# Comprehensive Reconnaissance Report

Professional Security Assessment

**Target**

**192.168.1.50**

**Generated**

**2025-09-02 16:34:49**

## Executive Summary

**Services Detected**

53

**Open Ports**

0

**Vulnerabilities**

0

## Risk Assessment

### High Risk Services

8

### Medium Risk Services

4

### Low Risk Services

48

# Network Scan Results

## TCP Fast Scan

```
# Nmap 7.95 scan initiated Tue Sep  2 15:32:27 2025 as: /usr/
libNmap scan report for 192.168.1.50 (192.168.1.50)
Host is up (0.0020s 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?
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  ftp         ProFTPD 1.3.1
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 139.82 seconds
ort any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Sep  2 15:34:47 2025 -- 1 IP address (1 host
up) scanned in 139.82 seconds
```

## TCP Full Scan

```
# Nmap 7.95 scan initiated Tue Sep  2 15:32:27 2025 as: /usr/
libNmap scan report for 192.168.1.50 (192.168.1.50)
Host is up (0.0026s 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?
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  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)
39086/tcp open  status      1 (RPC #100024)
44654/tcp open  nlockmgr    1-4 (RPC #100021)
47917/tcp open  mountd      1-3 (RPC #100005)
57400/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 152.22 seconds
 report any incorrect results at https://nmap.org/submit/ .
```

```
# Nmap done at Tue Sep  2 15:34:59 2025 -- 1 IP address (1 host up) scanned in 152.22 seconds
```

## UDP Fast Scan

```
# Nmap 7.95 scan initiated Tue Sep  2 15:32:27 2025 as: /usr/libWarning: 192.168.1.50 giving up on port because retransmission cap hit (6).
Nmap scan report for 192.168.1.50 (192.168.1.50)
Host is up (0.0028s latency).
Not shown: 70 open|filtered udp ports (no-response), 26 closed udp ports (port-unreach)
PORT     STATE SERVICE
53/udp   open  domain
111/udp  open  rpcbind
137/udp  open  netbios-ns
2049/udp open  nfs
MAC Address: 08:00:27:58:9E:87 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 22.88 seconds
58:9E:87 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

# Nmap done at Tue Sep  2 15:32:50 2025 -- 1 IP address (1 host up) scanned in 22.88 seconds
```

# Service Analysis

## Irc

**Port/Protocol:** Multiple

#### Multiple Instances

**Instance 1:**
**Target:** 192.168.1.50

**Nmap Irc Banner:** Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-02 15:35 +01 Nmap scan report for 192.168.1.50 (192.168.1.50) Host is up (0.0014s 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 1.46 seconds

**Irc Raw Banner:** :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname... :irc.Metasploitable.LAN NOTICE AUTH :*** Found your hostname (cached)

