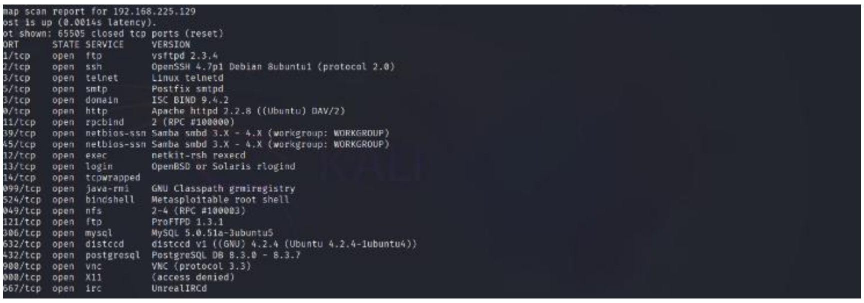
01 VULNERABILITY SCANNING

A. PREPARE ENVIRONMENT

1. Start your Kali VM and the Metasploitable VM on the same host-only or NAT network. Confirm network connectivity:
   - ip a (on Kali) → identify your attacker IP
   - ping 192.168.96.128→ confirm target reachable.

B. NMAP — DISCOVERY & SERVICE VERSION

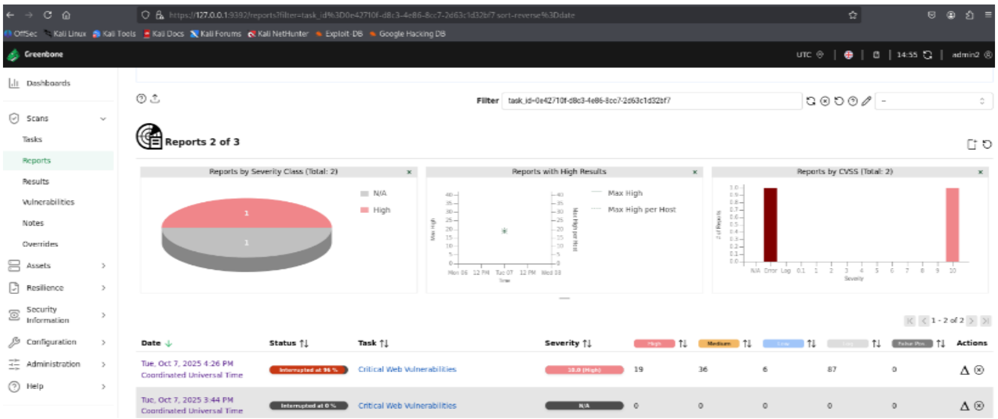
1. **Quick host discovery** (ping sweep):
   - nmap -sn 192.168.96.128
2. **Service/version enumeration** (one target):
   - nmap -sV -p- --min-rate 1000 192.168.96.128
   - Explanation: -sV probes service versions; -p- scans all ports.
3. **More invasive/scripted scan** (detect specific vulnerabilities):
   - nmap -sV --script=vuln 192.168.96.128
4. Save output:
   - nmap -sV -vv -p -oN nmap_scan.txt 192.168.96.128



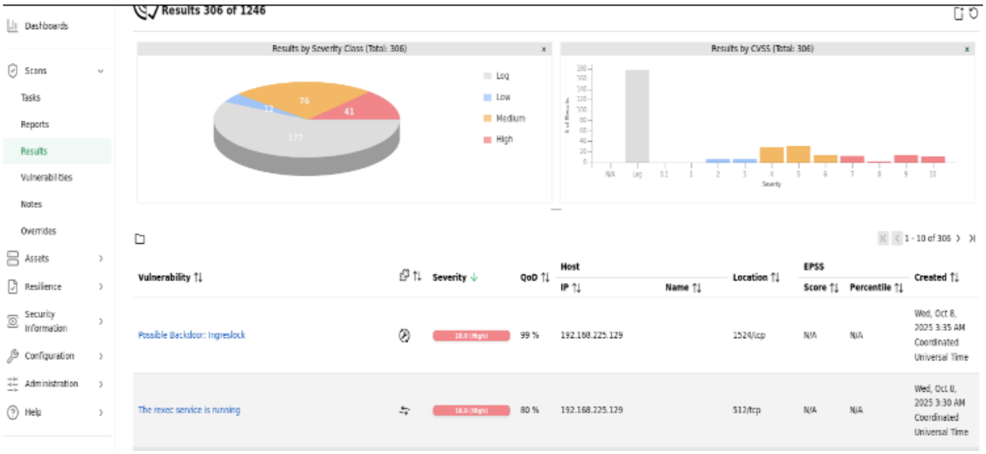
```
map scan report for 192.168.225.129
ost is up (0.0014s latency).
ot shown: 65505 closed tcp ports (reset)
ORT      STATE SERVICE     VERSION
1/tcp    open  ftp         vsftpd 2.3.4
2/tcp    open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
3/tcp    open  telnet      Linux telnetd
5/tcp    open  smtp        Postfix smtpd
3/tcp    open  domain      ISC BIND 9.4.2
0/tcp    open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
11/tcp   open  rpcbind     2 (RPC #100000)
39/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
45/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
12/tcp   open  exec        netkit-rsh rexecd
13/tcp   open  login       OpenBSD or Solaris rlogind
14/tcp   open  tcpwrapped
099/tcp  open  java-rmi    GNU Classpath grmiregistry
524/tcp  open  bindshell   Metasploitable root shell
049/tcp  open  nfs         2-4 (RPC #100003)
121/tcp  open  ftp         ProFTPD 1.3.1
306/tcp  open  mysql       MySQL 5.0.51a-3ubuntu5
632/tcp  open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
900/tcp  open  vnc         VNC (protocol 3.3)
000/tcp  open  X11         (access denied)
667/tcp  open  irc         UnrealIRCd
```

