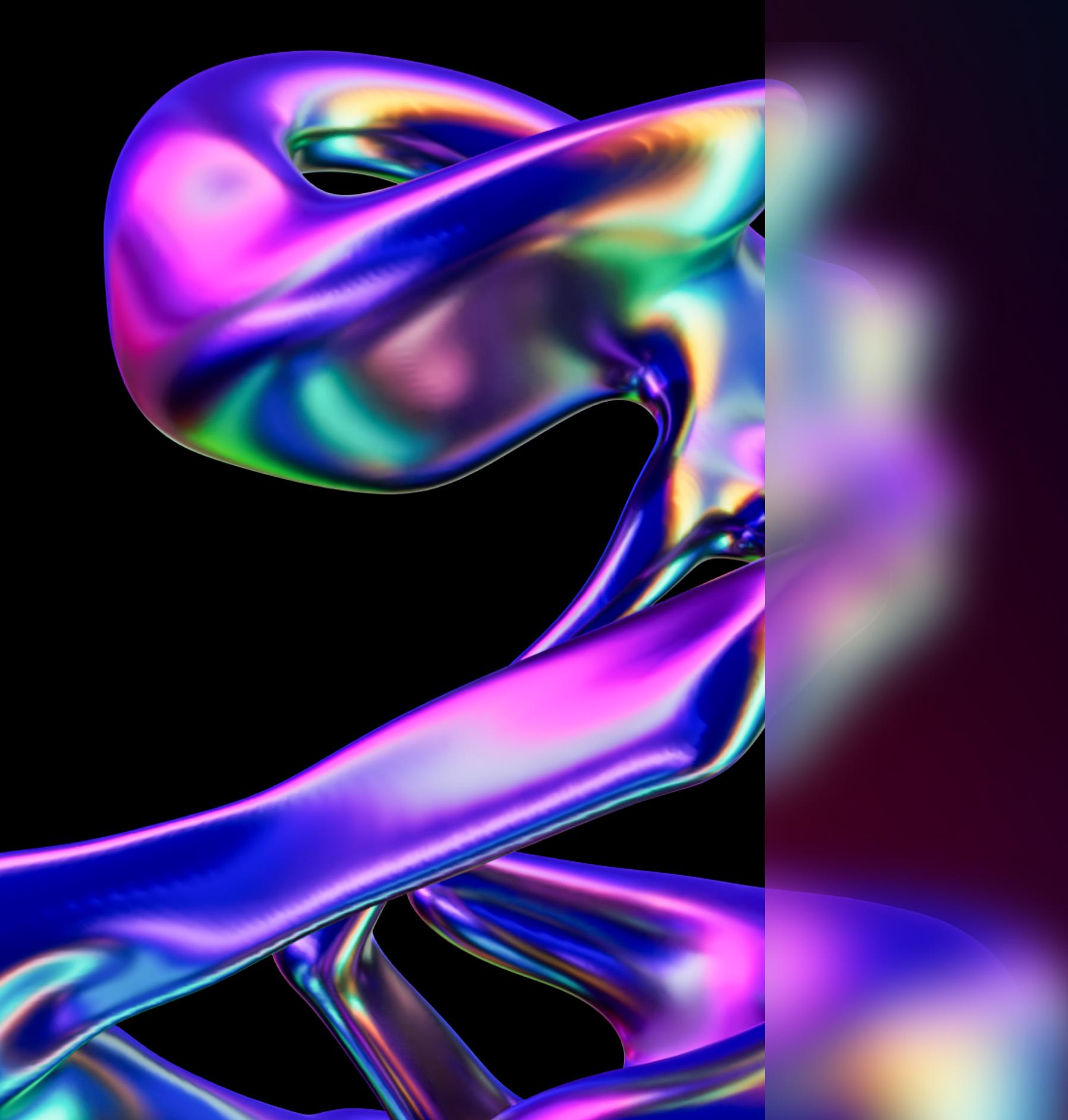




RICCARDO AGOSTINO MONTI

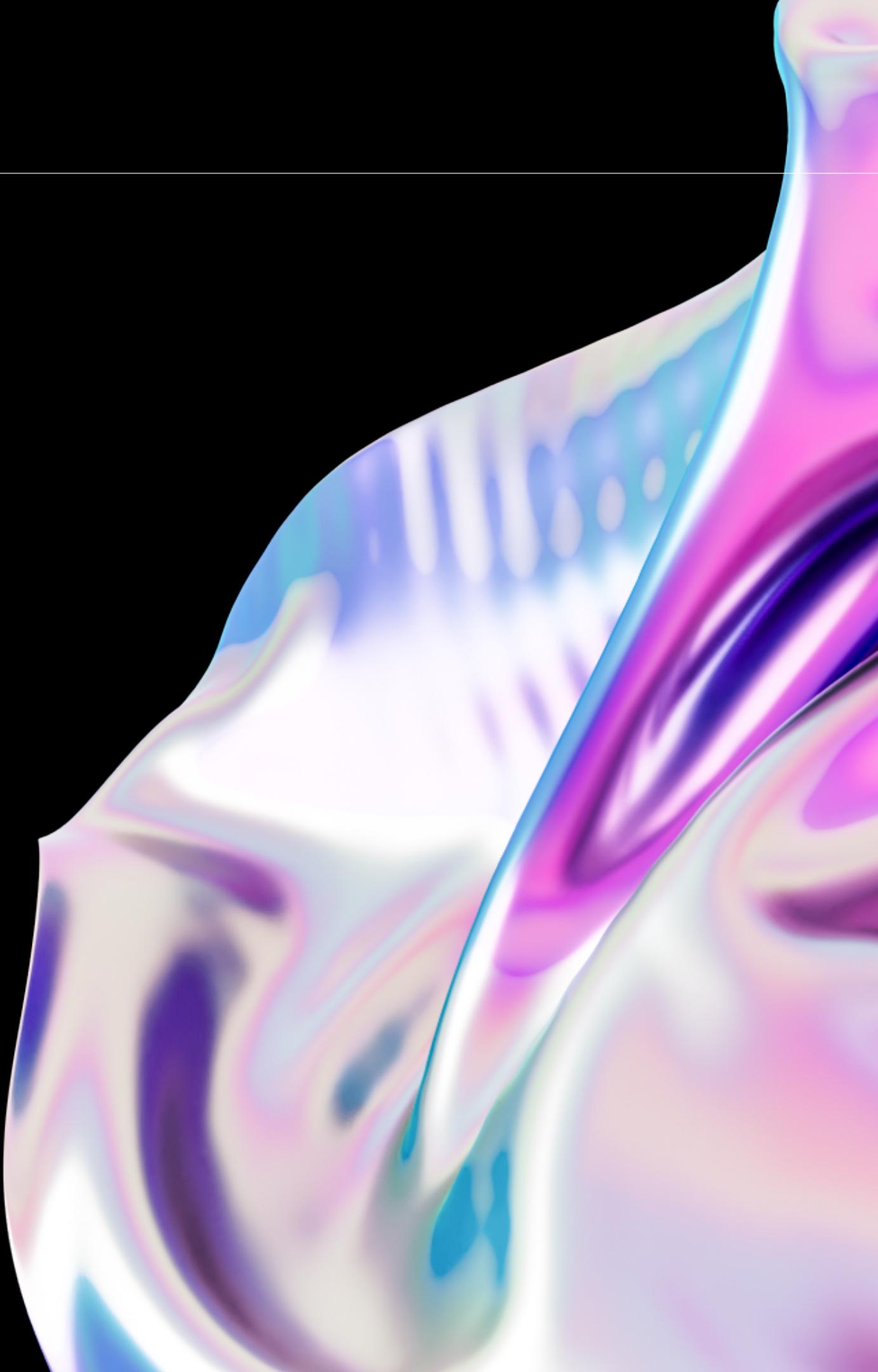


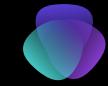
Consegna S5 Week-End CyberSecurity

Remediation Meta



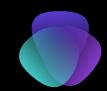
Il progetto di questa settimana ci chiedeva di effettuare azioni di Remediation su 4 vulnerabilità High-Critical che l'applicativo di Vulnerability Assessment chiamato "Nessus" trovava effettuando la scansione sul client MetaSploitable2





Le 4 vulnerabilità scelte sono:

- 1) 51988 - Bind Shell BackDoor Detection
- 2) 11356 - NFS Exported Share Information Disclosure
- 3) 61708 - VNC Server 'password' password
- 4) 90509 - Samba Badlock Vulnerability



51988 - Bind Shell BackDoor Detection

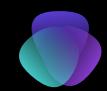
La prima vulnerabilità presa in considerazione è quella che Nessus numera come 51988.

