PROGETTO GIORNO 5

Per questo progetto abbiamo dovuto fare una scansione completa di Nessus sulla nostra macchina virtuale Metasploitable.

Da Nessus abbiamo scaricato il report completo delle vulnerabilità della nostra macchina, esportandone quelle critiche ed evidenziando quelle da risolvere.

Vulnerabilities Total: 134

SEVERITY	CVSS V3.0	PLUGIN	NAME
CRITICAL	9.8	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	51988	Bind Shell Backdoor Detection
CRITICAL	9.8	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	9.8	125855	phpMyAdmin prior to 4.8.6 SQLi vulnerablity (PMASA-2019-3)
CRITICAL	10.0	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0*	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0*	61708	VNC Server 'password' Password

Scegliere da 2 a 4 volnerabilità critiche sulla macchina Metasploitable2 per poi provare ad implementare delle azioni di rimedio.

Abbiamo evidenziato le vulnerabilità critiche da risolvere.

Per dimostrare l'efficacia delle azioni di rimedio eseguire nuovamente la scansione sul target e confrontare i risultati con quelli precedentemente ottenuti.

Remediation:

- **VNC Server Password**
  Sinossi:
  Un server VNC in esecuzione sull'host remoto è protetto con una password debole.
  Descrizione:

Il server VNC in esecuzione sull'host remoto è protetto con una password debole. Nessus è stato in grado di accedere utilizzando l'autenticazione VNC e una password di "password". Un utente malintenzionato remoto e non autenticato potrebbe sfruttarlo per assumere il controllo del sistema.
Soluzione:
Proteggi il servizio VNC con una password complessa.
Fattore di rischio:
Critico
Host:
192.168.32.101
Porta:
TCP/5900/VNC

Nessus ha effettuato l'accesso utilizzando una password di "password".

Andremo quindi a cambiare la password di VNC tramite i passaggi in figura:

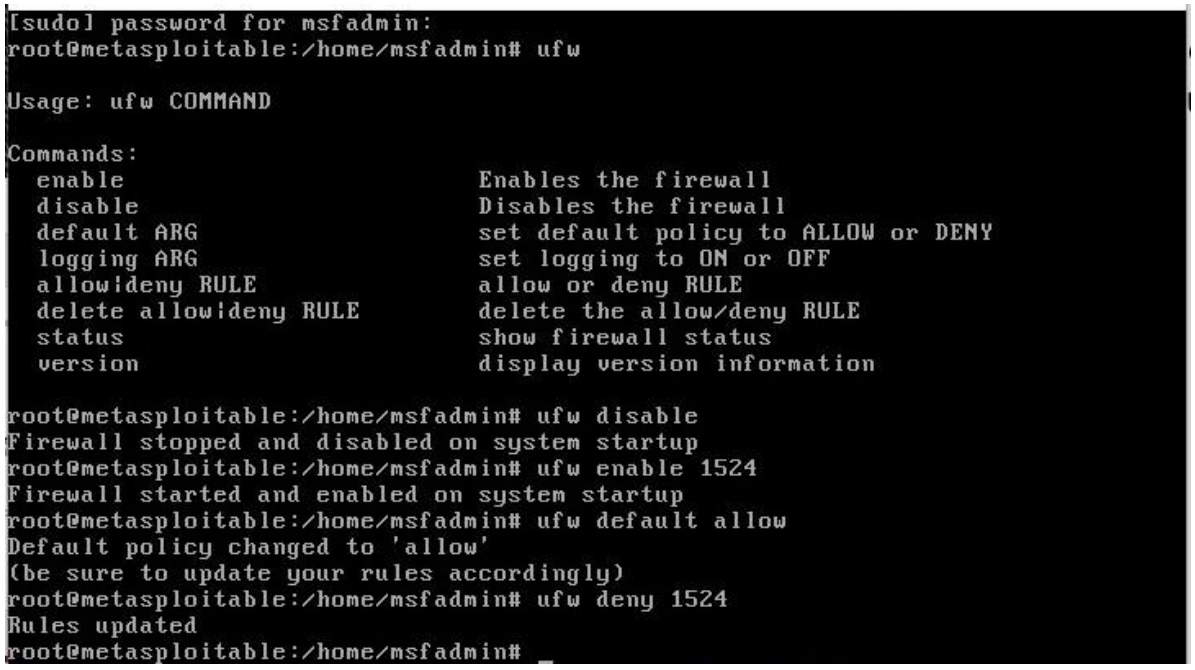
- **Rilevamento backdoor Bind Shell**
  Sinossi:
  L'host remoto potrebbe essere stato compromesso.
  Descrizione:
  Una shell è in ascolto sulla porta remota senza che sia richiesta alcuna autenticazione. Un utente malintenzionato può utilizzarlo connettendosi alla porta remota e inviando direttamente comandi.
  Soluzione:
  Verificare se l'host remoto è stato compromesso e, se necessario, reinstallare il sistema.
  Fattore di rischio:
  Critico
  Porta:
  TCP/1524/wild_shell

