Comprehensive Reconnaissance Report

Professional Security Assessment

Target	Generated
192.168.1.113	2025-09-01 23:39:51

Executive Summary

Services Detected

27

Open Ports

0

Vulnerabilities

0

Risk Assessment

High Risk Services

2

Medium Risk Services

3

Low Risk Services

26

Network Scan Results

TCP Fast Scan

```
# Nmap 7.95 scan initiated Mon Sep  1 22:49:59 2025 as: /usr/
libNmap scan report for 192.168.1.113 (192.168.1.113)
Host is up (0.0055s latency).
Not shown: 991 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 5.3p1 Debian 3ubuntu4 (Ubuntu
Linux; protocol 2.0)
80/tcp   open  http        Apache httpd 2.2.14 ((Ubuntu)
mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch
proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14
OpenSSL...)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup:
WORKGROUP)
143/tcp  open  imap        Courier Imapd (released 2008)
443/tcp  open  ssl/http    Apache httpd 2.2.14 ((Ubuntu)
mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch
proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14
OpenSSL...)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup:
WORKGROUP)
5001/tcp open  java-object Java Object Serialization
8080/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
8081/tcp open  http        Jetty 6.1.25
1 service unrecognized despite returning data. If you know the
service/version, please submit the following fingerprint at
https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port5001-TCP:V=7.95%I=7%D=9/1%Time=68B6150E%P=x86_64-pc-linux-
gnu%r(NUL
SF:L,4,"\xac\xed\0\x05");
MAC Address: 08:00:27:AB:58:94 (PCS Systemtechnik/Oracle
VirtualBox virtual NIC)
Service Info: OS: 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 14.64 seconds
report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Mon Sep  1 22:50:13 2025 -- 1 IP address (1 host
up) scanned in 14.64 seconds
```

TCP Full Scan

```
# Nmap 7.95 scan initiated Mon Sep  1 22:49:59 2025 as: /usr/
libNmap scan report for 192.168.1.113 (192.168.1.113)
Host is up (0.00064s latency).
Not shown: 65526 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 5.3p1 Debian 3ubuntu4 (Ubuntu
Linux; protocol 2.0)
80/tcp   open  http        Apache httpd 2.2.14 ((Ubuntu)
mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch
proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14
OpenSSL...)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup:
WORKGROUP)
143/tcp  open  imap        Courier Imapd (released 2008)
443/tcp  open  ssl/http    Apache httpd 2.2.14 ((Ubuntu)
mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch
proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14
OpenSSL...)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup:
WORKGROUP)
5001/tcp open  java-object Java Object Serialization
8080/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
8081/tcp open  http        Jetty 6.1.25
MAC Address: 08:00:27:AB:58:94 (PCS Systemtechnik/Oracle
VirtualBox virtual NIC)
Service Info: OS: 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 19.00 seconds
ase report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Mon Sep  1 22:50:17 2025 -- 1 IP address (1 host
up) scanned in 19.00 seconds
```

UDP Fast Scan

```
# Nmap 7.95 scan initiated Mon Sep  1 22:49:59 2025 as: /usr/
libWarning: 192.168.1.113 giving up on port because
retransmission cap hit (6).
Nmap scan report for 192.168.1.113 (192.168.1.113)
Host is up (0.00068s latency).
Not shown: 85 closed udp ports (port-unreach)
PORT      STATE         SERVICE
17/udp    open|filtered qotd
68/udp    open|filtered dhcpc
111/udp   open|filtered rpcbind
120/udp   open|filtered cfdptkt
136/udp   open|filtered profile
137/udp   open          netbios-ns
138/udp   open|filtered netbios-dgm
445/udp   open|filtered microsoft-ds
1026/udp  open|filtered win-rpc
1718/udp  open|filtered h225gatedisc
1900/udp  open|filtered upnp
3283/udp  open|filtered netassistant
3456/udp  open|filtered IISrpc-or-vat
49152/udp open|filtered unknown
49186/udp open|filtered unknown
MAC Address: 08:00:27:AB:58:94 (PCS Systemtechnik/Oracle
VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 85.10 seconds
7:AB:58:94 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

# Nmap done at Mon Sep  1 22:51:24 2025 -- 1 IP address (1 host
up) scanned in 85.10 seconds
```

