Criticità Risolte Metasploitable2

1)NFS Exported Share Information Disclosure

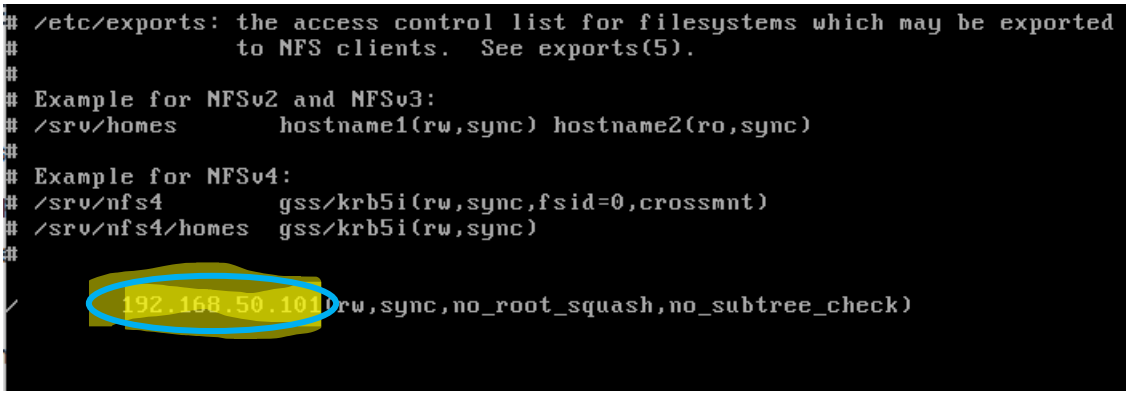
Tutte le macchine possedevano i privilegi per modificare gli share remoti di NFS

Tramite il comando sudo su, vengono concessi i permessi di amministratore del server, questo ci servirà per tutte le operazioni di remediation;

Utilizzando il comando apt-get install nfs-kernel-server così da installare nel caso non ci fosse già il pacchetto di NFS server per avere un sistema che permetta agli altri host di montare e accedere alle condivisioni presenti sul tuo sistema.

Di seguito con il comando in foto, modifichiamo quelle impostazioni:

A seguito dell'invio del comando l'interfaccia si presenta così, con al posto dell'indirizzo cerchiato un asterisco che indica che le modifiche sono effettuabili da ogni dispositivo sulla rete, in questo modo abbiamo vincolato la modifica delle impostazioni NFS a quel singolo indirizzo.



Salvando il file la modifica è effettiva ed il problema viene risolto correttamente.

2)VNC server password ‘password’

Nessus si loggava tranquillamente al servizio VNC utilizzando la password ‘password’;

Per risolvere il problema è bastato cambiare la password al servizio VNC:

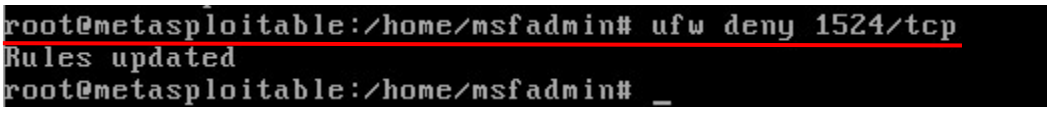
Scrivendo sudo su per i permessi e di seguito, vncpasswd come in figura accediamo al comando per la modifica della password del servizio, verrà richiesta la nuova password e poi una conferma;

Una volta terminato le nuove credenziali si salveranno automaticamente e il problema verrà risolto.

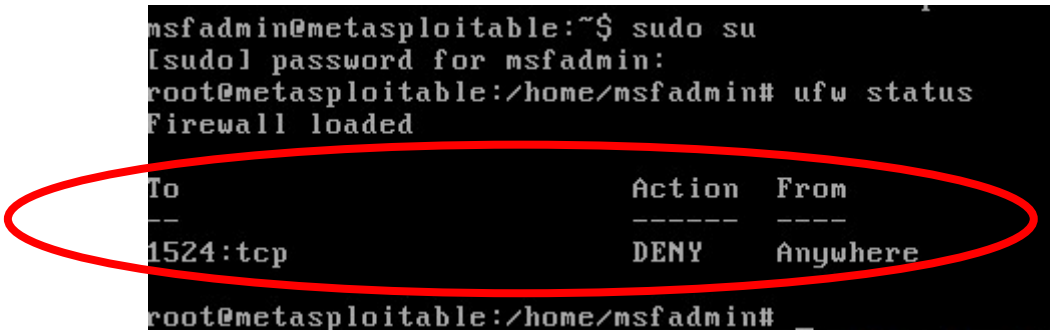
3)Bind-shell backdoor detection

Per la remediation di questa vulnerabilità ho optato per l’utilizzo di una regola di firewall, (inizialmente con iptables ma non funzionava molto bene) perciò ho utilizzato UFW “uncomplicated firewall” un firewall già presente su Metasploitable.

