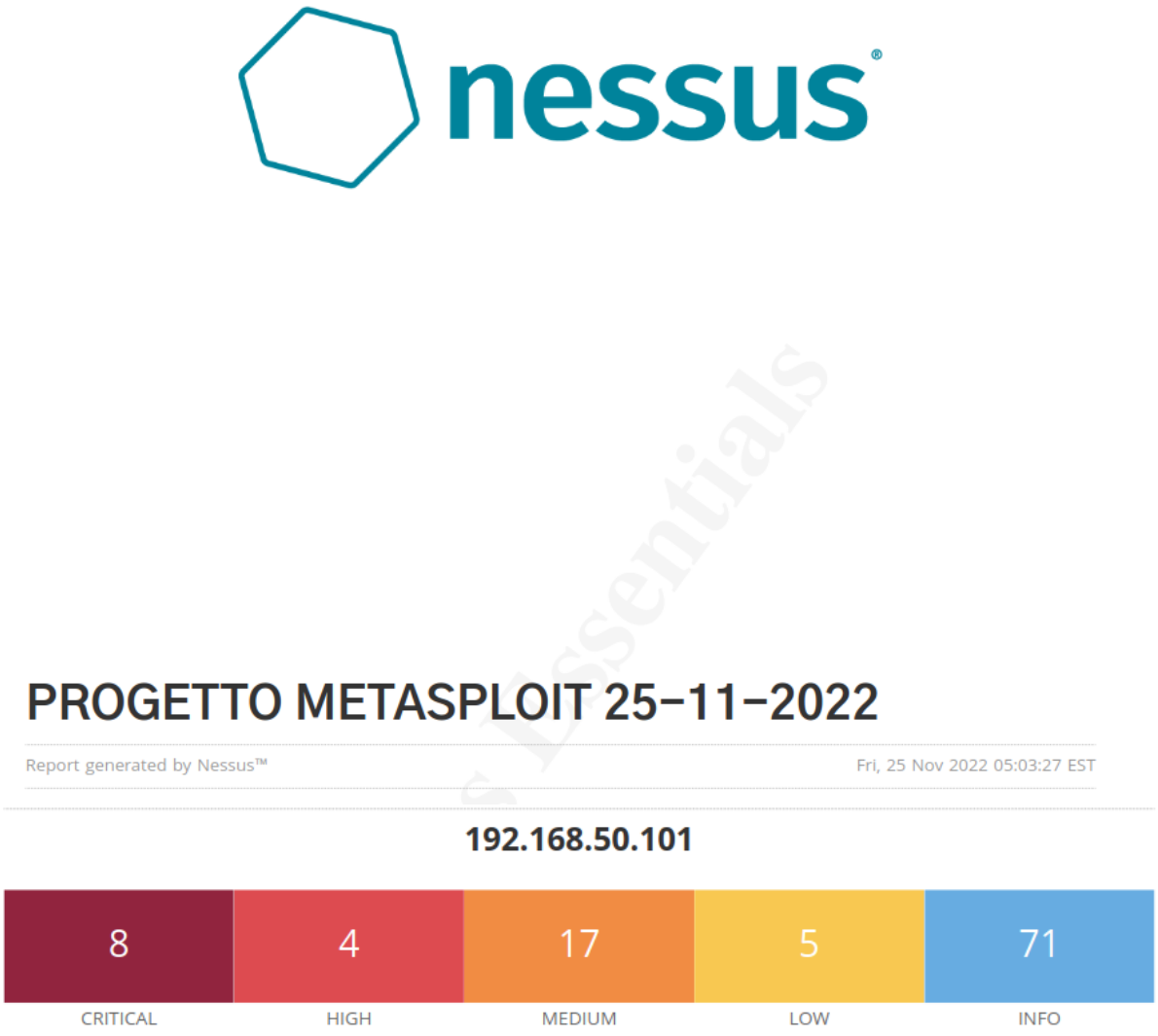
CUORE ANDREA

25-11-2022

VULNERABILITY REMEDIATION:

	HOST	IP HOST	OS HOST
NESSUS	METASPLOIT	192.168.50.101	KALI LINUX



BIND SHELL BACKDOOR DETECTION:

Per risolvere questo problema ho abilitato una regola di Firewall su macchina metasploitable che blocca il traffico in entrata sulla porta 1524

```
msfadmin@metasploitable:~$ sudo iptables -I INPUT -p TCP --dport 1524 -j DROP
msfadmin@metasploitable:~$ sudp iptables -L
-bash: sudp: command not found
msfadmin@metasploitable:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       tcp  --  anywhere             anywhere            tcp dpt:ingreslock

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
msfadmin@metasploitable:~$ _
```

NFS EXPORTED SHARE INFORMATION DISCLOSURE/ NFS SHARES WORLD READABLE

Per la risoluzione di queste vulnerabilità ho configurato L'NFS andando ad inserire l'indirizzo IP della macchina metasploit come unico ip autorizzato (bloccando cosi qualsiasi altro IP)

```
  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)
```

VNC SERVER "PASSWORD" PASSWORD

Per risolvere questa vulnerabilità abbiamo modificato la password che di default era "password" in una password "più forte"

```
root@metasploitable:~/.vnc# pwd
/root/.vnc
root@metasploitable:~/.vnc# ls
metasploitable:0.log  metasploitable:1.log  metasploitable:2.log  xstartup
metasploitable:0.pid  metasploitable:1.pid  passwd
root@metasploitable:~/.vnc# cd ..
root@metasploitable:~# vncpasswd /root/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)? n
root@metasploitable:~#
```