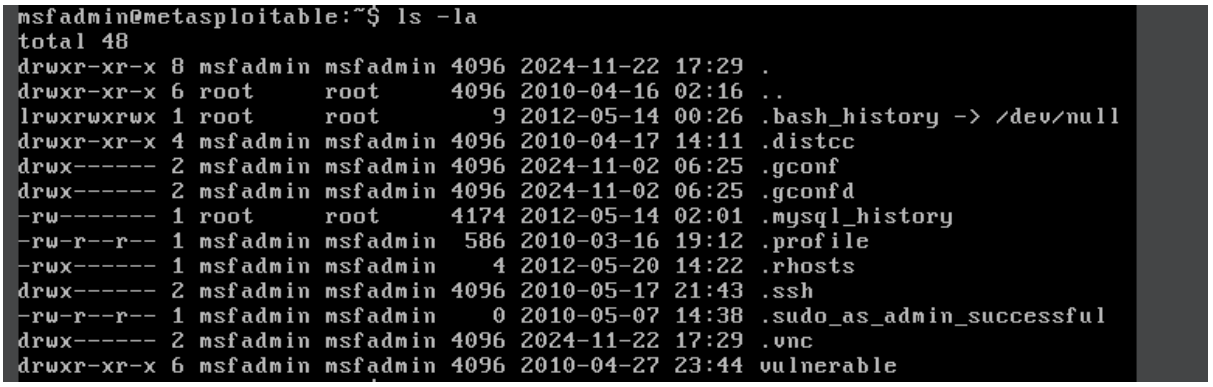
Remediation in Meta

Table of content

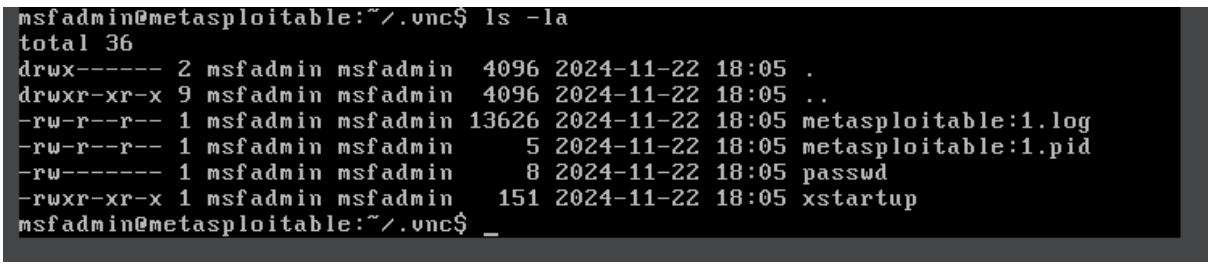
Risoluzione vulnerabilità 61708 - VNC Server 'password' Password

La vulnerabilità riscontrata risiede nella password per attivare il software VNC che consente di condividere il desktop di Meta attraverso una rete. La password impostata è “passoword”, avendo quindi una password semplicissima e per nulla sicura l'obiettivo è quello di renderla più complessa per impedire accessi indesiderati.

Il primo passo fatto è stato usare il comando **ls -la** per vedere tutti i file e cartelle anche quelli nascosti con i relativi permessi. Come si può notare dalla figura sotto, la cartella di interesse è quella nella penultima riga che ha i permessi di scrittura, lettura ed esecuzione solo per l’utente.



Mi sono quindi spostato all’interno della cartella e con il comando **ls -la** ho visualizzato i permessi di scrittura del file psswd che contiene la password di VNC Server, notando che il file ha i permessi di lettura e scrittura per l’utente, ma non l’esecuzione.

