

# Report Progetto settimanale UNIT 2 WEEK 5

## Remediation

### Impostazioni VM

Nel Progetto abbiamo tre VM impostate:

**Kali** 192.168.32.100 (rete interna)

**Metasploitable** 192.168.50.101 (rete interna)

**pfSense** configurato con 3 schede di rete

WAN DHCP (NAT)

LAN1 192.168.32.105 (rete interna)

LAN2 192.168.50.105 (rete interna)

Kali e Metasploitable sono in comunicazione tra loro tramite pfSense anche con reti diverse, con rispettivi gateway 192.168.32.105 per Kali e 192.168.50.105 per Metasploitable.

Controllo la connessione tra le macchine con il comando ping e accedo a pfSense dal browser di Kali (<https://192.168.32.105>), abilitando tutto il traffico in entrata per poter eseguire il test senza nessun ostacolo dal firewall.

Da terminale Kali lancio Nessus con il comando

**/bin/systemctl start nessusd.service**

Successivamente dal browser faccio l'accesso a Nessus tramite

<https://kali:8834>

Avvio una nuova scan con "New Scan" e configuro una "Basic Network Scan":

Imposto il nome della scansione e la descrizione, come target scelgo l'IP di Metasploitable.

Il tipo di scan sarà su tutte le porte comuni ed il resto dei valori in default.

**Dalla precedente scansione con nmap ho potuto notare come più porte fossero aperte, per cui cercherò i file di configurazione collegandomi direttamente alla porta telnet da Kali usando find e confrontando con Metasploitable se la destinazione è quella corretta.**

### Remedy Actions

11356 - NFS Exported Share Information Disclosure

42256 - NFS Shares World Readable

10437 - NFS Share Export List

È POSSIBILE ACCEDERE ALLE CONDIVISIONI NFS SULL'HOST REMOTO.

IL SERVER NFS REMOTO ESPORTA CONDIVISIONI LEGGIBILI DA TUTTI.

IL SERVER NFS REMOTO ESPORTA UN ELENCO DI CONDIVISIONI.

La soluzione è andare a modificare il file di configurazione sull'host remoto.

In questo caso il file di configurazione è nel path **/etc/exports**

```

GNU nano 2.0.7      File: /etc/exports
# /etc/exports: the access control list for filesystems which may be exported
#                 to NFS clients.  See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes      hostname1(rw,sync) hostname2(ro,sync)
#
# Example for NFSv4:
# /srv/nfs4       gss/krb5i(rw,sync,fsid=0,crossmnt)
# /srv/nfs4/homes gss/krb5i(rw,sync)
#
/*(noaccess,root_squash,no_subtree_check)

```

Modifico con nano l'ultima stringa in modo tale che nessuno abbia accesso e conseguentemente non possa sfruttare la vulnerabilità per risalire a root. Questo può essere modificato successivamente nel caso si voglia utilizzare il servizio per un particolare indirizzo, network, gruppo, ecc.

[61708 - VNC Server 'password' Password](#)

[19288 - VNC Server Security Type Detection](#)

[65792 - VNC Server Unencrypted Communication Detection](#)

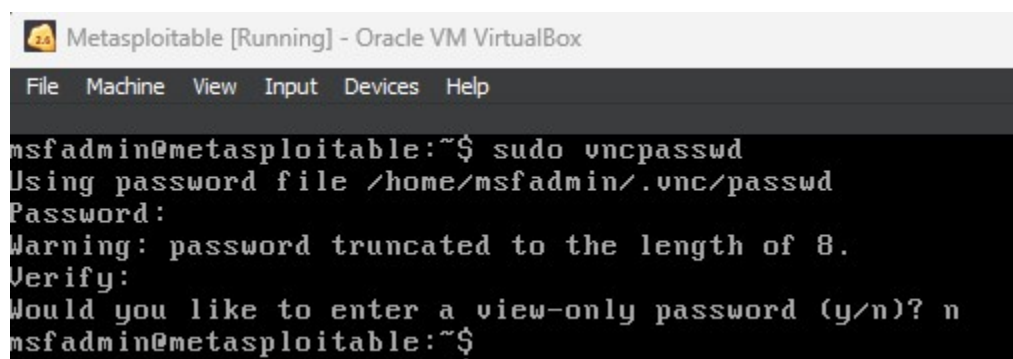
[10342 - VNC Software Detection](#)

UN SERVER VNC IN ESECUZIONE SULL'HOST REMOTO È PROTETTO DA UNA PASSWORD DEBOLE.