**Msf Exploit Found:** no

**Msf Exploit Mods:** none

**Msf Exploit Cves:** none

**Port:** 6697

**Risk Level:** low

**Instance 2:**
**Target:** 192.168.1.50

**Nmap Irc Banner:** Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-02 16:01 +01 Nmap scan report for 192.168.1.50

## Ajp13

**Port/Protocol:** 8009/tcp
**Port:** 8009

**Target:** 192.168.1.50

**Port:** 8009

**Protocol:** tcp

**Note:** No footprint module available for ajp13

## Nlockmgr

**Port/Protocol:** 44654/tcp
**Port:** 44654

**Target:** 192.168.1.50

**Port:** 44654

**Protocol:** tcp

**Note:** No footprint module available for nlockmgr

## Domain

**Port/Protocol:** Multiple

#### Multiple Instances

**Instance 1:**
**Target:** 192.168.1.50

**Port:** 53

**Protocol:** tcp

**Note:** No footprint module available for domain

**Risk Level:** low

**Instance 2:**
**Target:** 192.168.1.50

**Port:** 53

**Protocol:** udp

**Note:** No footprint module available for domain

**Risk Level:** low

## Wdbrpc

**Port/Protocol:** 17185/udp
**Port:** 17185

**Target:** 192.168.1.50

**Port:** 17185

**Protocol:** udp

**Note:** No footprint module available for wdbrpc

## Backorifice

**Port/Protocol:** 31337/udp
**Port:** 31337

**Target:** 192.168.1.50

**Port:** 31337

**Protocol:** udp

**Note:** No footprint module available for backorifice

## X11

**Port/Protocol:** 6000/tcp
**Port:** 6000

**Target:** 192.168.1.50

**Port:** 6000

**Protocol:** tcp

**Note:** No footprint module available for x11

## Exec-

**Port/Protocol:** 512/tcp
**Port:** 512

**Target:** 192.168.1.50

**Port:** 512

**Protocol:** tcp

**Note:** No footprint module available for exec?

## Ftp

**Port/Protocol:** Multiple

**Multiple Instances**

**Instance 1:**
**Target:** 192.168.1.50

**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-Vsftpd-Backdoor:**
- **| Vulnerable:**
- **| State:** VULNERABLE (Exploitable)
- **| Ids:** BID:48539 CVE:CVE-2011-2523
- **| Disclosure Date:** 2011-07-03
- **| Exploit Results:**
- **| Shell Command:** id
- **| Results:** uid=0(root) gid=0(root)
- **| References:**
- **| Https:** //cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523

## Unknown

**Port/Protocol:** 49152/udp
**Port:** 49152

**Target:** 192.168.1.50

**Port:** 49152

**Protocol:** udp

**Note:** No footprint module available for unknown

## Smtp

**Port/Protocol:** 25/tcp
**Port:** 25

**Target:** 192.168.1.50

**Smtp Open:** yes

**Smtp Banner:** Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-02 16:33 +01

**Open Relay:** yes

**Smtp Exploit Found:** no

**Smtp Exploit Mods:** none

**Smtp Exploit Cves:** none

**Port:** 25

## Netbios-Ssn

**Port/Protocol:** Multiple

#### Multiple Instances

**Instance 1:**
**Target:** 192.168.1.50

**Port:** 139

**Protocol:** tcp

**Note:** No footprint module available for netbios-ssn

**Risk Level:** low

**Instance 2:**
**Target:** 192.168.1.50

**Port:** 445

**Protocol:** tcp

**Note:** No footprint module available for netbios-ssn

**Risk Level:** low

## 22

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

**Vulnerabilities Detected**

### ExploitDB CVEs:

none

### Metasploit CVEs:

none

**Target:** 192.168.1.50

**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

## 2121

**Port/Protocol:** ftp
**Port:** 2121
**Version:** 1.3.1

**Vulnerabilities Detected**

### ExploitDB CVEs:

none

### Metasploit CVEs:

none

**Target:** 192.168.1.50

**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

## Status

**Port/Protocol:** 39086/tcp
**Port:** 39086

**Target:** 192.168.1.50

**Port:** 39086

**Protocol:** tcp

**Note:** No footprint module available for status

## Sometimes-Rpc6

**Port/Protocol:** 32771/udp
**Port:** 32771

**Target:** 192.168.1.50

**Port:** 32771

**Protocol:** udp

**Note:** No footprint module available for sometimes-rpc6

## Ms-Sql-S

**Port/Protocol:** 1433/udp
**Port:** 1433

**Target:** 192.168.1.50

**Port:** 1433

**Protocol:** udp

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

## Vnc

**Port/Protocol:** 5900/tcp
**Port:** 5900

**Target:** 192.168.1.50

**Nmap Vnc Banner:** Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-02 16:12 +01 Nmap scan report for 192.168.1.50 (192.168.1.50) Host is up (0.0060s 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 1.41 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:** 192.168.1.50

**Port:** 1524

**Protocol:** tcp

**Note:** No footprint module available for bindshell

## Http

**Port/Protocol:** Multiple

### Multiple Instances

**Instance 1:**
**Target:** 192.168.1.50

**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://192.168.1.50/.htaccess.zip', 'type': 'general_endpoint', 'parameters': ['id', 'file', 'page', 'param', 'action']}, {'url': 'http://192.168.1.50/.htpasswd.php', 'type': 'dynamic_file', 'parameters': ['id', 'file', 'page', 'include', 'path', 'cmd', 'exec', 'param', 'action']}, {'url': 'http://192.168.1.50/.htaccess.txt', 'type': 'general_endpoint', 'parameters': ['id', 'file', 'page', 'param', 'action']}, {'url': 'http://192.168.1.50/.hta.zip', 'type': 'general_endpoint', 'parameters': ['id', 'file', 'page', 'param', 'action']}, {'url': 'http://192.168.1.50/.htpasswd.zip', 'type': 'general_endpoint', 'parameters': ['id', 'file', 'page', 'param', 'action']}, {'url': 'http://192.168.1.50/.htaccess.config', 'type': 'sensitive_file', 'parameters': ['file', 'path', 'include']}, {'url': 'http://192.168.1.50/server-status', 'type': 'general_endpoint', 'parameters': ['id', 'file', 'page', 'param', 'action']}, {'url': 'http://192.168.1.50/.hta.config', 'type': 'sensitive_file', 'parameters': ['file', 'path', 'include']}, {'url': 'http://192.168.1.50/.htpasswd', 'type': 'general_endpoint', 'parameters': ['id', 'file', 'page', 'param', 'action']}, {'url': 'http://192.168.1.50/cgi-bin/', 'type': 'general_endpoint', 'parameters': ['id', 'file', 'page', 'param', 'action']}, {'url': 'http://192.168.1.50/test', 'type': 'general_endpoint', 'parameters': ['id', 'file', 'page', 'param', 'action']}, {'url': 'http://192.168.1.50/phpMyAdmin',