Service Analysis

Qotd

Port/Protocol: 17/udp
Port: 17

Target: 192.168.1.113

Port: 17

Protocol: udp

Note: No footprint module available for qotd

Netbios-Ssn

Port/Protocol: Multiple

Multiple Instances

Instance 1:
Target: 192.168.1.113

Port: 139

Protocol: tcp

Note: No footprint module available for netbios-ssn

Risk Level: low

Instance 2:
Target: 192.168.1.113

Port: 445

Protocol: tcp

Note: No footprint module available for netbios-ssn

Risk Level: low

Upnp

Port/Protocol: Multiple

Multiple Instances

Instance 1:
Target: 192.168.1.113

Port: 5000

Protocol: udp

Note: No footprint module available for upnp

Risk Level: low

Instance 2:
Target: 192.168.1.113

Port: 1900

Protocol: udp

Note: No footprint module available for upnp

Risk Level: low

Netbios-Dgm

Port/Protocol: 138/udp
Port: 138

Target: 192.168.1.113

Port: 138

Protocol: udp

Note: No footprint module available for netbios-dgm

Unknown

Port/Protocol: Multiple

Multiple Instances

Instance 1:
Target: 192.168.1.113

Port: 49186

Protocol: udp

Note: No footprint module available for unknown

Risk Level: low

Instance 2:
Target: 192.168.1.113

Port: 49188

Protocol: udp

Note: No footprint module available for unknown

Risk Level: low

H225Gatedisc

Port/Protocol: 1718/udp
Port: 1718

Target: 192.168.1.113

Port: 1718

Protocol: udp

Note: No footprint module available for h225gatedisc

Nat-T-Ike

Port/Protocol: 4500/udp
Port: 4500

Target: 192.168.1.113

Port: 4500

Protocol: udp

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

Rpcbind

Port/Protocol: 111/udp
Port: 111

Target: 192.168.1.113

Port: 111

Protocol: udp

Note: No footprint module available for rpcbind

Http-Burp

Port/Protocol:
Port: N/A

Tool: burp

Target: 192.168.1.113

Urls: http://192.168.1.113/

Issues: {'name': 'Backup file', 'type': 'vulnerability', 'severity': 'Info',
'confidence': 'Certain', 'host': '', 'path': '/railsgoat/assets/application.js', 'url': '/
railsgoat/assets/application.js', 'evidence': [{'type': 'FirstOrderEvidence',
'detail': {'payload': {'bytes':
'L3JhaWxzZ29hdC9hc3NldHMvYXBwbGljYXRpb24uanMuZ3o=', 'flags': 0},
'band_flags': ['in_band']}, 'request_response': {'url': 'http://192.168.1.113/
railsgoat/assets/application.js.gz?body=1', 'request': [{'type': 'DataSegment',
'data': 'R0VUIA==', 'length': 4}, {'type': 'HighlightSegment', 'data':
'L3JhaWxzZ29hdC9hc3NldHMvYXBwbGljYXRpb24uanMuZ3o=', 'length': 35},
{'type': 'DataSegment', 'data':
'P2JvZHk9MSBIVFRQLzEuMQ0KSG9zdDogMTkyLjE2OC4xLjExMw0KQ2FjaGUtQ29udHJvbDogbWF4LV
QnJhbmQiO3Y9IjgiLCAiQ2hyb21pdW0iO3Y9IjEzOCINClNlYy1DSC1VQS1Nb2JpbGU6ID8wDQpTZWM
'length': 874}], 'response': [{'type': 'DataSegment', 'data': 'SFRUUC8xLjEg',
'length': 9}, {'type': 'HighlightSegment', 'data': 'MjAw', 'length': 3}, {'type':
'DataSegment', 'data':
'IE9LDQpEYXRlOiBNb24sIDAxIFNlcCAyMDI1IDEyOjUzOjIyIEdNVA0KU2VydmVyOiBBcGFjaGUvMi4yLj
'length': 275}, {'type': 'HighlightSegment', 'data':
'TW9uLCAxNyBNYXIgMjAxNCAwNDo1ODowMSBHTVQ=', 'length': 29},
{'type': 'DataSegment', 'data': 'DQpFVGFnOiA=', 'length': 8}, {'type':
'HighlightSegment', 'data': 'IjRmZjdiLTI4MjhkLTRmNGM2NDM4ZjI4NDAi',
'length': 27}, {'type': 'DataSegment', 'data':
'DQpBY2NlcHQtUmFuZ2VzOiBieXRlcw0KVmFyeTogQWNjZXB0LUVuY29kaW5nDQpDb25uZWN0aW9
'length': 80}, {'type': 'HighlightSegment', 'data':
'YXBwbGljYXRpb24veC1nemlw', 'length': 18}, {'type': 'DataSegment', 'data':
'DQpDb250ZW50LUxlbmd0aDog', 'length': 18}, {'type': 'HighlightSegment',
'data': 'MTY0NDkz', 'length': 6}, {'type': 'DataSegment', 'data':
'DQoNCh+LCACBf6lRAgPMvel220iyLvp/
PwWJ9pEBM0mJdlWd3aAhHpeHLld7asvd5WqK5QWRkAibBFgAqMEi+1nOe9wfd637QvcVbnyRAxIDV
dB50Pv9tE2U3nZ/Dy/BklsXrovMqPstCSrocDv48GCLPoijW/
uHh59+RdTBLV4eUig8vk9lyM4/yzkn89esyGnzOrew5p33O7QJP0/
VNFl8sis7Do6PvBf0dPtRdeJFuknlYxGki', 'length': 204}, {'type': 'SnipSegment',