  Nessus è stato in grado di eseguire il comando "id" utilizzando la seguente richiesta:
  Ciò ha prodotto il seguente output troncato (limitato a 10 linee):

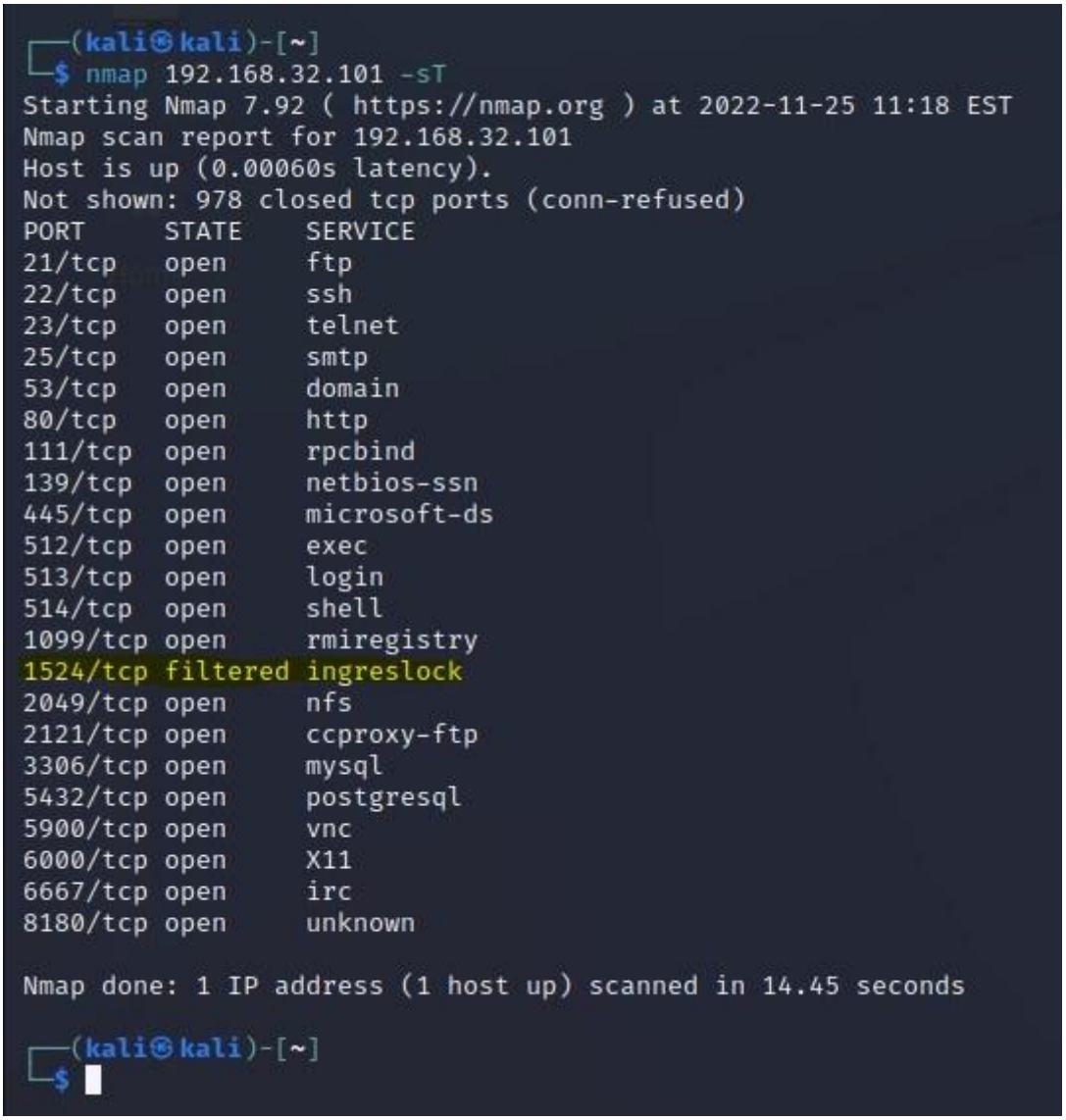
  root@metasploitable:/# uid=0(root) gid=0(root) groups=0(root)

root@metasploitable:/#

Andremo ad aggiungere un FireWall sulla porta 1524 tramite i comandi:

