Ritardo prima della visualizzazione della richiesta della password durante l'accesso tramite SSH/Telnet

Sommario

Introduzione

Questo documento descrive il ritardo prima che la richiesta della password venga visualizzata quando si accede tramite SSH/Telnet.

Questo problema si verifica in genere quando si cerca di accedere tramite SSH o Telnet all'interfaccia mgmt0 su un Nexus 5K/6K.

Dopo aver immesso l'ID utente, il testo viene visualizzato e si verifica un ritardo maggiore rispetto al previsto, prima che venga visualizzata la richiesta della password.

```
login as: admin
<delay for several seconds before below text is appears>
Nexus 5000 Switch
Using keyboard-interactive authentication.
Password:
```

Problema: Ritardo prima della visualizzazione della richiesta della password durante l'accesso tramite SSH/Telnet

Il problema si verifica a causa della ricerca DNS inversa.

Per impostazione predefinita, la ricerca del dominio ip è abilitata sul Nexus e, se un elenco di server DNS (nome-server ip) è configurato in Gestione VRF, lo switch eseguirà una ricerca DNS inversa dell'indirizzo IP di origine dell'utente ogni volta che si connette alla porta mgmt0 tramite SSH o Telnet.

Una ricerca DNS inversa ha lo scopo di verificare la legittimità dell'indirizzo IP di origine e di impedire lo spoofing IP.

Di seguito è riportato un esempio in cui è stato utilizzato un server DNS 10.67.84.45

Il server DNS in questo caso non dispone di una voce per l'indirizzo IP di origine del client e non

fornisce una risposta. In questo modo, lo switch Nexus esegue più query, in quanto il server non restituisce alcun risultato e questo causa un ritardo.

```
ip domain-lookup

vrf context management
  ip name-server 10.67.84.45
```

Da questo output di **show hosts**, è possibile verificare che è presente un server DNS configurato per la gestione VRF e che la ricerca del dominio IP è abilitata.

```
N5548P-2# show hosts
DNS lookup enabled

Name servers for vrf:management is  10.67.84.45

Host                    Address
```

Le clip di Ethanalzyer sono state acquisite dopo l'immissione del nome utente e l'attesa della richiesta della password.

Mostra che lo switch Nexus esegue due ricerche DNS inverse sull'indirizzo IP di origine dell'utente, 62.84.137.10

SSH all'interfaccia N5K mgmt0

```
Username: admin
<delay for several seconds>

N5548P-2# ethanalyzer local interface mgmt display-filter dns
Capturing on eth0
2015-05-09 22:11:44.105674  10.67.84.56 -> 10.67.84.45      DNS Standard query PTR 6
2.84.137.10.in-addr.arpa
2015-05-09 22:11:49.102673  10.67.84.56 -> 10.67.84.45      DNS Standard query PTR 6
2.84.137.10.in-addr.arpa

N5548P-2# 2 packets captured
The password prompt is then displayed for the user
Nexus 5000 Switch
Using keyboard-interactive authentication.
Password
:
```

Analogamente, quando si accede tramite Telnet, lo switch esegue prima la ricerca DNS inversa indicata in precedenza sull'indirizzo IP di origine dell'utente e quindi visualizza il prompt di accesso.

Telnet su interfaccia N5K mgmt0

```
telnet to switch 10.67.84.56
N5548P-2# ethanalyzer local interface mgmt display-filter dns
Capturing on eth0
2015-05-09 22:24:56.303878  10.67.84.56 -> 10.67.84.45      DNS Standard query PTR 6
2.84.137.10.in-addr.arpa
```

```
2015-05-09 22:25:01.302680  10.67.84.56 -> 10.67.84.45      DNS Standard query PTR 6
2.84.137.10.in-addr.arpa
2 packets captured
```

Viene quindi visualizzato il prompt di accesso:

```
Nexus 5000 Switch
login: admin
Password:
```

Soluzione

Soluzione 1. Modificare l'elenco dei server DNS configurati in Nexus in modo che il server DNS che risponde venga consultato prima del server DNS che non risponde.

Se Nexus riceve un record DNS valido dal server DNS locale, non consulterà il secondo server DNS dell'elenco. Ciò riduce il ritardo.

Esempio:

```
vrf context management
no ip name-server 10.67.84.45
ip name-server  10.67.84.48 10.67.84.45
```

Èpossibile utilizzare questi comandi per verificare l'elenco corrente dei server DNS in cui il server locale è incluso per primo nell'elenco:

```
N5548P-2# sh hosts
DNS lookup enabled

Name servers for vrf:management is  10.67.84.48 10.67.84.45

Host                    Address
```

Da queste acquisizioni di Ethanalyzer, viene eseguita prima la ricerca del nome IP e viene ricevuta una risposta.

Seguito da una ricerca da nome a indirizzo IP in cui viene ricevuta una risposta.

In questo caso, non si è osservato alcun ritardo notevole nell'accesso tramite SSH o Telnet.

```
N5548P-2# ethanalyzer local interface mgmt display-filter dns
Capturing on eth0
2015-05-09 22:55:46.037079  10.67.84.56 -> 10.67.84.48 DNS Standard query PTR
 20.196.104.64.in-addr.arpa
2015-05-09 22:55:46.037444 10.67.84.48 -> 10.67.84.56  DNS Standard query res
ponse PTR no-sense-1.cisco.com
2015-05-09 22:55:46.041907  10.67.84.56 -> 10.67.84.48 DNS Standard query A n
o-sense-1.cisco.com
2015-05-09 22:55:46.042295 10.67.84.48 -> 10.67.84.56  DNS Standard query res
ponse A 64.104.196.20
```

Soluzione 2. Rimuovere l'elenco DNS dal VRF di gestione.

Esempio:

gestione contesto vrf

```
no ip name-server 10.67.84.48 10.67.84.45
```

- Disabilita ricerca dominio IP

```
no ip domain-lookup
```

> **Nota:** Richiesta di miglioramento aperta per disabilitare la ricerca DNS inversa per SSH/Telnet.

CSCur27501 Disabilita la ricerca r-DNS per SSH/Telnet