Con i permessi di root e il comando mostrato in figura ho filtrato con il firewall la porta che Nessus mi aveva segnalato bloccandone il traffico Tcp in entrata.



Poi con il comando ufw status ho controllato che la regola si fosse salvata nel firewall;

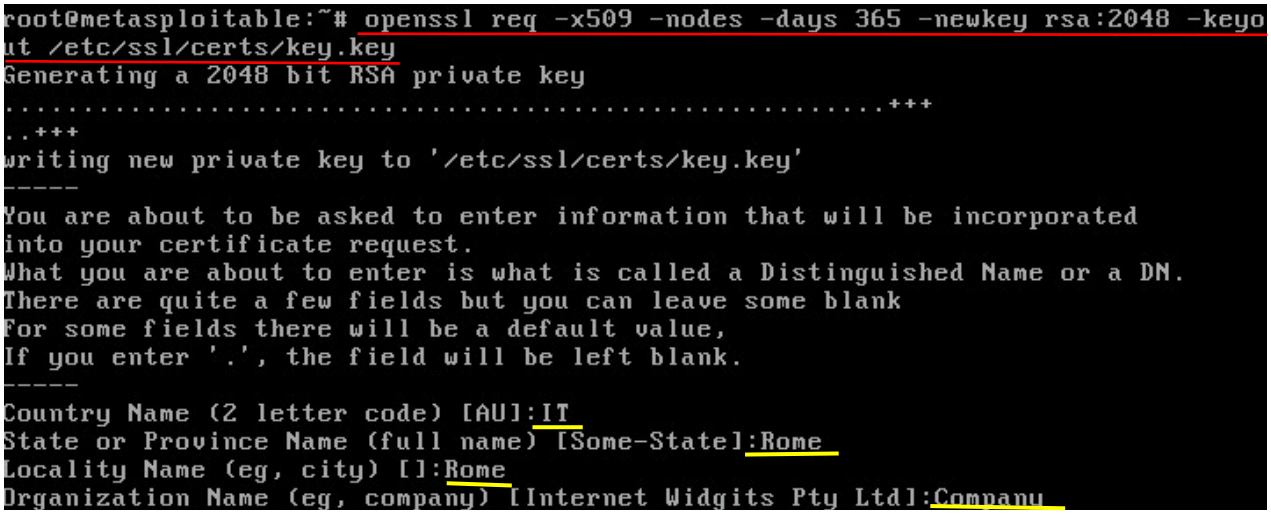


Una volta che la regola viene visualizzata sulla lista del firewall allora è stata salvata e la vulnerabilità è risolta.

4)SSL version 2 and 3 Protocol Detection

Per quanto riguarda il problema dei certificati SSL, per prima cosa ho cancellato tutti i file di ssh_host;

Successivamente, con il comando sottolineato nella figura sottostante, ho riconfigurato la chiave di cifratura per il certificato SSL



