Comprehensive Reconnaissance Report

Professional Security Assessment

Target	Generated
10.1.3.2	2025-09-03 22:34:28

Executive Summary

Services Detected

53

Open Ports

0

Vulnerabilities

0

Risk Assessment

High Risk Services

8

Medium Risk Services

3

Low Risk Services

49

Network Scan Results

TCP Fast Scan

```
# Nmap 7.95 scan initiated Wed Sep  3 21:47:34 2025 as: /usr/
libNmap scan report for 10.1.3.2
Host is up (0.00073s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE      VERSION
21/tcp   open  ftp          vsftpd 2.3.4
22/tcp   open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1
(protocol 2.0)
23/tcp   open  telnet       Linux telnetd
25/tcp   open  smtp         Postfix smtpd
53/tcp   open  domain       ISC BIND 9.4.2
80/tcp   open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind      2 (RPC #100000)
139/tcp  open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup:
WORKGROUP)
445/tcp  open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup:
WORKGROUP)
512/tcp  open  exec         netkit-rsh rexecd
513/tcp  open  login        OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
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  ccproxy-ftp?
3306/tcp open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc          VNC (protocol 3.3)
6000/tcp open  X11          (access denied)
6667/tcp open  irc          UnrealIRCd
8009/tcp open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:58:9E:87 (PCS Systemtechnik/Oracle
VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain,
irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/
o:linux:linux_kernel

Service detection performed. Please report any incorrect results
at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 158.26 seconds
incorrect results at https://nmap.org/submit/ .
# Nmap done at Wed Sep  3 21:50:12 2025 -- 1 IP address (1 host
up) scanned in 158.26 seconds
```

TCP Full Scan

```
# Nmap 7.95 scan initiated Wed Sep  3 21:47:34 2025 as: /usr/
libNmap scan report for 10.1.3.2
Host is up (0.00019s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 2.3.4
22/tcp    open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1
(protocol 2.0)
23/tcp    open  telnet      Linux telnetd
25/tcp    open  smtp        Postfix smtpd
53/tcp    open  domain      ISC BIND 9.4.2
80/tcp    open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup:
WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup:
WORKGROUP)
512/tcp   open  exec        netkit-rsh rexecd
513/tcp   open  login
514/tcp   open  tcpwrapped
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
3632/tcp  open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu
4.2.4-1ubuntu4))
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc         VNC (protocol 3.3)
6000/tcp  open  X11         (access denied)
6667/tcp  open  irc         UnrealIRCd
6697/tcp  open  irc         UnrealIRCd
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
8787/tcp  open  drb         Ruby DRb RMI (Ruby 1.8; path /usr/
lib/ruby/1.8/drb)
42179/tcp open  nlockmgr    1-4 (RPC #100021)
51351/tcp open  mountd      1-3 (RPC #100005)
52503/tcp open  status      1 (RPC #100024)
56793/tcp open  java-rmi    GNU Classpath grmiregistry
MAC Address: 08:00:27:58:9E:87 (PCS Systemtechnik/Oracle
VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain,
irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/
o:linux:linux_kernel

Service detection performed. Please report any incorrect results
at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 128.90 seconds
any incorrect results at https://nmap.org/submit/ .
```

```
# Nmap done at Wed Sep  3 21:49:43 2025 -- 1 IP address (1 host
up) scanned in 128.90 seconds
```

