REMEDIATION META

Apache PHP-CGI Remote Code Execution

Questa vulnerabilità consente l'esecuzione di codice arbitrario su server che utilizzano **PHP-CGI** in combinazione con **Apache**. È causata da una cattiva gestione degli argomenti di linea di comando (***query string***) da parte di PHP quando eseguito tramite **mod_cgi** o **mod_fastcgi**.

Un attaccante può sfruttare questa falla per eseguire comandi di sistema inviando richieste HTTP malformate al server web, ottenendo potenzialmente **accesso completo** al sistema.

L'attaccante può inviare richieste come:

http://vulnerable-server/index.php?-s

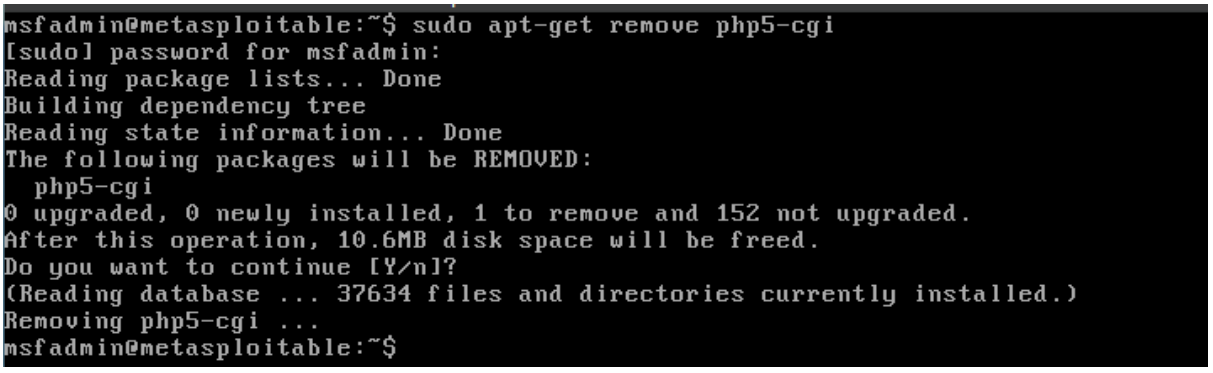
Questo comando forza PHP a mostrare il codice sorgente dei file ***.php*** o eseguire comandi arbitrari con l'utente di Apache (***www-data***).

L'attaccante può lanciare comandi shell (***ls, cat /etc/passwd, ecc.***), avendo accesso completo ai dati sensibili del server.

La soluzione consigliata è **rimuovere completamente *php-cgi***.

Comando per rimuovere *php-cgi* su Metasploitable:

sudo apt-get remove php5-cgi



Questa azione elimina l'interprete PHP-CGI, prevenendo così l'esposizione del server a questo tipo di attacco.

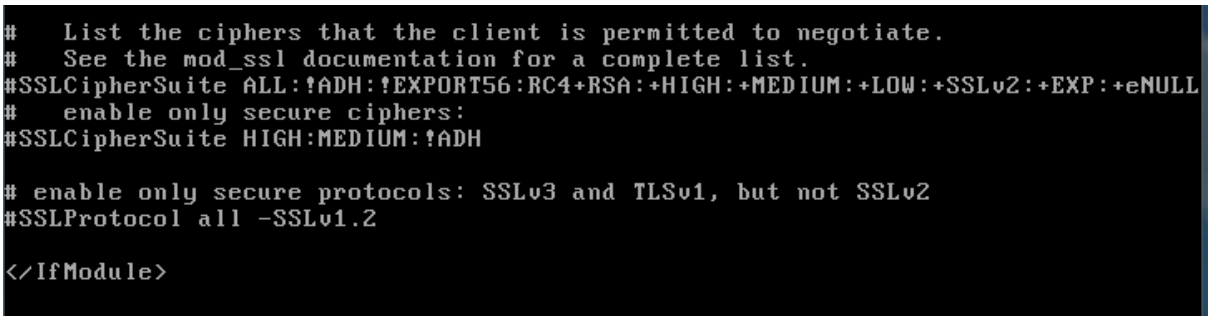
SSL Version 2 and 3 Protocol Detection

La vulnerabilità **SSL Version 2 and 3 Protocol Detection** significa che il server supporta ancora i protocolli **SSLv2** e **SSLv3**, entrambi considerati **obsoleti e insicuri**, soggetti a numerosi attacchi noti, come **POODLE** per **SSLv3**.

Per risolvere la vulnerabilità andiamo a modificare il file di configurazione SSL con:

sudo nano /etc/apache2/mods-available/ssl.conf

Modificando la direttiva “SSLProtocol” con “TLSv1.2” per essere più sicuri.

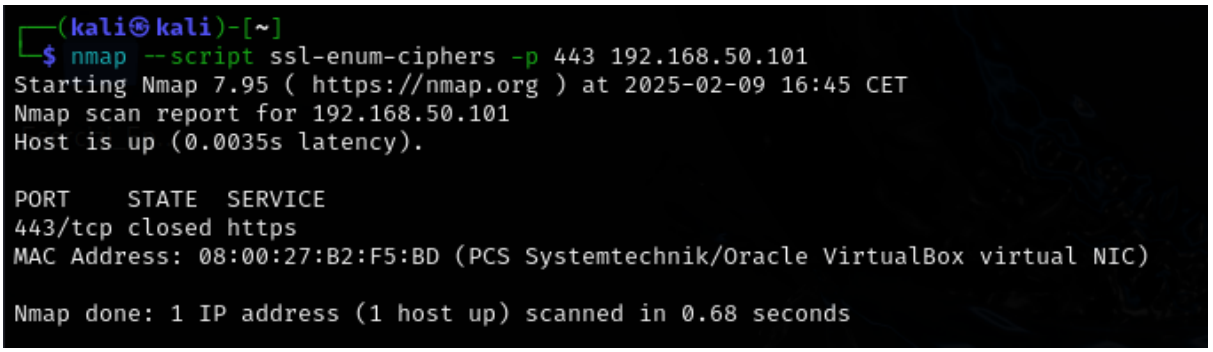


Salviamo il file, e riavviamo Apache con:

sudo service apache2 restart

Da Kali andiamo a controllare lo stato della porta 443 con:

nmap --script ssl-enum-ciphers -p 443 192.168.50.101



La porta 443 per i servizi HTTPS risulta chiusa, il che significa che Apache non è configurato per i servizi HTTPS.