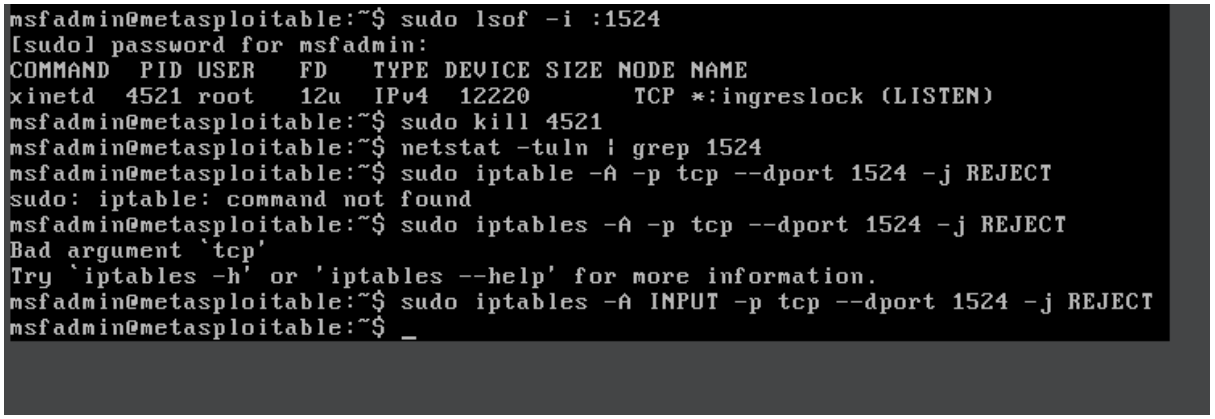


Dopo vari tentativi nel modificare il file psswd ed aggiornare i server ho utilizzato il comando **sudo su.** Ho ottenuto i permessi di root ed ho eseguito il file con il comando **vncpasswd .** Ho impostato quindi una password più complessa, usando una combinazione di maiuscole, caratteri speciali e numeri, nello specifico quella scelta è stata: P@55w0rd.

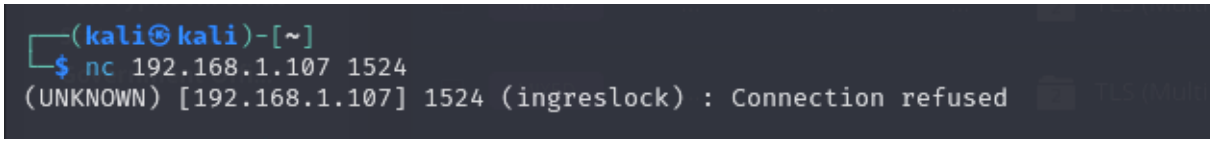
Risoluzione vulnerabilità 51988 - Bind Shell Backdoor Detection

Questa vulnerabilità presenta una shell che sta ascoltando sulla porta 1524 senza richiedere alcuna autenticazione. Un attaccante potrebbe sfruttarla collegandosi alla porta remota e controllare il sistema.

Ho usato il comando **sudo lsof -i :1524** per individuare il PID del processo in esecuzione sulla porta. Ho terminato il processo ed aggiunto una regola firewall per proteggere la porta con il comando **sudo iptables -A INPUT -p tcp --dport 1524 -j REJECT.**



Ho poi testato la regola provando a connettermi alla porta da Kali con il comando **nc 192.168.1.107 1524.**

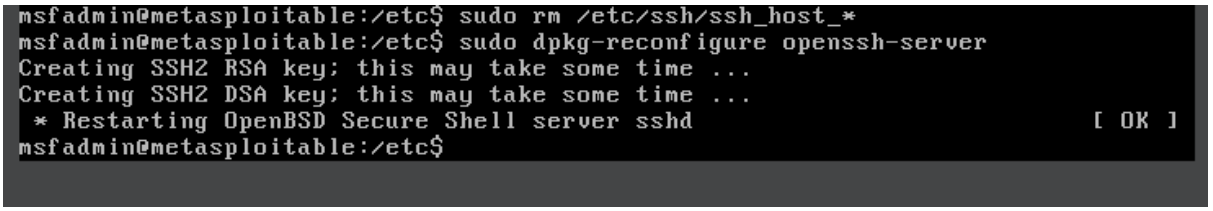


Risoluzione vulnerabilità 32314 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

Questa vulnerabilità riguardava le chiavi host SSH remote che Nessus ha rivelato come deboli.

Per risolverla è bastato cancellare il file SSH con le chiavi deboli tramite il comando **sudo rm /etc/ssh/ssh_host_***.

Poi ho rigenerato nuove chiavi SSH con il comando **sudo dpkg-reconfigure openssh-server**.