UDP Fast Scan

```
# Nmap 7.95 scan initiated Wed Sep  3 21:47:34 2025 as: /usr/
libWarning: 10.1.3.2 giving up on port because retransmission cap
hit (6).
Nmap scan report for 10.1.3.2
Host is up (0.00055s latency).
Not shown: 77 closed udp ports (port-unreach)
PORT      STATE         SERVICE
17/udp    open|filtered qotd
53/udp    open          domain
68/udp    open|filtered dhcpc
69/udp    open|filtered tftp
111/udp   open          rpcbind
123/udp   open|filtered ntp
137/udp   open          netbios-ns
138/udp   open|filtered netbios-dgm
445/udp   open|filtered microsoft-ds
497/udp   open|filtered retrospect
515/udp   open|filtered printer
520/udp   open|filtered route
998/udp   open|filtered puparp
999/udp   open|filtered applix
1023/udp  open|filtered unknown
1433/udp  open|filtered ms-sql-s
2048/udp  open|filtered dls-monitor
2049/udp  open          nfs
4444/udp  open|filtered krb524
5060/udp  open|filtered sip
49153/udp open|filtered unknown
49190/udp open|filtered unknown
49194/udp open|filtered unknown
MAC Address: 08:00:27:58:9E:87 (PCS Systemtechnik/Oracle
VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 80.72 seconds
 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

# Nmap done at Wed Sep  3 21:48:55 2025 -- 1 IP address (1 host
up) scanned in 80.72 seconds
```

Service Analysis

Vsinet

Port/Protocol: 996/udp
Port: 996

Target: 10.1.3.2

Port: 996

Protocol: udp

Note: No footprint module available for vsinet

Ssh

Port/Protocol: 22/tcp
Port: 22
Version: 4.7p1

Vulnerabilities Detected

ExploitDB CVEs:

none

Metasploit CVEs:

none

Target: 10.1.3.2

Port: 22

Server: OpenSSH

Version: 4.7p1

Auth Methods:

Exploitdb Mods: OpenSSH 2.3 < 7.7 - Username Enumeration (PoC) (linux/remote/45210.py), OpenSSH 2.3 < 7.7 - Username Enumeration (linux/remote/45233.py), OpenSSH < 6.6 SFTP (x64) - Command Execution (linux_x86-64/remote/45000.c), OpenSSH < 6.6 SFTP - Command Execution (linux/remote/45001.py), OpenSSH < 7.4 - 'UsePrivilegeSeparation Disabled' Forwarded Unix Domain So (linux/local/40962.txt), OpenSSH < 7.4 - agent Protocol Arbitrary Library Loading (linux/remote/40963.txt), OpenSSH < 7.7 - User Enumeration (2) (linux/remote/45939.py)

Exploitdb Cves: none

Msf Mods: none

Msf Cves: none

Postgresql

Port/Protocol: 5432/tcp
Port: 5432

Target: 10.1.3.2

Nmap Postgresql Banner: Starting Nmap 7.95 (https://nmap.org) at 2025-09-03 22:17 +01 Nmap scan report for 10.1.3.2 Host is up (0.00036s latency). PORT STATE SERVICE VERSION 5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7 MAC Address: 08:00:27:58:9E:87 (PCS Systemtechnik/Oracle VirtualBox virtual NIC) Service detection performed. Please report any incorrect results at https://nmap.org/submit/ . Nmap done: 1 IP address (1 host up) scanned in 6.82 seconds

Raw Postgresql Banner: [!] No banner — PostgreSQL requires proper handshake.

Msf Exploit Found: yes

Msf Exploit Mods: exploit/linux/http/acronis_cyber_infra_cve_2023_45249, exploit/linux/http/appsmith_rce_cve_2024_55964, exploit/linux/http/beyondtrust_pra_rs_unauth_rce, exploit/linux/postgres/postgres_payload, exploit/multi/http/manage_engine_dc_pmp_sqli, exploit/multi/http/rudder_server_sqli_rce, exploit/multi/postgres/postgres_copy_from_program_cmd_exec, exploit/multi/postgres/postgres_createlang, exploit/windows/misc/manageengine_eventlog_analyzer_rce, exploit/windows/postgres/postgres_payload

Msf Exploit Cves: CVE-2007-3280, CVE-2014-3996, CVE-2015-7387, CVE-2019-9193, CVE-2023-30625, CVE-2023-45249, CVE-2024-12356, CVE-2024-55963, CVE-2024-55964, CVE-2025-1094