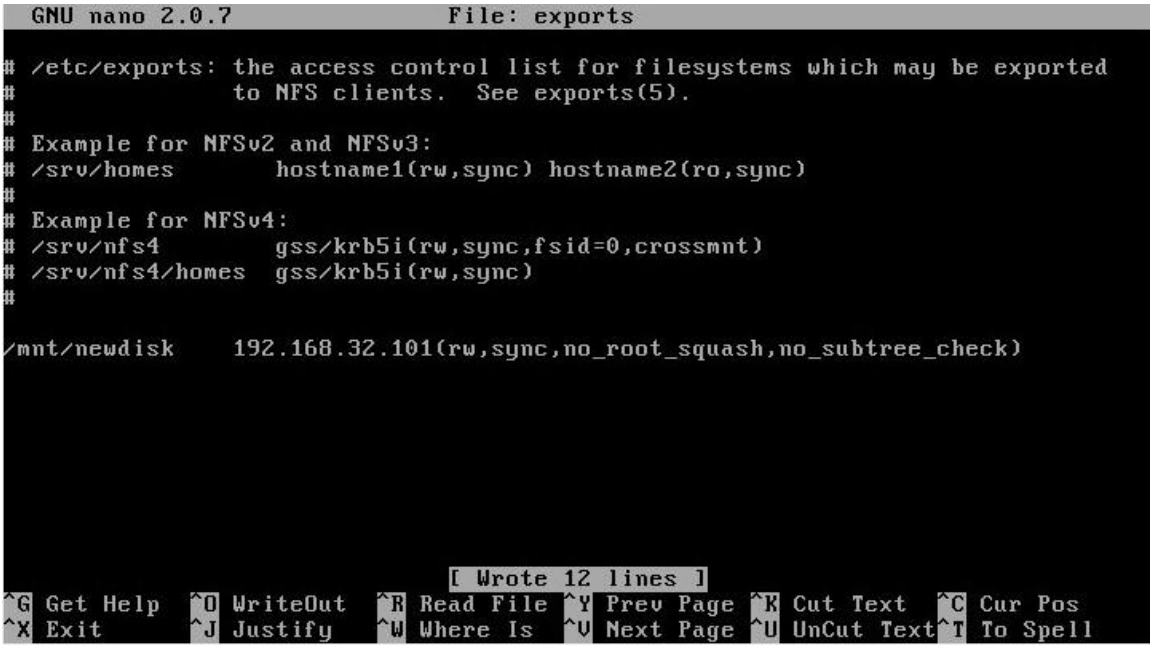


Per fare un controllo, andremo a lanciare una scansione con nmap sulla macchina Kali per confermare che la porta in questione, la 1524, risulterà filtrata.



- **Divulgazione di informazioni sulle azioni esportate NFS**
  Sinossi:
  È possibile accedere alle condivisioni NFS sull'host remoto.
  Descrizione:
  Almeno una delle condivisioni NFS esportate dal server remoto può essere montata dall'host di scansione. Un utente malintenzionato potrebbe essere in grado di sfruttare questo per leggere (ed eventualmente scrivere) file su host remoto.
  Soluzione:
  Configurare NFS sull'host remoto in modo che solo gli host autorizzati possano montare le proprie condivisioni remote.
  Fattore di rischio:
  Critico
  Porta:
  UDP/2049/RPC-NFS

  Andremo a risolvere tramite:



Riproveremo quindi una scansione con Nessus sulla macchina Metasploitable2:

192.168.32.101

6	7	25	6	84
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 128

SEVERITY	CVSS V3.0	PLUGIN	NAME
CRITICAL	9.8	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	9.8	125855	phpMyAdmin prior to 4.8.6 SQLi vulnerablity (PMASA-2019-3)
CRITICAL	10.0	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)

Com’è possibile vedere dalla nuova scansione di Nessus le vulnerabilità critiche evidenziate sono state risolte.