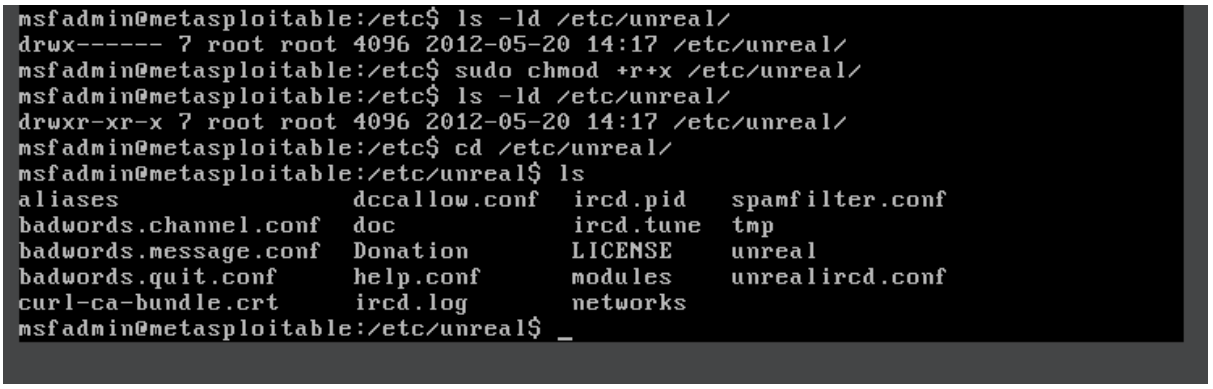


Ed infine ho riavviato il servizio SSH.

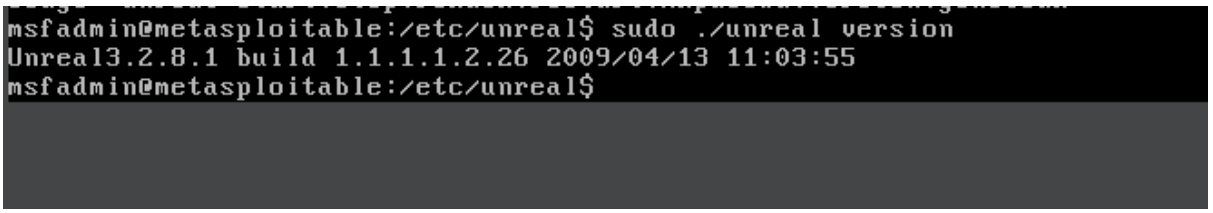
Risoluzione vulnerabilità 46882 - UnrealIRCd Backdoor Detection

La vulnerabilità riguarda una versione compromessa di UnrealIRCd distribuita con una backdoor nota. Questa backdoor consente a un attaccante di eseguire codice arbitrario sull'host interessato. La soluzione proposta da Nessus per risolvere il problema, è quella di rimuovere la versione compromessa e installarne una pulita.

Per prima cosa mi sono posizionato nella cartella unreal, inizialmente non riuscivo ad accedervi, con il comando **ls -ld /etc/unreal** ho verificato i permessi della cartella e li ho modificati e successivamente ho verificato il contenuto della cartella.



Con in comando **sudo ./unreal version** ho identificato la versione



La versione 3.2.8.1 installata è proprio quella affetta della presenza di una backdoor com’è spiegato nei link forniti dal report di Nessus.

Scaricata la versione più recente ho usato questo comando **tar -xzvf unrealircd-latest.tar.gz** per estrarre il file compresso.

```
msfadmin@metasploitable:~$ ls
unrealircd-6.1.9.1  unrealircd-latest.tar.gz  vulnerable
msfadmin@metasploitable:~$ cd unrealircd-6.1.9.1/
msfadmin@metasploitable:~/unrealircd-6.1.9.1$
```

Dopo vari tentativi l'ultima versione di UnrealIRCd non é supportata su Meta e le versioni precedenti alla 6.1.9.1 non sono più rilasciate per il download sul sito di UnrealIRCd.

```
/tmp/cc0YZK4C.s: Assembler messages:
/tmp/cc0YZK4C.s:149: Error: no such instruction: `xgetbv'
make[1]: *** [src/libpcre2_8_la-pcre2_jit_compile.lo] Error 1
make[1]: Leaving directory `/home/msfadmin/unrealircd-6.1.9.1/extras/pcre2-10.44
'
make: *** [all] Error 2
msfadmin@metasploitable:~/unrealircd-6.1.9.1$
```

UnrealIRCd 4 EOL

Since 2021, UnrealIRCd 4 is **no longer supported**. It is no longer receiving any bug fixes, including **no security fixes** anymore.