Port: 5432

Ntp

Port/Protocol: 123/udp
Port: 123

Target: 10.1.3.2

Port: 123

Protocol: udp

Note: No footprint module available for ntp

Dls-Monitor

Port/Protocol: 2048/udp
Port: 2048

Target: 10.1.3.2

Port: 2048

Protocol: udp

Note: No footprint module available for dls-monitor

Tcpwrapped

Port/Protocol: 514/tcp
Port: 514

Target: 10.1.3.2

Port: 514

Protocol: tcp

Note: No footprint module available for tcpwrapped

Exec

Port/Protocol: 512/tcp
Port: 512

Target: 10.1.3.2

Port: 512

Protocol: tcp

Note: No footprint module available for exec

Netbios-Ns

Port/Protocol: 137/udp
Port: 137

Target: 10.1.3.2

Port: 137

Protocol: udp

Note: No footprint module available for netbios-ns

Dhcpc

Port/Protocol: 68/udp
Port: 68

Target: 10.1.3.2

Port: 68

Protocol: udp

Note: No footprint module available for dhcpc

Sip

Port/Protocol: 5060/udp
Port: 5060

Target: 10.1.3.2

Port: 5060

Protocol: udp

Note: No footprint module available for sip

Unknown

Port/Protocol: Multiple

Multiple Instances

Instance 1:
Target: 10.1.3.2

Port: 1023

Protocol: udp

Note: No footprint module available for unknown

Risk Level: low

Instance 2:
Target: 10.1.3.2

Port: 1027

Protocol: udp

Note: No footprint module available for unknown

Risk Level: low

21

Port/Protocol: ftp
Port: 21
Version: 2.3.4

Vulnerabilities Detected

ExploitDB CVEs:

none

Metasploit CVEs:

none

Target: 10.1.3.2

Port: 21

Server: vsftpd

Version: 2.3.4

Anonymous Login Allowed: yes

Anonymous Upload Allowed: no

Backdoor Detected: yes

Ftp Syst:

- **| Stat:**
- **| Ftp Server Status:**
- **| Type:** ASCII
- **| Ftp-Anon:** Anonymous FTP login allowed (FTP code 230)
- **Mac Address:** 08:00:27:58:9E:87 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
- **Service Info:** OS: Unix

