054)/0/WRITE: wrote entire 22 bytes request
*Apr 6 13:32:54.458: TPLUS(00000054)/0/READ: socket event 1
*Apr 6 13:32:54.458: TPLUS(00000054)/0/READ: read entire 12 header bytes (expect 6 bytes data)
*Apr 6 13:32:54.458: TPLUS(00000054)/0/READ: socket event 1
*Apr 6 13:32:54.458: TPLUS(00000054)/0/READ: read entire 18 bytes response
*Apr 6 13:32:54.458: TPLUS(00000054)/0/2432818: Processing the reply packet
*Apr 6 13:32:54.458: TPLUS: Received authen response status PASS (2)
*Apr 6 13:32:54.462: AAA/AUTHOR (0x54): Pick method list 'default'
*Apr 6 13:32:54.462: TPLUS: Queuing AAA Authorization request 84 for processing
*Apr 6 13:32:54.462: TPLUS(00000054) log in timer started 1020 sec timeout
*Apr 6 13:32:54.462: TPLUS: processing authorization request id 84
*Apr 6 13:32:54.462: TPLUS: Protocol set to NoneSkipping
*Apr 6 13:32:54.462: TPLUS: Sending AV service=shell
Apr 6 13:32:54.462: TPLUS: Sending AV cmd
*Apr 6 13:32:54.462: TPLUS: Authorization request created for 84(cisco)
*Apr 6 13:32:54.462: TPLUS: using previously set server 10.106.60.182 from group tacacs+
*Apr 6 13:32:54.462: TPLUS(00000054)/0/NB_WAIT/2432818: Started 5 sec timeout
*Apr 6 13:32:54.462: TPLUS(00000054)/0/NB_WAIT: socket event 2
*Apr 6 13:32:54.462: TPLUS(00000054)/0/NB_WAIT: wrote entire 62 bytes request
*Apr 6 13:32:54.462: TPLUS(00000054)/0/READ: socket event 1
*Apr 6 13:32:54.462: TPLUS(00000054)/0/READ: Would block while reading
*Apr 6 13:32:54.470: TPLUS(00000054)/0/READ: socket event 1
*Apr 6 13:32:54.470: TPLUS(00000054)/0/READ: read entire 12 header bytes (expect 18 bytes data)
*Apr 6 13:32:54.470: TPLUS(00000054)/0/READ: socket event 1
*Apr 6 13:32:54.470: TPLUS(00000054)/0/READ: read entire 30 bytes response
*Apr 6 13:32:54.470: TPLUS(00000054)/0/2432818: Processing the reply packet
*Apr 6 13:32:54.470: TPLUS: Processed AV priv-lvl=15
*Apr 6 13:32:54.470: TPLUS: received authorization response for 84: PASS
*Apr 6 13:32:54.470: AAA/AUTHOR/EXEC(00000054): processing AV cmd=
*Apr 6 13:32:54.470: AAA/AUTHOR/EXEC(00000054): processing AV priv-lvl=15
*Apr 6 13:32:54.470: AAA/AUTHOR/EXEC(00000054): Authorization successful

كتر شتم حاتفم مادختساب TACACS م داخ نيوكت دن ع ، هج و مل انم عا طخ ا ح حصت جارخ ا ج ذومن اذه
ح حص ريغ اق بس م .

```
*Apr 6 13:35:07.826: AAA/BIND(00000055): Bind i/f
*Apr 6 13:35:07.826: AAA/AUTHEN/LOGIN (00000055): Pick method list 'default'
*Apr 6 13:35:07.826: TPLUS: Queuing AAA Authentication request 85 for processing
*Apr 6 13:35:07.826: TPLUS(00000055) log in timer started 1020 sec timeout
*Apr 6 13:35:07.826: TPLUS: processing authentication start request id 85
*Apr 6 13:35:07.826: TPLUS: Authentication start packet created for 85()
*Apr 6 13:35:07.826: TPLUS: Using server 10.106.60.182
*Apr 6 13:35:07.826: TPLUS(00000055)/0/NB_WAIT/225FE2DC: Started 5 sec timeout
*Apr 6 13:35:07.830: TPLUS(00000055)/0/NB_WAIT: socket event 2
*Apr 6 13:35:07.830: TPLUS(00000055)/0/NB_WAIT: wrote entire 38 bytes request
*Apr 6 13:35:07.830: TPLUS(00000055)/0/READ: socket event 1
*Apr 6 13:35:07.830: TPLUS(00000055)/0/READ: Would block while reading
*Apr 6 13:35:07.886: TPLUS(00000055)/0/READ: socket event 1
*Apr 6 13:35:07.886: TPLUS(00000055)/0/READ: read entire 12 header bytes (expect 6 bytes data)
*Apr 6 13:35:07.886: TPLUS(00000055)/0/READ: socket event 1
*Apr 6 13:35:07.886: TPLUS(00000055)/0/READ: read entire 18 bytes response
*Apr 6 13:35:07.886: TPLUS(00000055)/0/225FE2DC: Processing the reply packet
*Apr 6 13:35:07.886: TPLUS: received bad AUTHEN packet: length = 6, expected 43974
*Apr 6 13:35:07.886: TPLUS: Invalid AUTHEN packet (check keys).
```

ةلص تاذا تامول عم

- [Cisco IOS رل ع TACACS نيوكت](#)
- [Cisco Systems - تادنت سمل او ينق تلالا مع دللا](#)

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسمل اذ ه Cisco ت مچرت
ملاعلاء ن أ عي مچ ي ف ن ي م دخت سمل ل معد ي و تح م مي دقت ل ة ي رش ب ل و
امك ة ق ي قد ن و ك ت ن ل ة ي ل أ ة مچرت ل ض ف أ ن أ ة ظ حال م ي ج ر ي . ة ص ا خ ل م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا ع م ل ا ح ل ا و ه
ي ل ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco
Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص أ ل ا ي ز ي ل ج ن ا ل ا دن تسمل ا