Descrizione :

La Shell è in ascolto sulla porta remota senza chiedere prima alcune autenticazione. Un utente malintenzionato può accedere alla porta in remoto ed eseguire comandi.

Soluzione di Nessus:

Verificare se l'Host è stato manomesso da remoto e, se necessario, reinstalla il sistema.

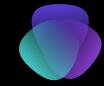


La mia soluzione:

Dopo aver verificato che l'Host non sia stato compromesso ho aggiunto una regola nel firewall che blocchi le connessioni alla porta che utilizza il servizio, visto che è inutilizzato. Nel caso in cui il servizio sia utilizzato è opportuno aggiungere un'autenticazione all'accesso remoto.

```
msfadmin@metasploitable:~$ sudo ufw enable  
Firewall started and enabled on system startup  
msfadmin@metasploitable:~$ sudo ufw deny 1524  
Rule added  
msfadmin@metasploitable:~$ sudo ufw status  
Firewall loaded
```

| To | Action | From |
|----------|--------|----------|
| -- | ----- | ----- |
| 1524:tcp | DENY | Anywhere |
| 1524:udp | DENY | Anywhere |



11356 - NFS Exported Share Information Disclosure

La seconda vulnerabilità presa in considerazione è quella che Nessus numera come 11356.

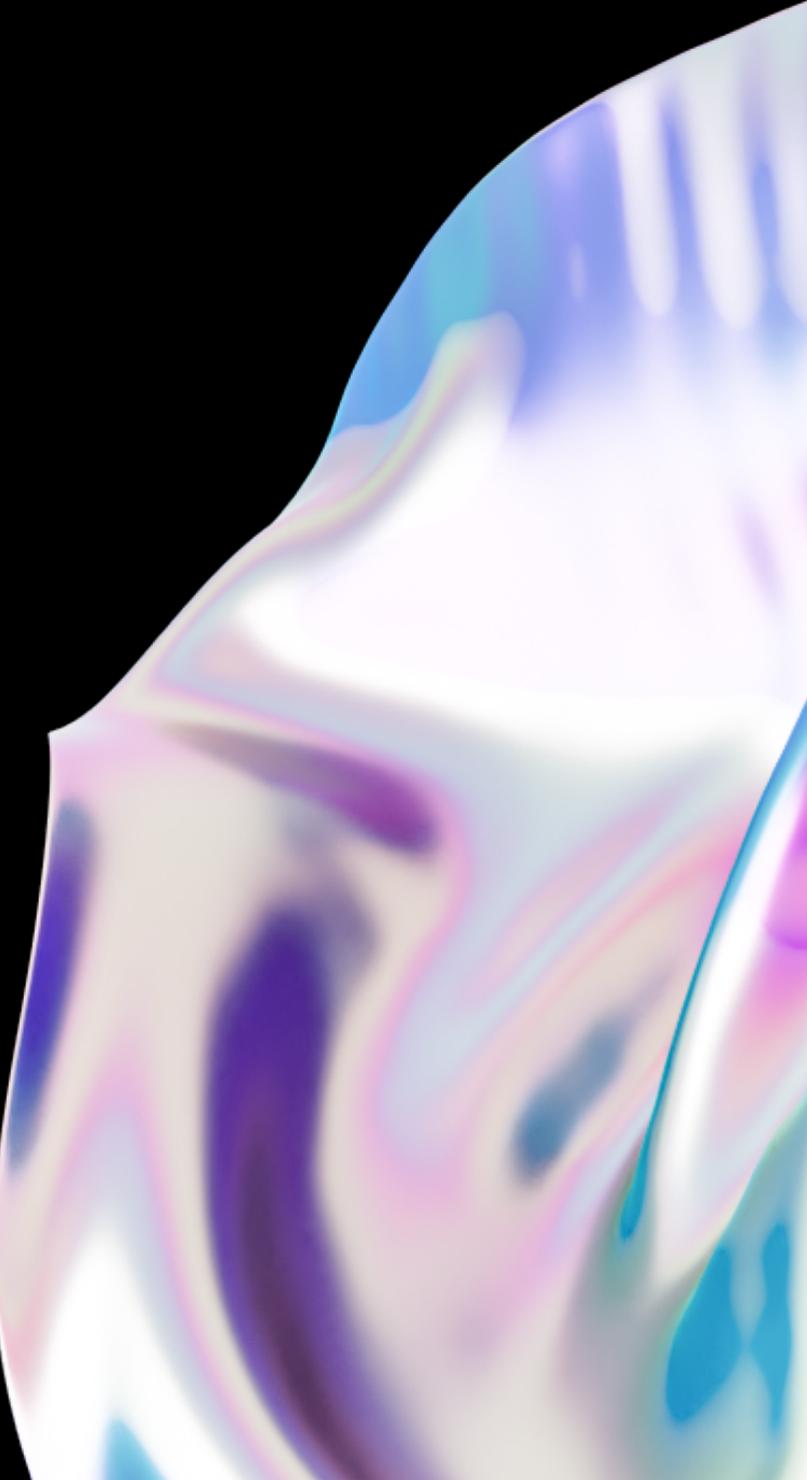
Descrizione :