UN SERVER VNC È IN ESECUZIONE SULL'HOST REMOTO.

UN SERVER VNC CON UNO O PIÙ "TIPI DI SICUREZZA" NON CRITTOGRAFATI È IN ESECUZIONE SULL'HOST REMOTO. L'HOST REMOTO ESEGUE UN SOFTWARE DI VISUALIZZAZIONE REMOTA (VNC).

Il file di configurazione password è criptato ed è nel path /home/msfadmin/.vnc/passwd  
Cambio la password per l'utente msfadmin.



```

Metasploitable [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
msfadmin@metasploitable:~$ sudo vncpasswd
Using password file /home/msfadmin/.vnc/passwd
Password:
Warning: password truncated to the length of 8.
Verify:
Would you like to enter a view-only password (y/n)? n
msfadmin@metasploitable:~$

```

In seguito, cancello la password per il root, in modo che soltanto quella di msfadmin sia valida, non avendo modo di cambiare la password root (criptata).

```
Metasploitable [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
msfadmin@metasploitable:~$ cd /root && ls -la
.          .config      .gconf       .profile     .ssh
..         Desktop   .gconfd      .purple      .vnc
.bash_history .filezilla  .gstreamer-0.10 reset_logs.sh vnc.log
.bashrc     .fluxbox    .mozilla     .rhosts      .Xauthority
msfadmin@metasploitable:/root$ sudo su
[sudo] password for msfadmin:
root@metasploitable:~# cd .vnc && ls -la
metasploitable:0.log  metasploitable:1.log  passwd
metasploitable:0.pid  metasploitable:2.log  xstartup
root@metasploitable:~/vnc# rm passwd
root@metasploitable:~/vnc# _
```

## 10203 - rexecd Service Detection

## 51988 - Bind Shell Backdoor Detection

IL SERVIZIO REXECD È IN ESECUZIONE SULL'HOST REMOTO.

L'HOST REMOTO POTREBBE ESSERE STATO COMPROMESSO.

Come suggerisce Nessus, si deve modificare il file di configurazioni per impedire che possa essere abusato, in quanto non fornisce alcun buon mezzo di comunicazione.

Il file è nel path [/etc/inetd.conf](#)

Inoltre, Nessus ha identificato la backdoor nella porta 1524 che si riferisce al Remote Shell (RSH) che è associato al protocollo "rsh" o "rlogin".

In questo caso decido di disabilitare sia il servizio shell sia quello exec.

```
GNU nano 2.0.7      File: /etc/inetd.conf
#<off># netbios-ssn    stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.telnetd
telnet               stream  tcp     nowait  telnetd /usr/sbin/tcpd  /usr/sbin/in.telnetd
#<off># ftp            stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.tftpd
tftp                 dgram   udp     wait    nobody   /usr/sbin/tcpd  /usr/sbin/in.tftpd
#<off># shell          stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rlogind
login                stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rlogind
#<off># exec           stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rlogind
ingreslock stream tcp nowait root /bin/bash bash -i
```

Dovremmo disabilitare altri servizi come Telnet e TFTP che usano connessioni non criptate e sono potenziali punti per accesso non autorizzato.