## Radacct

**Port/Protocol:** 1646/udp
**Port:** 1646

**Target:** 192.168.1.50

**Port:** 1646

**Protocol:** udp

**Note:** No footprint module available for radacct

## Mountd

**Port/Protocol:** 47917/tcp
**Port:** 47917

**Target:** 192.168.1.50

**Port:** 47917

**Protocol:** tcp

**Note:** No footprint module available for mountd

## Rpcbind

**Port/Protocol:** Multiple

### Multiple Instances

**Instance 1:**
**Target:** 192.168.1.50

**Port:** 111

**Protocol:** udp

**Note:** No footprint module available for rpcbind

**Risk Level:** low

**Instance 2:**
**Target:** 192.168.1.50

**Port:** 111

**Protocol:** tcp

**Note:** No footprint module available for rpcbind

**Risk Level:** low

## Nfs

**Port/Protocol:** Multiple

#### Multiple Instances

**Instance 1:**
**Target:** 192.168.1.50

**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:** 192.168.1.50

**Nfs Version:** nfs

## Login-

**Port/Protocol:** 513/tcp
**Port:** 513

**Target:** 192.168.1.50

**Port:** 513

**Protocol:** tcp

**Note:** No footprint module available for login?

## Msantipiracy

**Port/Protocol:** 2222/udp
**Port:** 2222

**Target:** 192.168.1.50

**Port:** 2222

**Protocol:** udp

**Note:** No footprint module available for msantipiracy

## Ssh

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

**Vulnerabilities Detected**

### ExploitDB CVEs:

none

### Metasploit CVEs:

none

**Target:** 192.168.1.50

**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:** 192.168.1.50

**Nmap Postgresql Banner:** Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-02 16:16 +01 Nmap scan report for 192.168.1.50 (192.168.1.50) Host is up (0.0027s 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 7.31 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

## 21

**Port/Protocol:** ftp
**Port:** 21
**Version:** 2.3.4

**Vulnerabilities Detected**

### ExploitDB CVEs:

none

### Metasploit CVEs:

none

**Target:** 192.168.1.50

**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-Vsftpd-Backdoor:**
- **| Vulnerable:**
- **| State:** VULNERABLE (Exploitable)
- **| Ids:** BID:48539 CVE:CVE-2011-2523
- **| Disclosure Date:** 2011-07-03