Smtp

Port/Protocol: 25/tcp
Port: 25

Target: 10.1.3.2

Smtp Open: yes

Smtp Banner: Starting Nmap 7.95 (https://nmap.org) at 2025-09-03 22:30 +01

Open Relay: yes

Smtp Exploit Found: no

Smtp Exploit Mods: none

Smtp Exploit Cves: none

Port: 25

Java-Rmi

Port/Protocol: 1099/tcp
Port: 1099

Target: 10.1.3.2

Port: 1099

Protocol: tcp

Note: No footprint module available for java-rmi

Status

Port/Protocol: 52503/tcp
Port: 52503

Target: 10.1.3.2

Port: 52503

Protocol: tcp

Note: No footprint module available for status

Domain

Port/Protocol: Multiple

Multiple Instances

Instance 1:
Target: 10.1.3.2

Port: 53

Protocol: tcp

Note: No footprint module available for domain

Risk Level: low

Instance 2:
Target: 10.1.3.2

Port: 53

Protocol: udp

Note: No footprint module available for domain

Risk Level: low

Telnet

Port/Protocol: 23/tcp
Port: 23

Target: 10.1.3.2

Port: 23

Protocol: tcp

Note: No footprint module available for telnet

Netbios-Ssn

Port/Protocol: Multiple

Multiple Instances

Instance 1:
Target: 10.1.3.2

Port: 445

Protocol: tcp

Note: No footprint module available for netbios-ssn

Risk Level: low

Instance 2:
Target: 10.1.3.2

Port: 139

Protocol: tcp

Note: No footprint module available for netbios-ssn

Risk Level: low

Qotd

Port/Protocol: 17/udp
Port: 17

Target: 10.1.3.2

Port: 17

Protocol: udp

Note: No footprint module available for qotd

Route

Port/Protocol: 520/udp
Port: 520

Target: 10.1.3.2

Port: 520

Protocol: udp

Note: No footprint module available for route

Mountd

Port/Protocol: 51351/tcp
Port: 51351

Target: 10.1.3.2

Port: 51351

Protocol: tcp

Note: No footprint module available for mountd

Wap-Wsp

Port/Protocol: 9200/udp
Port: 9200

Target: 10.1.3.2

Port: 9200

Protocol: udp

Note: No footprint module available for wap-wsp

Microsoft-Ds

Port/Protocol: 445/udp
Port: 445

Target: 10.1.3.2

Port: 445

Protocol: udp

Note: No footprint module available for microsoft-ds

Distccd

Port/Protocol: 3632/tcp
Port: 3632

Target: 10.1.3.2

Port: 3632

Protocol: tcp

Note: No footprint module available for distccd

Puparp

Port/Protocol: 998/udp
Port: 998

Target: 10.1.3.2

Port: 998

Protocol: udp

Note: No footprint module available for puparp

Login

Port/Protocol: 513/tcp
Port: 513

Target: 10.1.3.2

Port: 513

Protocol: tcp

Note: No footprint module available for login

Ms-
Sql-S

Port/Protocol: 1433/udp
Port: 1433

Target: 10.1.3.2

Port: 1433

Protocol: udp

Note: No footprint module available for ms-sql-s

Applix

Port/Protocol: 999/udp
Port: 999

Target: 10.1.3.2

Port: 999

Protocol: udp

Note: No footprint module available for applix

Drb

Port/Protocol: 8787/tcp
Port: 8787

Target: 10.1.3.2

Port: 8787

Protocol: tcp

Note: No footprint module available for drb

22

Port/Protocol: ssh
Port: 22
Version: 4.7p1

Vulnerabilities Detected

ExploitDB CVEs:

none

Metasploit CVEs:

none

Target: 10.1.3.2

Port: 22

Server: OpenSSH

Version: 4.7p1

Auth Methods:

Exploitdb Mods: OpenSSH 2.3 < 7.7 - Username Enumeration (PoC) (linux/remote/45210.py), OpenSSH 2.3 < 7.7 - Username Enumeration (linux/remote/45233.py), OpenSSH < 6.6 SFTP (x64) - Command Execution (linux_x86-64/remote/45000.c), OpenSSH < 6.6 SFTP - Command Execution (linux/remote/45001.py), OpenSSH < 7.4 - 'UsePrivilegeSeparation Disabled' Forwarded Unix Domain So (linux/local/40962.txt), OpenSSH < 7.4 - agent Protocol Arbitrary Library Loading (linux/remote/40963.txt), OpenSSH < 7.7 - User Enumeration (2) (linux/remote/45939.py)

Exploitdb Cves: none

Msf Mods: none

Msf Cves: none

Nlockmgr

Port/Protocol: 42179/tcp
Port: 42179

Target: 10.1.3.2

Port: 42179

Protocol: tcp

Note: No footprint module available for nlockmgr

Ajp13

Port/Protocol: 8009/tcp
Port: 8009

Target: 10.1.3.2

Port: 8009

Protocol: tcp

Note: No footprint module available for ajp13

Retrospect

Port/Protocol: 497/udp
Port: 497

Target: 10.1.3.2

Port: 497

Protocol: udp

Note: No footprint module available for retrospect

Nat-T-Ike

Port/Protocol: 4500/udp
Port: 4500

Target: 10.1.3.2

Port: 4500

Protocol: udp

Note: No footprint module available for nat-t-ike

Nfs

Port/Protocol: Multiple

Multiple Instances

Instance 1:
Target: 10.1.3.2

Nfs Version: nfs

Nfs Exports: none

Nfs Exports Count: 0

Rpc Services Count: 23

Exploits Found: yes

Metasploit Modules: exploit/multi/http/atlassian_confluence_namespace_ognl_injection, exploit/multi/http/atlassian_confluence_rce_cve_2024_21683, exploit/multi/http/atlassian_confluence_unauth_backup, exploit/multi/http/atlassian_confluence_webwork_ognl_injection, exploit/netware/sunrpc/pkernel_callit, exploit/osx/local/nfs_mount_root, exploit/windows/ftp/labf_nfsaxe, exploit/windows/ftp/xlink_client, exploit/windows/ftp/xlink_server, exploit/windows/nfs/xlink_nfsd

Port: 2049

Risk Level: low

Instance 2:
Target: 10.1.3.2

Nfs Version: nfs

X11

Port/Protocol: 6000/tcp
Port: 6000

Target: 10.1.3.2

Port: 6000

Protocol: tcp

Note: No footprint module available for x11

Shell-

Port/Protocol: 514/tcp
Port: 514

Target: 10.1.3.2

Port: 514

Protocol: tcp

Note: No footprint module available for shell?