Oltre ai dati sottolineati, il codice mi ha chiesto anche un nome da associare alla chiave e una mail;

```
MIIESzCCAzOgAwIBAgIJAPUs08TdxHrYMA0GCSqGSIb3DQEBBQUAMHYxCzAJBgNV
BAYTAklUMQ0wCwYDVQQIEwRSb211MQ0wCwYDVQQHEwRSb211MRAwDgYDVQQKEwdD
b21wYW55MQswCQYDVQQLEwJCMTENMAsGA1UEAxMETHVjYTEbMBkGCSqGSIb3DQEJ
ARYMR0dHQGxpdmUuY29tMB4XDTIzMDYwNDA5NDc1MloXDTI0MDYwMzA5NDc1Mlow
djELMAkGA1UEBhMCSVQxDTALBgNVBAgTBFJvbWUxDTALBgNVBAcTBFJvbWUxEDAO
BgNVBAoTB0NvbXBhbnkxCzAJBgNVBAsTAklxMQ0wCwYDVQQDEwRMdWNhMRswGQYJ
KoZIhvcNAQkBFgxHR0dAbGl2ZS5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAw
ggEKAoIBAQD3L1dfTWNvGrLWxuxw5A4t8OAOy2GnqOHuoLJNWsSxObRMtWcv7Ssa
eorGlTuyGScyAGCLRnlvfvSUkPoYcGWJEtU2lmjMaOJIK1uZpT0X2RRDaXhzb6kC
NVLd/S1F7jArMBh7oVvetLHms5SaQwCBBPD/Ks9M80RRtXaKBOG7lh8fcK1DWsi5
aj1P2M6YWAYQOhViy5qQlqrt/LHLGxPmL+Qq9FrlbTOuZUWUIxN7jgZBKND9U9Ve
RUd3vYFewe9SdgwBVrg5DS8ekVzeLPwbYshn5G1+yzXn923BJYs9syTc98sUxiFW
AeDhwfty99PrTlOUI3yeY00H6cVDr0eJAgMBAAGjgdswgdgwHQYDVR0OBBYEFKRA
ZDc8/mKnD/nVTo3T7QSsTYnmMIGoBgNVHSMEgaAwgZ2AFKRAZDc8/mKnD/nVTo3T
7QSsTYnmoXqkeDB2MQswCQYDVQQGEwJJVDENMAsGA1UECBMEUm9tZTENMAsGA1UE
BxMEUm9tZTEQMA4GA1UEChMHQ29tcGFueTELMAkGA1UECxMCQjExDTALBgNVBAMT
BEx1YzExGzAZBgkqhkiG9w0BCQEWDEdHR0BsaXZlLmNvbYIJAPUs08TdxHrYMAwG
A1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEFBQADggEBAFwVQjYj8HYfl+tV5QKwgtSc
JXJbSgNx7WkoN9S8C5x6XWBni0jomMd6jYWfar9d9n9FlhLoLEFT8Aif4QvDMC5G
y2sNtFKz0RzOIB98o1AgQD6UdKD5zetL1O19x9fPfFoUqJoStuX5F2AnPHS+i+SI
eKOnP0OCgUzzygydUKSIzigWLdZvvfLoAgkoVbd3ZWasIO0C/IcY/2ZoXUZAnBcd
5SzRa7kXumrxDKWgSPaUWCt1LyNUFpXCHhP+5TUm0yO2bVauA4Skl j8QBe7FPhcS
X1XOc8Xy7SfJEDerU4UDGANcLN8R7wXRF0INR8XGhztfS5qQkjnmM4SvPkN9yjw=
-----END CERTIFICATE-----
root@metasploitable:~#
```

Una volta inseriti tutti i dati richiesti ed inviato il codice, il terminale di metasploitable genera un certificato che viene salvato nel file e nel percorso scelto precedentemente.

L'ultimo passo da fare perché il procedimento venga reso effettivo è riavviare il server SSL con il nuovo certificato.

```
root@metasploitable:/home/msfadmin# sudo dpkg-reconfigure openssh-server
 * Restarting OpenBSD Secure Shell server sshd                          [ OK
root@metasploitable:/home/msfadmin#
```

Con questo procedimento ho risolto solo uno dei problemi di SSL.

5)Apache Tomcat AJP Injection

Per l'utilizzo ulteriore del firewall ho bloccato il protocollo tcp dalla porta 8009 che era quella collegata al servizio di apache, anche se il problema della vulnerabilità non viene risolto ho notato che in questo modo è possibile mascherare a nessus il problema, quindi per risolvere in qualche modo il problema di dover mantenere certe applicazioni in versioni più vecchie.

```
To                         Action  From
--                         ------  ----
1524:tcp                   DENY    Anywhere
8009:tcp                   DENY    Anywhere

root@metasploitable:/home/msfadmin#
```

Conclusioni:

Attraverso le regole di firewall ho potuto notare che è possibile bloccare e filtrare diversi servizi come la lettura delle versioni di alcuni sistemi come apache tomcat, o anche la visione di una backdoor presente nel sistema, anche se non una delle soluzioni più efficienti.

Alcuni problemi erano invece solo risolvibili tramite l'aggiornamento del sistema a una versione supportata, e quindi che risolvesse la maggior parte dei difetti.

Ad ogni modo con alcuni degli accorgimenti adottati per dare maggiore sicurezza al nostro server hanno funzionato, ed hanno anche risolto più di una vulnerabilità per ogni singolo difetto del sistema.