In seguito, vado a identificare dove è stata messa la backdoor, non potendo usare altri metodi.

```
root@metasploitable: ~
File Actions Edit View Help
root@metasploitable:~# netstat -tuln | grep 1524
tcp        0      0 0.0.0.0:1524        0.0.0.0:*          LISTEN
root@metasploitable:~# lsof -i:1524
COMMAND PID USER  FD  TYPE DEVICE SIZE NODE NAME
xinetd  4441 root   10u  IPv4 11959      TCP *:ingreslock (LISTEN)
```

Con netstat controllo i servizi in ascolto sulla porta 1524 e identificato il PID eseguo ps aux.

```
root@metasploitable: /home/msfadmin

File Actions Edit View Help
postfix 4422 0.0 0.0 5460 1680 ? S 02:36 0:00 qmgr -l -t fifo -u
root 4423 0.0 0.0 5388 1148 ? Ss 02:36 0:00 /usr/sbin/nmbd -D
root 4425 0.0 0.0 7724 1364 ? Ss 02:36 0:00 /usr/sbin/smbd -D
root 4429 0.0 0.0 7724 812 ? S 02:36 0:00 /usr/sbin/smbd -D
root 4441 0.0 0.0 2424 868 ? Ss 02:36 0:00 /usr/sbin/xinetd -pidfile /var/run/xinetd.pid
daemon 4480 0.0 0.0 2316 528 ? SN 02:36 0:00 distccd --daemon --user daemon --allow 0.0.0.0
daemon 4481 0.0 0.0 2316 572 ? SN 02:37 0:00 distccd --daemon --user daemon --allow 0.0.0.0
proftpd 4483 0.0 0.0 9948 1596 ? Ss 02:37 0:00 proftpd: (accepting connections)
daemon 4497 0.0 0.0 1984 420 ? Ss 02:37 0:00 /usr/sbin/atd
root 4508 0.0 0.0 2104 892 ? Ss 02:37 0:00 /usr/sbin/cron
root 4536 0.0 0.0 2052 348 ? Ss 02:37 0:00 /usr/bin/jsvc -user tomcat55 -cp /usr/share/ja
root 4537 0.0 0.0 2052 476 ? S 02:37 0:00 /usr/bin/jsvc -user tomcat55 -cp /usr/share/ja
tomcat55 4539 1.3 2.0 31692 83448 ? S1 02:37 0:03 /usr/bin/jsvc -user tomcat55 -cp /usr/share/ja
```

Con nano esploro il file trovato.

```
Metasploitable [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
GNU nano 2.0.7 File: /usr/sbin/xinetd

*****^@^@^@t^Q^@^@^@^@^@D$+G
*****^@^@^@t^Q^@^@^@^@^@D$+,
*****^@^@^@t^Q^@^@^@^@^@D$+^Q
*****^@^@^@t^Q^@^@^@^@^@D$+^L*****^@^@^@t^Q^@^@^@^@^@D$+^L*****$
**E^H^@D$+t^@^@^@C **^TlIã^@D$yt^F^H1^@C^@^@^@^@^@^@^@^@^@U^@S^@D^E^H^@D$+
^K^T^@^@K^X^@D^K^@^@K^@^@P^@K^@D^K^H^@^@P^@K^L^@^@^@^@E^P^CP^K^@^@^@^@
^A^@^@^@i^@U^@H^@D$+T$^D^@' ****^O^@^@^@í^@&^@^@^@U^@^@X^@u^@u^@H^@l^@l^@L^@}^@e^@T$
****F^H^@L^@A^@^@^@^@L^@D$^Hhu^F^H^@D$^D^@v^F^H^@D$^P^@D$^B^@^@^@^@ ****F^H^@L^@A^@^@^@
^
X^@F^H^@t^C^@^@^@G^@^@^@^@^@^@^@L^@D$^H8u^F^H^@D$^D^@v^F^H^@D$^C^@^@^@^@K^@^@^@u^@f^@E^@
^@D$^D<^@^@^@^@D$^p^@E^H^@AT^@^@^@X^@F^H^@ \^@L^@D$^H^@u^F^H^@D$^D^@v^F^H^@D$^C^@^@^@^@
^@^@^@^@D$^D^@^@^@^@^@^@^@D^@D^@X^@D$^@E^@^@^@t^Y^@D$^D^@E^@D$^@K^@^@^@^@^@^@r^@?^@P^@F^@
^@^@^@^@D$
^@^@^@^@^@^@^@^@T^@F^H^@U^@D$^D
^@^@^@^@D$
^@^@^@^@ ^@^@^@P^@F^H^@ ****^@^@^@^@^@^@F^@HU^@ U^@u^@HS^@X^@L^@t^@^@H^@D1^@A90u ^@S^@D$
^@^@^@^@t^@^@^@l^@H^@^@Pl^@l^@gr^@^@^@&^@^@^@^@^@Uw^@F^H^@D$^H^@D$^D^@v^F^H^@^@L$^@q^@^@^@
^@A^@^@^@^@^@^@4$^@^@^@^@A^@^@^@^@f^@^@^@^@E^@D$^H^@^@H^@^@D$^D^@D^@^@^@^@^@D^@D$^@
t^@F^H^@^@E ^@D^@0^@F^H^@t^@&^@C^@H^@e$^@D$^H^@x^@F^H^@D$^D^@x^@F^H^@D$^G^@^@^@^@D$^L^@^@^@
T^@^@^@^@O^@, ^@B^@^@^@^@^@D^@^@^@l^@_l^@y, ^@B^@O^@H^@^@^@A^@X^@Q^@^@^@^@^@^@^@^@1^@^@%^@B^@^@
```