C. OPENVAS / GREENBONE (GVM) — VULNERABILITY SCANNING

1. Initialize / start GVM (example):
   - sudo gvm-start — wait until services are up.
2. Use the GVM web UI (usually https://127.0.0.1:9392) — log in with admin.
3. Create a new target (192.168.96.128), create a task, run a full & deep scan.
4. Export the results as PDF/CSV and save into evidence folder.



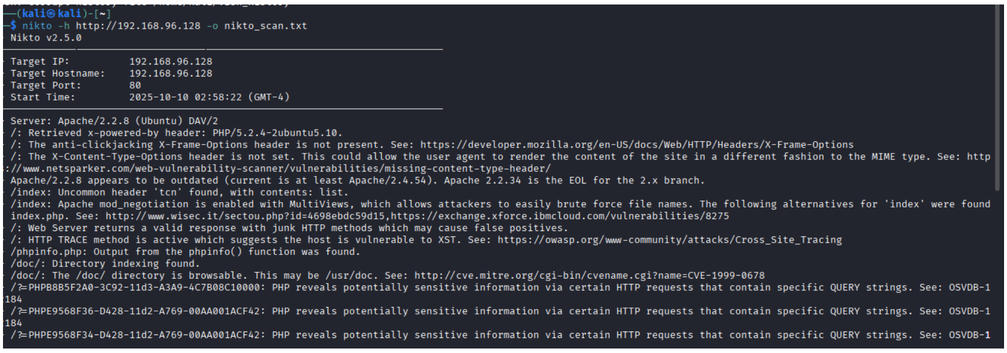
Date	Status	Task	Severity	High	Medium	Low	Log	False Pos.	Actions
Tue, Oct 7, 2025 4:26 PM Coordinated Universal Time	Interrupted at 96 %	Critical Web Vulnerabilities	10.0 (High)	19	36	6	87	0	
Tue, Oct 7, 2025 3:44 PM Coordinated Universal Time	Interrupted at 0 %	Critical Web Vulnerabilities	N/A	0	0	0	0	0	



Vulnerability		Severity	QoD	Host IP	Host Name	Location	EPSS Score	EPSS Percentile	Created
Possible Backdoor: Ingreslock		10.0 (High)	99 %	192.168.225.129		1524/tcp	N/A	N/A	Wed, Oct 8, 2025 3:35 AM Coordinated Universal Time
The rexec service is running		10.0 (High)	80 %	192.168.225.129		512/tcp	N/A	N/A	Wed, Oct 8, 2025 3:30 AM Coordinated Universal Time

D. NIKTO — WEB SERVER CHECKS

1. Run Nikto against web host:
   - nikto -h http://192.168.96.128 -o nikto_scan.txt
2. Review for outdated components, dangerous headers, default files.



```
┌──(kali㉿kali)-[~]
└─$ nikto -h http://192.168.96.128 -o nikto_scan.txt
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.96.128
+ Target Hostname:    192.168.96.128
+ Target Port:        80
+ Start Time:         2025-10-10 02:58:22 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: http
s://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found
  index.php. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ /phpinfo.php: Output from the phpinfo() function was found.
+ /doc/: Directory indexing found.
+ /doc/: The /doc/ directory is browsable. This may be /usr/doc. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0678
+ /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-1
2184
+ /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-1
2184
+ /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-1
```