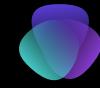
E' presente almeno una delle condivisioni NFS esportate dal server remoto che potrebbe essere montata dall'host che esegue la scansione.

Un attaccante potrebbe prenderne vantaggio per leggere (e potenzialmente scrivere) file sull'host remoto

Soluzione di Nessus:

Configurare NSF sul host remoto in modo che solo gli host autorizzati possano montare connessioni remote.



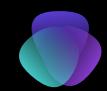


La mia soluzione:

Per risolvere questo problema ho modificato il file Exports presente nella cartella etc aggiungendo l'ip di metasploitable2 alla lista degli utenti autorizzati.

```
GNU nano 2.0.7          File: /etc/exports      Modified

# /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)
#
# 
# 192.168.50.101(rw,sync,no_root_squash,no_subtree_check)
```



61708 - VNC Server 'password' password

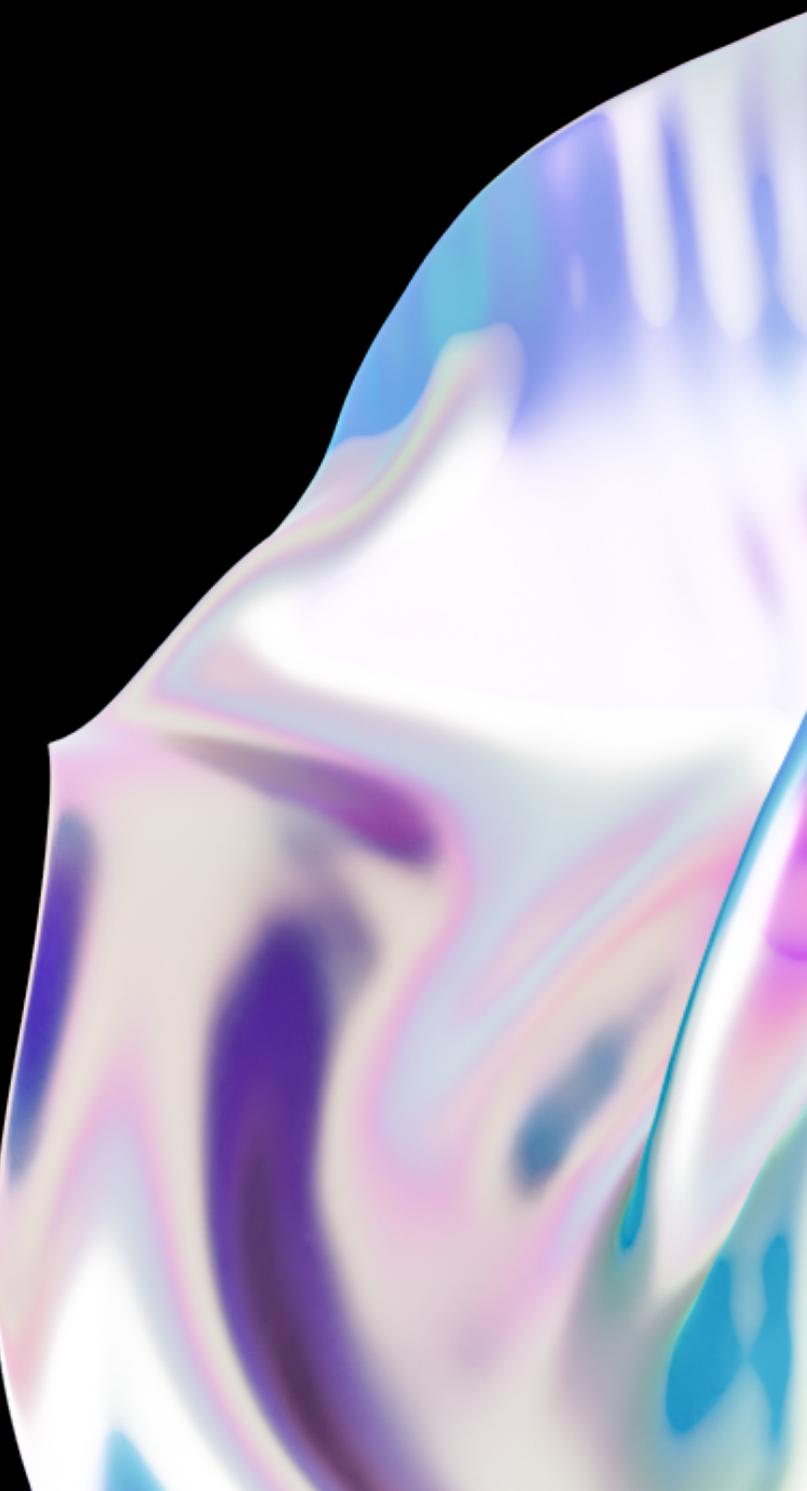
La terza vulnerabilità presa in considerazione è quella che Nessus numera come 61708.