Rpcbind

Port/Protocol: Multiple

Multiple Instances

Instance 1:
Target: 10.1.3.2

Port: 111

Protocol: udp

Note: No footprint module available for rpcbind

Risk Level: low

Instance 2:
Target: 10.1.3.2

Port: 111

Protocol: tcp

Note: No footprint module available for rpcbind

Risk Level: low

Printer

Port/Protocol: 515/udp
Port: 515

Target: 10.1.3.2

Port: 515

Protocol: udp

Note: No footprint module available for printer

Ccproxy-Ftp-

Port/Protocol: 2121/tcp
Port: 2121

Target: 10.1.3.2

Port: 2121

Protocol: tcp

Note: No footprint module available for ccproxy-ftp?

Irc

Port/Protocol: 6667/tcp
Port: 6667

Target: 10.1.3.2

Nmap Irc Banner: Starting Nmap 7.95 (https://nmap.org) at 2025-09-03 22:31 +01 Nmap scan report for 10.1.3.2 Host is up (0.00045s latency). PORT STATE SERVICE VERSION 6667/tcp open irc UnrealIRCd MAC Address: 08:00:27:58:9E:87 (PCS Systemtechnik/Oracle VirtualBox virtual NIC) Service Info: Host: irc.Metasploitable.LAN Service detection performed. Please report any incorrect results at https://nmap.org/submit/ . Nmap done: 1 IP address (1 host up) scanned in 1.15 seconds

Irc Raw Banner: :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...

Msf Exploit Found: no

Msf Exploit Mods: none

Msf Exploit Cves: none

Port: 6667

Krb524

Port/Protocol: 4444/udp
Port: 4444

Target: 10.1.3.2

Port: 4444

Protocol: udp

Note: No footprint module available for krb524

Ftp

Port/Protocol: Multiple

Multiple Instances

Instance 1:
Target: 10.1.3.2

Port: 2121

Server: ProFTPD

Version: 1.3.1

Anonymous Login Allowed: no

Anonymous Upload Allowed: no

Backdoor Detected: no

Ftp Syst:

Exploitdb Mods: none

Exploitdb Cves: none

Msf Mods: none

Msf Cves: none

Risk Level: high

Instance 2:
Target: 10.1.3.2

Port: 21

Server: vsftpd

2121

Port/Protocol: ftp
Port: 2121
Version: 1.3.1

Vulnerabilities Detected

ExploitDB CVEs:

none

Metasploit CVEs:

none

Target: 10.1.3.2

Port: 2121

Server: ProFTPD

Version: 1.3.1

Anonymous Login Allowed: no

Anonymous Upload Allowed: no

Backdoor Detected: no

Exploitdb Mods: none

Exploitdb Cves: none

Msf Mods: none

Msf Cves: none

Netbios-Dgm

Port/Protocol: 138/udp
Port: 138

Target: 10.1.3.2

Port: 138

Protocol: udp

Note: No footprint module available for netbios-dgm

Mysql

Port/Protocol: 3306/tcp
Port: 3306

Target: 10.1.3.2

Port: 3306

Protocol: tcp

Error: Decoding error: 'utf-8' codec can't decode byte 0xaa in position 36: invalid start byte