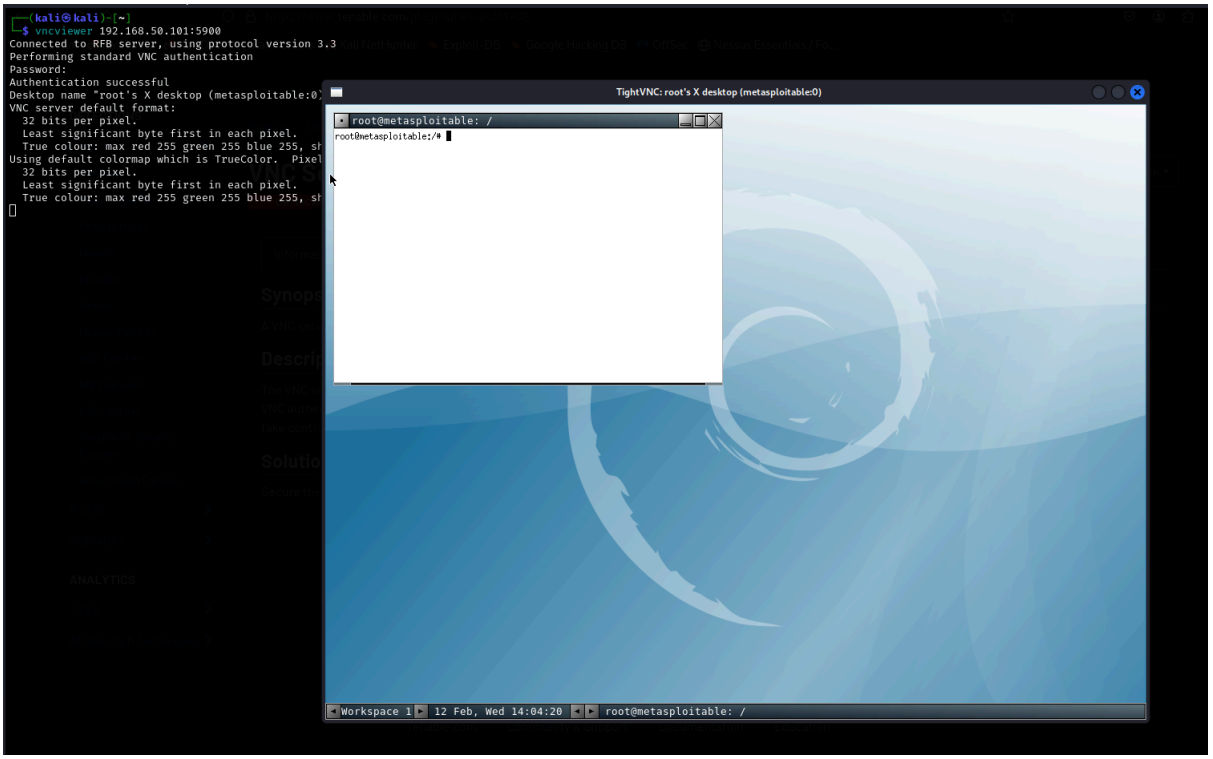
VNC Server 'password' Password

Questa vulnerabilità consente l'accesso remoto non autorizzato utilizzando una password di default estremamente debole, ovvero **“password”**. Il problema rappresenta un rischio elevato, poiché un attaccante potrebbe ottenere il controllo completo della sessione remota, con potenziali implicazioni sulla sicurezza del sistema target.

Testiamo la vulnerabilità, da Kali, connettiamoci al server VNC di Meta alla porta 5900, con il comando:

vncviewer 192.168.50.101:5900

Proviamo ad inserire la password “password” e riusciamo a loggare, quindi la vulnerabilità è presente.



Per risolvere la vulnerabilità basta cambiare la password di VNC (da Meta) con una meno “banale”.

Per farlo abbiamo prima di tutto bisogno di loggarci come root su Meta, dato che quando ci si connette al servizio tramite la porta 5900 viene automaticamente utilizzato l’utente root. Inseriamo quindi prima ***sudo su***, con relativa password di login per l’utente root poi:

vncpasswd

```
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
msfadmin@metasploitable:~$ sudo su
[sudo] password for msfadmin:
root@metasploitable:/home/msfadmin# vncpasswd
Using password file /root/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)? y
Password:
Verify:
root@metasploitable:/home/msfadmin#
```

Il terminale ci chiederà di inserire la nuova password (che non potrà essere più lunga di 8 caratteri) e poi di verificarla.

Proviamo infine a connetterci di nuovo da Kali, utilizzando la vecchia “password”

```
┌──(kali㉿kali)-[~]
└─$ vncviewer 192.168.50.101:5900
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Password:
Authentication failure
```

Possiamo a questo punto considerare la vulnerabilità come risolta.