Still using UnrealIRCd 4?

If you are still using UnrealIRCd 4.x then you should upgrade ASAP to UnrealIRCd 6. The configuration file requires no mandatory changes, so in most cases upgrad

If you are using third party modules, then check on modules.unrealircd.org if they have been ported to. Otherwise, you can post the module source on the modules

Releases

The currently supported UnrealIRCd versions (and EOL dates) can be seen in the table below:

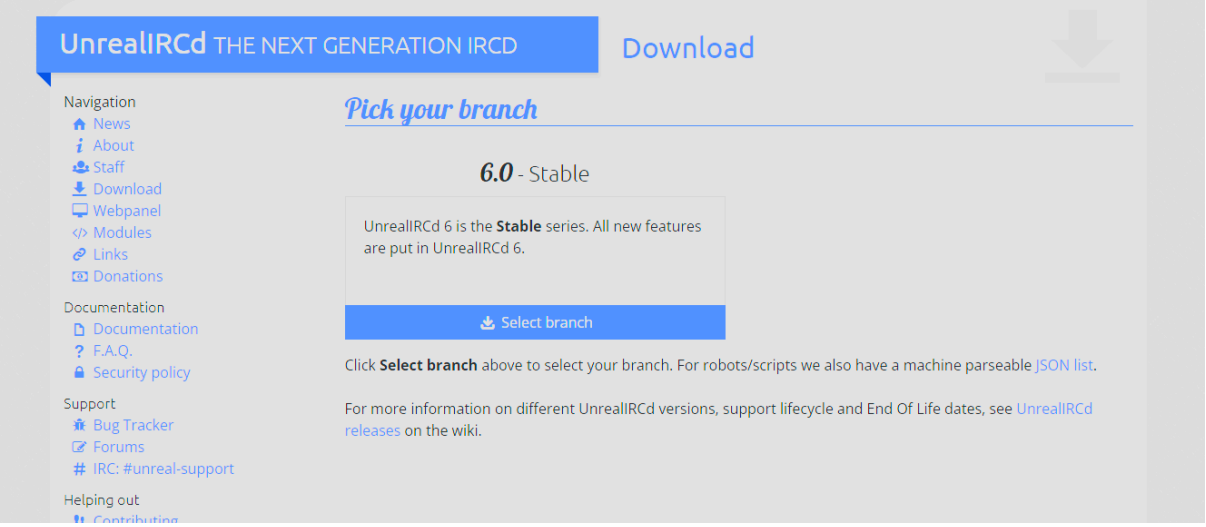
Series	First stable release	Security fixes only	End of life (EOL)	Duration	Comment
UnrealIRCd 3.2	2004-04-25	2015-12-11	2016-12-31	12.5 years	Very old, unsupported, do not use
UnrealIRCd 4	2015-12-24	2019-05-20	2020-12-31	5 years	Old, unsupported, do not use
UnrealIRCd 5	2019-12-13	2022-07-01	2023-07-01	3.5 years	No longer supported
UnrealIRCd 6	2021-12-17	-	-	-	Stable

There is no strict release cadence of the major versions.

When a new major version is released we will announce the exact end dates of the previous major release. The previous major release is always supported for **at le**

See also:

- History of UnrealIRCd releases - a historic overview from 1999 until now



Quindi per rimuovere la vulnerabilità critica l'unica possibilità è stata quella di rimuovere totalmente il server da Meta. In un ipotetico scenario si dovrebbe valutare la necessità di un server IRC, nel caso sia necessario l'utilizzo di un server di questo tipo per la comunicazione sarà necessario valutare un servizio simile, ma sicuro.