Posso notare che il file binario per il demone inetd è criptato, per cui posso pensare che sia questo il file compromesso, dal momento che di default non lo è.

Fermo il servizio e controllo che non sia eseguito.

```
root@metasploitable:/home/msfadmin# /etc/init.d/xinetd stop
* Stopping internet superserver xinetd
... done.
root@metasploitable:/home/msfadmin# ps aux | grep xinetd
root      4677  0.0  0.0   3004   756 pts/0    R+   03:34   0:00 grep xinetd
root@metasploitable:/home/msfadmin#
```

Decido di rimuoverlo senza sostituirlo, non avendo trovato nessun file consono.

```
Metasploitable [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@metasploitable:~# rm /usr/sbin/xinetd
root@metasploitable:~# reboot_
```

Successivamente chiudo la porta associata.

```
root@metasploitable: ~  
File Actions Edit View Help  
root@metasploitable:~# ufw delete allow 1524/tcp  
Rules updated  
root@metasploitable:~# reboot
```

Così facendo il servizio xinetd non è più in esecuzione, i servizi nel file [/etc/inetd.conf](#) possono essere eseguiti come demoni standalone ed essere configurati e lanciati individualmente. Per un utilizzo temporaneo possono essere eseguiti utilizzando il path nel file [/etc/inetd.conf](#)

Per un utilizzo permanente si può creare un init script in [/etc/init.d](#) per ogni servizio, mettere i permessi corretti per gli script per renderli eseguibili ed usare il comando update-rc.d per abilitarli, così che il sistema li faccia partire all'avvio.

### 90509 - Samba Badlock Vulnerability

### 25240 - Samba Server Detection

### 104887 - Samba Version

UN SERVER SMB IN ESECUZIONE SULL'HOST REMOTO È INTERESSATO DALLA VULNERABILITÀ BADLOCK.

UN SERVER SMB È IN ESECUZIONE SULL'HOST REMOTO.

È STATO POSSIBILE OTTENERE LA VERSIONE SAMBA DAL SISTEMA OPERATIVO REMOTO.

Non potendo aggiornare alla versione successiva, utilizzo pfSense per bloccare il traffico sulle porte affette da questa vulnerabilità.