## Iad1

**Port/Protocol:** 1030/udp
**Port:** 1030

**Target:** 192.168.1.50

**Port:** 1030

**Protocol:** udp

**Note:** No footprint module available for iad1

## Tcpwrapped

**Port/Protocol:** 514/tcp
**Port:** 514

**Target:** 192.168.1.50

**Port:** 514

**Protocol:** tcp

**Note:** No footprint module available for tcpwrapped

## Drb

**Port/Protocol:** 8787/tcp
**Port:** 8787

**Target:** 192.168.1.50

**Port:** 8787

**Protocol:** tcp

**Note:** No footprint module available for drb

## Tftp

**Port/Protocol:** 69/udp
**Port:** 69

**Target:** 192.168.1.50

**Port:** 69

**Protocol:** udp

**Note:** No footprint module available for tftp

## Asf-Rmcp

**Port/Protocol:** 623/udp
**Port:** 623

**Target:** 192.168.1.50

**Port:** 623

**Protocol:** udp

**Note:** No footprint module available for asf-rmcp

## Telnet

**Port/Protocol:** 23/tcp
**Port:** 23

**Target:** 192.168.1.50

**Port:** 23

**Protocol:** tcp

**Note:** No footprint module available for telnet

## Adobeserver-3

**Port/Protocol:** 3703/udp
**Port:** 3703

**Target:** 192.168.1.50

**Port:** 3703

**Protocol:** udp

**Note:** No footprint module available for adobeserver-3

## Distccd

**Port/Protocol:** 3632/tcp
**Port:** 3632

**Target:** 192.168.1.50

**Port:** 3632

**Protocol:** tcp

**Note:** No footprint module available for distccd

## Login

**Port/Protocol:** 513/tcp
**Port:** 513

**Target:** 192.168.1.50

**Port:** 513

**Protocol:** tcp

**Note:** No footprint module available for login

## Rockwell-Csp2

**Port/Protocol:** 2223/udp
**Port:** 2223

**Target:** 192.168.1.50

**Port:** 2223

**Protocol:** udp

**Note:** No footprint module available for rockwell-csp2

## Netbios-Ns

**Port/Protocol:** 137/udp
**Port:** 137

**Target:** 192.168.1.50

**Port:** 137

**Protocol:** udp

**Note:** No footprint module available for netbios-ns

## Dls-Monitor

**Port/Protocol:** 2048/udp
**Port:** 2048

**Target:** 192.168.1.50

**Port:** 2048

**Protocol:** udp

**Note:** No footprint module available for dls-monitor

## Cisco-Sccp

**Port/Protocol:** 2000/udp
**Port:** 2000

**Target:** 192.168.1.50

**Port:** 2000

**Protocol:** udp

**Note:** No footprint module available for cisco-sccp

## Blackjack

**Port/Protocol:** 1025/udp
**Port:** 1025

**Target:** 192.168.1.50

**Port:** 1025

**Protocol:** udp

**Note:** No footprint module available for blackjack

## Ndmp

**Port/Protocol:** 10000/udp
**Port:** 10000

**Target:** 192.168.1.50

**Port:** 10000

**Protocol:** udp

**Note:** No footprint module available for ndmp

## Netbios-Dgm

**Port/Protocol:** 138/udp
**Port:** 138

**Target:** 192.168.1.50

**Port:** 138

**Protocol:** udp

**Note:** No footprint module available for netbios-dgm

## Dhcpc

**Port/Protocol:** 68/udp
**Port:** 68

**Target:** 192.168.1.50

**Port:** 68

**Protocol:** udp

**Note:** No footprint module available for dhcpc

## Cfdptkt

**Port/Protocol:** 120/udp
**Port:** 120

**Target:** 192.168.1.50

**Port:** 120

**Protocol:** udp

**Note:** No footprint module available for cfdptkt

## Https

**Port/Protocol:** 443/udp
**Port:** 443

**Target:** 192.168.1.50

**Port:** 443

**Protocol:** udp

**Note:** No footprint module available for https

## Mysql

**Port/Protocol:** 3306/tcp
**Port:** 3306

**Target:** 192.168.1.50

**Port:** 3306

**Protocol:** tcp

**Error:** Decoding error: 'utf-8' codec can't decode byte 0xff in position 4: invalid start byte

## Bakbonenetvault

**Port/Protocol:** 20031/udp
**Port:** 20031

**Target:** 192.168.1.50

**Port:** 20031

**Protocol:** udp

**Note:** No footprint module available for bakbonenetvault

## Retrospect

**Port/Protocol:** 497/udp
**Port:** 497

**Target:** 192.168.1.50

**Port:** 497

**Protocol:** udp

**Note:** No footprint module available for retrospect

## H225Gatedisc

**Port/Protocol:** 1718/udp
**Port:** 1718

**Target:** 192.168.1.50

**Port:** 1718

**Protocol:** udp

**Note:** No footprint module available for h225gatedisc

## Java-Rmi

**Port/Protocol:** 1099/tcp
**Port:** 1099

**Target:** 192.168.1.50

**Port:** 1099

**Protocol:** tcp

**Note:** No footprint module available for java-rmi

# Vulnerability Summary

### 22 (ssh)

| VULNERABILITY TYPE | DETAILS |
|---|---|
| ExploitDB CVEs | none |
| Metasploit CVEs | none |

### 2121 (ftp)

| VULNERABILITY TYPE | DETAILS |
|---|---|
| ExploitDB CVEs | none |
| Metasploit CVEs | none |

### Ssh (22/tcp)

| VULNERABILITY TYPE | DETAILS |
|---|---|
| ExploitDB CVEs | none |
| Metasploit CVEs | none |

### 21 (ftp)

| VULNERABILITY TYPE | DETAILS |
|---|---|
| ExploitDB CVEs | none |
| Metasploit CVEs | none |

**No known vulnerabilities detected in scanned services.**

**Report Generated:** 2025-09-02 16:34:49

**Target:** 192.168.1.50

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