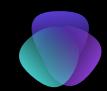
Descrizione :

Il server VNC in esecuzione sull'host remoto è protetto da una password debole. Nessus è stato in grado di effettuare il login utilizzando l'autenticazione una password di tipo "password". Un attaccante remoto non autenticato potrebbe sfruttare questo exploit per prendere il controllo del sistema.

Soluzione di Nessus:

Secure the VNC service with a strong password.





La mia soluzione:

Andiamo a cambiare la password in una più complessa, nel mio caso <<#94&2a>>.

```
root@metasploitable:~# vncpasswd
Using password file /root/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)? n
```



90509 - Samba Badlock Vulnerability

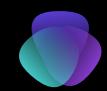
La quarta vulnerabilità presa in considerazione è quella che Nessus numera come 90509.

Descrizione :

La versione di Samba, in esecuzione sull'host remoto è affetta da un difetto, noto come Badlock, presente nel SAM e nella Local Security Authority LSA Domain Policy a causa di una negoziazione impropria del livello di autenticazione sui canali RPC. Un hacker man-in-the-middle in grado di intercettare il traffico tra un client e un server che ospita un database SAM può sfruttare questa falla per forzare un downgrade del livello di autenticazione, che consente l'esecuzione di chiamate di rete Samba arbitrarie nel contesto dell'utente intercettato, come visualizzare o modificare dati sensibili di sicurezza nel database di Active Directory o disabilitare servizi critici.

Soluzione di Nessus:

Aggiorna alla versione Samba 4.2.11 / 4.3.8 / 4.4.2 o successiva.



La mia soluzione:

Per risolvere questo problema possiamo mettere online la macchina di metasploitable e aggiornare Samba come suggerisce Nessus oppure disabilitare le porte che il servizio utilizza visto che anche in questo caso, il servizio è inutilizzato.

```
root@metasploitable:~# ufw deny 445  
Rule added  
root@metasploitable:~# ufw deny 139  
Rule added  
root@metasploitable:~# ufw status  
Firewall loaded
```

| To | Action | From |
|----------|--------|----------|
| -- | ----- | ----- |
| 1524:tcp | DENY | Anywhere |
| 1524:udp | DENY | Anywhere |
| 445:tcp | DENY | Anywhere |
| 445:udp | DENY | Anywhere |
| 139:tcp | DENY | Anywhere |
| 139:udp | DENY | Anywhere |