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	✓ 0 / 19.79 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	✗ 0 / 0 B	IPv4 TCP	*	*	192.168.50.101	139 (NetBIOS-SSN)	*	none		blocco esterno 139	
<input type="checkbox"/>	✗ 0 / 0 B	IPv4 TCP	*	*	192.168.50.101	445 (MS DS)	*	none		blocco esterno 445	

### 134862 - Apache Tomcat AJP Connector Request Injection (Ghostcat)

### 21186 - AJP Connector Detection

### 18261 - Apache Banner Linux Distribution Disclosure

### 11213 - HTTP TRACE / TRACK Methods Allowed

C'È UN CONNETTORE AJP VULNERABILE IN ASCOLTO SULL'HOST REMOTO.

C'È UN CONNETTORE AJP IN ASCOLTO SULL'HOST REMOTO.

IL NOME DELLA DISTRIBUZIONE LINUX IN ESECUZIONE SULL'HOST REMOTO È STATO TROVATO NEL BANNER DEL SERVER WEB.

LE FUNZIONI DI DEBUG SONO ABILITATE SUL SERVER WEB REMOTO.

Dal momento che non posso fare aggiornamenti ho cercato di risolvere in maniera tale che il rischio diventi minore.

Il file di configurazione è nel path [/etc/tomcat5.5/server.xml](#)

Il tentativo precedente con "secretRequired="true" non è bastato per risolvere le vulnerabilità, per cui ho deciso di disattivare direttamente il connettore, commentandolo, per prevenirne l'accesso esterno.

```

GNU nano 2.0.7      File: /etc/tomcat5.5/server.xml

                                noCompressionUserAgents="gozilla, traviata"
                                compressableMimeType="text/html,text/xml"

-->

<!-- Define a SSL HTTP/1.1 Connector on port 8443 -->
<!--
<Connector port="8443" maxHttpHeaderSize="8192"
          maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
          enableLookups="false" disableUploadTimeout="true"
          acceptCount="100" scheme="https" secure="true"
          clientAuth="false" sslProtocol="TLS" />
-->

<!-- Define an AJP 1.3 Connector on port 8009 -->
<!--
<Connector port="8009"
          secretRequired="True" redirectPort="8443" protocol="AJP/1.3" />
-->

```

In seguito, vado a modificare il file [/etc/apache2/apache2.conf](#)

```

GNU nano 2.0.7      File: /etc/apache2/apache2.conf

#
ServerTokens Prod

#
# Optionally add a line containing the server version and virtual host
# name to server-generated pages (internal error documents, FTP directory
# listings, mod_status and mod_info output etc., but not CGI generated
# documents or custom error documents).
# Set to "Email" to also include a mailto: link to the ServerAdmin.
# Set to one of:  On | Off | Email
#
ServerSignature Off

```

Cambio i ServerTokens da Full a Prod(product only) e il ServerSignature da On a Off, in questo modo il banner del server Apache non mostrerà più le informazioni di distribuzione.

Successivamente, vado a disabilitare la funzione di trace per il debug.

```

GNU nano 2.0.7      File: /etc/apache2/sites-available/default

NameVirtualHost *
<VirtualHost *>
    ServerAdmin webmaster@localhost

    DocumentRoot /var/www/
    <Directory />
        Options FollowSymLinks
        AllowOverride None
    </Directory>
    <Directory /var/www/>
        Options Indexes FollowSymLinks MultiViews
        AllowOverride None
        Order allow,deny
        allow from all
    </Directory>

    TraceEnable off_