Cfdptkt

Port/Protocol: 120/udp
Port: 120

Target: 192.168.1.113

Port: 120

Protocol: udp

Note: No footprint module available for cfdptkt

Iisrpc-Or-Vat

Port/Protocol: 3456/udp
Port: 3456

Target: 192.168.1.113

Port: 3456

Protocol: udp

Note: No footprint module available for iisrpc-or-vat

Imap

Port/Protocol: 143/tcp
Port: 143

Target: 192.168.1.113

Port: 143

Protocol: tcp

Note: No footprint module available for imap

Ssh

Port/Protocol: 22/tcp
Port: 22
Version: 5.3p1

Vulnerabilities Detected

ExploitDB CVEs:

none

Metasploit CVEs:

none

Target: 192.168.1.113

Port: 22

Server: OpenSSH

Version: 5.3p1

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

Http

Port/Protocol: Multiple

Multiple Instances

Instance 1:
Target: 192.168.1.113

Os Fingerprint: Linux 2.6.17 - 2.6.36

Http Banner: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/0.9.8k Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1

Https Banner: unknown

Discovered Endpoints: {'url': 'http://192.168.1.113/.svn/entries.zip', 'type': 'general_endpoint', 'parameters': ['id', 'file', 'page', 'param', 'action']}, {'url': 'http://192.168.1.113/.svnignore.config', 'type': 'sensitive_file', 'parameters': ['file', 'path', 'include']}, {'url': 'http://192.168.1.113/.svnignore.zip', 'type': 'general_endpoint', 'parameters': ['id', 'file', 'page', 'param', 'action']}, {'url': 'http://192.168.1.113/.htaccess.bak', 'type': 'sensitive_file', 'parameters': ['file', 'path', 'include']}, {'url': 'http://192.168.1.113/cgi-bin/', 'type': 'general_endpoint', 'parameters': ['id', 'file', 'page', 'param', 'action']}, {'url': 'http://192.168.1.113/.htpasswd.bak', 'type': 'sensitive_file', 'parameters': ['file', 'path', 'include']}, {'url': 'http://192.168.1.113/phpmyadmin', 'type': 'admin_panel', 'parameters': ['username', 'password', 'user', 'pass', 'admin', 'login', 'auth']}, {'url': 'http://192.168.1.113/.htpasswd', 'type': 'general_endpoint', 'parameters': ['id', 'file', 'page', 'param', 'action']}, {'url': 'http://192.168.1.113/.svn.php', 'type': 'dynamic_file', 'parameters': ['id', 'file', 'page', 'include', 'path', 'cmd', 'exec', 'param', 'action']}, {'url': 'http://

Netbios-Ns

Port/Protocol: 137/udp
Port: 137

Target: 192.168.1.113

Port: 137

Protocol: udp

Note: No footprint module available for netbios-ns

Profile

Port/Protocol: 136/udp
Port: 136

Target: 192.168.1.113

Port: 136

Protocol: udp

Note: No footprint module available for profile

Pcanywherestat

Port/Protocol: 5632/udp
Port: 5632

Target: 192.168.1.113

Port: 5632

Protocol: udp

Note: No footprint module available for pcanywherestat

Win-Rpc

Port/Protocol: 1026/udp
Port: 1026

Target: 192.168.1.113

Port: 1026

Protocol: udp

Note: No footprint module available for win-rpc

Microsoft-Ds

Port/Protocol: 445/udp
Port: 445

Target: 192.168.1.113

Port: 445

Protocol: udp

Note: No footprint module available for microsoft-ds

Applix

Port/Protocol: 999/udp
Port: 999

Target: 192.168.1.113

Port: 999

Protocol: udp

Note: No footprint module available for applix

Xdmcp

Port/Protocol: 177/udp
Port: 177

Target: 192.168.1.113

Port: 177

Protocol: udp

Note: No footprint module available for xdmcp

22

Port/Protocol: ssh
Port: 22
Version: 5.3p1

Vulnerabilities Detected

ExploitDB CVEs:

none

Metasploit CVEs:

none

Target: 192.168.1.113

Port: 22

Server: OpenSSH

Version: 5.3p1

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

Dhcpc

Port/Protocol: 68/udp
Port: 68

Target: 192.168.1.113

Port: 68

Protocol: udp

Note: No footprint module available for dhcpc

Java-Object

Port/Protocol: 5001/tcp
Port: 5001

Target: 192.168.1.113

Port: 5001

Protocol: tcp

Note: No footprint module available for java-object

Ssl-Http

Port/Protocol: 443/tcp
Port: 443

Target: 192.168.1.113

Port: 443

Protocol: tcp

Note: No footprint module available for ssl/http

Dhcps

Port/Protocol: 67/udp
Port: 67

Target: 192.168.1.113

Port: 67

Protocol: udp

Note: No footprint module available for dhcps

Netassistant

Port/Protocol: 3283/udp
Port: 3283

Target: 192.168.1.113

Port: 3283

Protocol: udp

Vulnerability Summary

Ssh (22/tcp)

VULNERABILITY TYPE	DETAILS
ExploitDB CVEs	none
Metasploit CVEs	none

22 (ssh)

VULNERABILITY TYPE	DETAILS
ExploitDB CVEs	none
Metasploit CVEs	none

No known vulnerabilities detected in scanned services.

Report Generated: 2025-09-01 23:39:51

Target: 192.168.1.113