Http

Port/Protocol: Multiple

Multiple Instances

Instance 1:
Target: 10.1.3.2

Os Fingerprint: Linux 2.6.9 - 2.6.33

Http Banner: Apache/2.2.8 (Ubuntu) DAV/2

Https Banner: unknown

Discovered Endpoints: {'url': 'http://10.1.3.2/.hta', 'type': 'general_endpoint', 'parameters': ['id', 'file', 'page', 'param', 'action']}, {'url': 'http://10.1.3.2/.htaccess.php', 'type': 'dynamic_file', 'parameters': ['id', 'file', 'page', 'include', 'path', 'cmd', 'exec', 'param', 'action']}, {'url': 'http://10.1.3.2/twiki', 'type': 'general_endpoint', 'parameters': ['id', 'file', 'page', 'param', 'action']}, {'url': 'http://10.1.3.2/.htpasswd.config', 'type': 'sensitive_file', 'parameters': ['file', 'path', 'include']}, {'url': 'http://10.1.3.2/.htpasswd.zip', 'type': 'general_endpoint', 'parameters': ['id', 'file', 'page', 'param', 'action']}, {'url': 'http://10.1.3.2/.hta.bak', 'type': 'sensitive_file', 'parameters': ['file', 'path', 'include']}, {'url': 'http://10.1.3.2/.htpasswd', 'type': 'general_endpoint', 'parameters': ['id', 'file', 'page', 'param', 'action']}, {'url': 'http://10.1.3.2/test', 'type': 'general_endpoint', 'parameters': ['id', 'file', 'page', 'param', 'action']}, {'url': 'http://10.1.3.2/phpinfo', 'type': 'general_endpoint', 'parameters': ['id', 'file', 'page', 'param', 'action']}, {'url': 'http://10.1.3.2/server-status', 'type': 'general_endpoint', 'parameters': ['id', 'file', 'page', 'param', 'action']}, {'url': 'http://10.1.3.2/index.php', 'type': 'dynamic_file', 'parameters': ['id', 'file', 'page', 'include', 'path', 'cmd', 'exec', 'param', 'action']}, {'url': 'http://10.1.3.2/phpinfo.php', 'type': 'dynamic_file', 'parameters': ['id', 'file',

Vnc

Port/Protocol: 5900/tcp
Port: 5900

Target: 10.1.3.2

Nmap Vnc Banner: Starting Nmap 7.95 (https://nmap.org) at 2025-09-03 22:33 +01 Nmap scan report for 10.1.3.2 Host is up (0.00066s latency). PORT STATE SERVICE VERSION 5900/tcp open vnc VNC (protocol 3.3) MAC Address: 08:00:27:58:9E:87 (PCS Systemtechnik/Oracle VirtualBox virtual NIC) Service detection performed. Please report any incorrect results at https://nmap.org/submit/ . Nmap done: 1 IP address (1 host up) scanned in 0.82 seconds

Raw Vnc Banner: RFB 003.003

Msf Exploit Found: no

Msf Exploit Mods: none

Msf Exploit Cves: none

Port: 5900

Bindshell

Port/Protocol: 1524/tcp
Port: 1524

Target: 10.1.3.2

Port: 1524

Protocol: tcp

Note: No footprint module available for bindshell

Http-Rpc-Epmap

Port/Protocol: 593/udp
Port: 593

Target: 10.1.3.2

Port: 593

Protocol: udp

Note: No footprint module available for http-rpc-epmap

Tftp

Port/Protocol: 69/udp
Port: 69

Target: 10.1.3.2

Port: 69

Protocol: udp

Note: No footprint module available for tftp

Xdmcp

Port/Protocol: 177/udp
Port: 177

Target: 10.1.3.2

Port: 177

Protocol: udp

Note: No footprint module available for xdmcp

Netassistant

Port/Protocol: 3283/udp
Port: 3283

Target: 10.1.3.2

Vulnerability Summary

Ssh (22/tcp)

VULNERABILITY TYPE	DETAILS
ExploitDB CVEs	none
Metasploit CVEs	none

21 (ftp)

VULNERABILITY TYPE	DETAILS
ExploitDB CVEs	none
Metasploit CVEs	none

22 (ssh)

VULNERABILITY TYPE	DETAILS
ExploitDB CVEs	none
Metasploit CVEs	none

2121 (ftp)

VULNERABILITY TYPE	DETAILS
ExploitDB CVEs	none
Metasploit CVEs	none

No known vulnerabilities detected in scanned services.

Report Generated: 2025-09-03 22:34:28

Target: 10.1.3.2

This report contains sensitive security information. Handle with appropriate care.