```

Tolgo i commenti per abilitare le pagine di errore, in modo tale che non vengano inavvertitamente mostrate informazioni sulla versione del server.

```
GNU nano 2.0.7      File: /etc/apache2/apache2.conf

    AllowOverride None
    Options IncludesNoExec
    AddOutputFilter Includes html
    AddHandler type-map var
    Order allow,deny
    Allow from all
    LanguagePriority en cs de es fr it nl sv pt-br ro
    ForceLanguagePriority Prefer Fallback
</Directory>

ErrorDocument 400 /error/HTTP_BAD_REQUEST.html.var
ErrorDocument 401 /error/HTTP_UNAUTHORIZED.html.var
ErrorDocument 403 /error/HTTP_FORBIDDEN.html.var
ErrorDocument 404 /error/HTTP_NOT_FOUND.html.var
ErrorDocument 405 /error/HTTP_METHOD_NOT_ALLOWED.html.var
ErrorDocument 408 /error/HTTP_REQUEST_TIME_OUT.html.var
ErrorDocument 410 /error/HTTP_GONE.html.var
ErrorDocument 411 /error/HTTP_LENGTH_REQUIRED.html.var
ErrorDocument 412 /error/HTTP_PRECONDITION_FAILED.html.var
ErrorDocument 413 /error/HTTP_REQUEST_ENTITY_TOO_LARGE.html.var
```

[90317 - SSH Weak Algorithms Supported](#)

[70658 - SSH Server CBC Mode Ciphers Enabled](#)

[71049 - SSH Weak MAC Algorithms Enabled](#)

[149334 - SSH Password Authentication Accepted](#)

IL SERVER SSH REMOTO È CONFIGURATO PER CONSENTIRE ALGORITMI DI CRITTOGRAFIA DEBOLI O NESSUN ALGORITMO.

IL SERVER SSH È CONFIGURATO PER UTILIZZARE CIPHER BLOCK CHAINING.

IL SERVER SSH REMOTO È CONFIGURATO PER CONSENTIRE GLI ALGORITMI MD5 E MAC A 96 BIT.

IL SERVER SSH SULL'HOST REMOTO ACCETTA L'AUTENTICAZIONE DELLA PASSWORD.

Il file di configurazione è nel path [/etc/ssh/sshd\\_config](#)



```
X11Forwarding yes
X11DisplayOffset 10
PrintMotd no
PrintLastLog yes
TCPKeepAlive yes
#UseLogin no

#MaxStartups 10:30:60
#Banner /etc/issue.net

# Allow client to pass locale environment variables
AcceptEnv LANG LC_*

Subsystem sftp /usr/lib/openssh/sftp-server

UsePAM yes

Ciphers aes128-ctr,aes192-ctr,aes256-ctr
MACs hmac-sha1
```

Dal file di configurazione cambio:

#### **ServerKeyBits 2048**

Aumento il numero di bits delle chiavi RSA da 768 a 2048.

#### **PermitRootLogin no**

Disabilito il root login via SSH, in quanto è raccomandato non usare root-user accounts.

#### **StrictModes yes**

Abilito StrictModes per aumentare la sicurezza (home, directories, file chiave).

#### **RSAAuthentication yes**

Abilito la chiave pubblica RSA.

#### **PubkeyAuthentication yes**

Abilito l'autenticazione per chiave pubblica generale.

#### **IgnoreRhosts yes**

Disabilito l'uso dei file .rhosts e .shosts per l'autenticazione.

#### **RhostsRSAAuthentication no**

Disabilito l'uso dei file .rhosts per l'autenticazione RSA.

#### **HostbasedAuthentication no**

Disabilito l'autenticazione basata sull'host che si basa sulle informazioni del client.

#### **PermitEmptyPasswords no**

Disabilito le password vuote.

#### **ChallengeResponseAuthentication no**

Disabilito i metodi challenge-response di autenticazione.

#### **PasswordAuthentication no**

Disabilito l'autenticazione usando passwords forzando l'autenticazione tramite chiavi pubbliche.

Poi aggiungo le chiavi per gli algoritmi di cifratura delle connessioni SSH.

La versione attuale è OpenSSH version 4.7p1, per cui non posso usare algoritmi più recenti come AES-GCM e HMAC-SHA2.



Il resto delle vulnerabilità importanti deriva da più fattori dipendenti tra loro.

Primo fattore da considerare è l'utilizzo della porta 25 SMTP e-mail non sicura.

Creo una regola che blocchi il traffico per la porta 25, che è affetta da molteplici vulnerabilità. Si dovrebbe impostare il client e-mail per usare il protocollo SMTPS (SMTP Secure) o STARTTLS (SMTP with Transport Layer Security) al suo posto.

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	✓ 1 / 1.60 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	✗ 0 / 0 B	IPv4 TCP	*	*	192.168.50.101	25 (SMTP)	*	none		blocco esterno 25	

Procedo allo stesso modo per la porta 22, creando una regola che blocchi il traffico. Se necessario si potrebbe modificare la regola per autorizzare soltanto chi la utilizza, dal momento che in parte è stata resa meno vulnerabile (ma non del tutto per via delle cifrature ormai obsolete).

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	✓ 0 / 99 KiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	✗ 0 / 0 B	IPv4 TCP	*	*	192.168.50.101	5432	*	none		blocco esterno postgresql	
<input type="checkbox"/>	✗ 0 / 144 B	IPv4 TCP	*	*	192.168.50.101	22 (SSH)	*	none		blocco esterno 22	

Per mettere al sicuro il database sulla porta 5432 ho deciso di applicare una regola che blocchi il traffico. Ovviamente è solo una misura temporanea, si consiglia l'uso di un proxy o middleware per gestire le comunicazioni tra le applicazioni ed il database su una macchina diversa che ospita un sistema operativo adeguato. In questo modo si può mantenere il database sulla porta di default senza utilizzare un DBMS (Database Management System) differente.

```
File Machine View Input Devices Help

// If your ISP provided one or more IP addresses for stable
// nameservers, you probably want to use them as forwarders.
// Uncomment the following block, and insert the addresses replacing
// the all-0's placeholder.

// forwarders {
//     0.0.0.0;
// };
interface-interval 1; //periodic search for new interfaces
auth-nxdomain no;     # conform to RFC1035

listen-on { any; };
listen-on-v6 { any; };

recursion yes;
max-ncache-ttl 3600;
};
```

Stesso ragionamento per la porta 53. Modificando il file nel path [/etc/bind/named.conf.options](#) ho mitigato alcune vulnerabilità del server DNS e ho ridotto l'impatto di potenziali attacchi DNS. Purtroppo, questo non è abbastanza per risolvere ogni vulnerabilità.

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	✓ 1 / 138 KiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	✗ 0 / 408 B	IPv4 TCP/UDP	*	*	192.168.50.101	53 (DNS)	*	none		blocco esterno 53	  

In questo caso ho deciso di bloccare il traffico con una regola firewall, temporaneamente. Se il rischio minore dopo le modifiche venisse accettato, questo non risolverebbe il problema della vulnerabilità ISC BIND. La scelta migliore sarebbe segmentare il network, in modo da isolare il server DNS da altri sistemi critici e posizionarlo in una parte separata del network. Questo aiuterebbe a contrastare potenziali attacchi e limiterebbe le problematiche ad altri servizi in caso fosse compromesso. Inoltre, la regola firewall potrebbe essere modificata per permettere soltanto traffico da fonti conosciute, come clienti autorizzati o altri server DNS dell'infrastruttura DNS.

pfSense può essere configurato in modo che agisca come DNS forwarder o resolver per la rete, in questo modo gestirebbe le richieste DNS dei clienti e comunicherebbe con server DNS esterni. Così facendo si aggiungerebbe un ulteriore livello di sicurezza e controllo sul traffico DNS. Inoltre si potrebbe crittografare il traffico tra il client ed il server DNS abilitando DNS su TLS (DoT) o DNS su HTTPS (DoH) per migliorare la sicurezza e la privacy delle comunicazioni rendendo più difficile intercettare o manipolare le query e le risposte DNS.

In ogni caso è da considerare l'implementazione di meccanismi per monitorare ed analizzare il traffico in modo da prevenire potenziali attacchi.

pfSense offre funzionalità IDS/IPS tramite pacchetti come Suricata o Snort.