SECURITY ASSESSMENT / AUTHORIZED LAB

Network Services Security Assessment

Initial access through DNS enumeration, anonymous FTP, POP3S, and SSH

DNS	FTP	POP3S	MAIL	SSH
AXFR	Anon	Creds	SSH key	Foothold

Target: 10.20.30.40
Date: 30 July 2026
Outcome: User-level SSH access and proof file recovered

EXECUTIVE SUMMARY

A full-service enumeration of the target identified a chain of configuration weaknesses that enabled initial access without exploiting a software vulnerability. The decisive path was an anonymous FTP share exposing password candidates, followed by POP3S credential validation, mailbox access, recovery of an SSH private key, and successful SSH authentication as user01.

Assessment outcome

The designated proof file was recovered after obtaining an interactive SSH shell as user01. The attack succeeded because multiple information-exposure and credential-handling weaknesses compounded into a complete authentication chain.

1. Scope and Initial Enumeration

Scope	Single Linux host in an authorized training environment
Target	10.20.30.40
Objective	Enumerate exposed services, identify a viable initial-access path, and recover the designated proof file
Approach	Service discovery, protocol-specific enumeration, credential validation, and authenticated access

Initial service discovery

The first Nmap scan identified common administration and infrastructure services. TCP port 53 stood out because the host was serving DNS over TCP. TCP/53 is legitimate and is commonly required for zone transfers and large DNS responses; however, its exposure made an AXFR check a logical next enumeration step.

Port	Service	Observation	Relevance
22/tcp	SSH	OpenSSH 8.2p1 Ubuntu	Potential access channel once credentials or a key were obtained
53/tcp	DNS	ISC BIND 9.16.1-Ubuntu	Prompted testing for an unauthorized zone transfer
110/tcp	POP3	Dovecot POP3	Possible mailbox-access path
995/tcp	POP3S	Dovecot over TLS	Encrypted mailbox authentication and message retrieval
2121/tcp	FTP-like	ProFTPD banner; initially unidentified by Nmap	Required additional service-specific validation

DNS zone transfer

COMMAND

```
dig axfr corp.local @10.20.30.40
```

The AXFR request succeeded and disclosed the internal DNS namespace. This confirmed a DNS configuration weakness and provided useful hostnames and addressing information:

AXFR RESULT

```
app.corp.local      10.20.40.5
dc1.corp.local      10.20.40.10
dc2.corp.local      10.20.40.10
int-ftp.corp.local  127.0.0.1
int-nfs.corp.local  10.20.40.70
ns.corp.local       127.0.0.1
unix01.corp.local       10.20.40.142
ws1.corp.local      10.20.40.101
ws2.corp.local      10.20.40.102
wsus.corp.local     10.20.40.80
```

> **Interpretation**
>
> The zone transfer was valuable reconnaissance, but the disclosed 10.20.40.0/24 systems were not directly routable from the assessment host. Connection attempts returned "No route to host", so enumeration continued against 10.20.30.40.

2. Discovery of the Initial-Access Path

Full TCP scan and hidden FTP service

A full TCP port scan identified an additional FTP service on port 30021 that was missed during the initial limited scan. Service detection showed a ProFTPD instance labelled "Internal FTP" and confirmed that anonymous login was permitted.

NMAP EVIDENCE

```
30021/tcp open  ftp
220 ProFTPD Server (Internal FTP) [10.20.30.40]
Anonymous FTP login allowed (FTP code 230)
drwxr-xr-x  2 ftp ftp 4096 Apr 18 2022 user01
```

Anonymous FTP data exposure

MIRROR COMMAND

```
wget -m --no-passive \
  ftp://anonymous:[REDACTED]@10.20.30.40:30021
```

The anonymous share exposed the directory **`/user01/credentials.txt`**, which contained several password-like strings. This provided both a probable username (user01) and a focused candidate password list.

Credential validation against POP3S

COMMAND

```
hydra -l user01 -P credentials.txt -S -s 995 10.20.30.40 pop3
```

> **Redacted laboratory credential**
>
> Username: user01
> Password: [REDACTED]

The successful result demonstrated password reuse or insecure credential storage: a password present in a publicly accessible FTP file authenticated to user01's mailbox over POP3S.

POP3S mailbox access

COMMANDS

```
openssl s_client -quiet -crlf -connect 10.20.30.40:995

USER user01
PASS [REDACTED]
LIST
RETR 1
QUIT
```

The mailbox contained one message from the administrator. The message supplied user01 with a new OpenSSH private key. The `-quiet -crlf` options were important: without quiet mode, OpenSSL intercepted the leading "R" in `RETR` as an interactive renegotiation command instead of passing it to Dovecot.

3. SSH Key Recovery and Successful Access

Private-key preparation

The private key was copied from the email into a local file. The first SSH attempt failed locally with **`error in libcrypto`**, meaning OpenSSH could not parse the file and therefore never offered the key to the server. The issue was caused by copy-and-paste formatting, including stray whitespace around the OpenSSH key boundaries. After preserving the exact header/footer and Base64 content, the key loaded correctly.

VALIDATION AND LOGIN

```
chmod 600 user01_id_rsa
ssh-keygen -y -f user01_id_rsa >/dev/null && echo "Key valid"
ssh -i user01_id_rsa user01@10.20.30.40
```

> **Verification**
>
> The corrected key authenticated without prompting for user01's password and produced an interactive shell with the prompt user01@app-server:~$. The designated proof file was then recovered.

Complete attack chain

1	**DNS enumeration**	TCP/53 prompted an AXFR test; the transfer exposed internal DNS records.
2	**Full-port discovery**	Port 30021 revealed a second ProFTPD service with anonymous access.
3	**Credential exposure**	The anonymous share exposed user01's password candidates in credentials.txt.
4	**Mailbox compromise**	A valid POP3S credential provided access to an email containing an SSH private key.
5	**SSH foothold**	After correcting the key formatting, SSH authentication as user01 succeeded and the designated proof file was recovered.

Result

Access obtained	Interactive SSH shell as user01
Authentication	OpenSSH private key recovered from POP3S mailbox
Objective	Designated proof file recovered
Exploit required	No software exploit; access resulted from chained configuration and credential-management weaknesses

4. Findings, Impact, and Remediation

Primary security findings

Finding	Impact	Risk
Unauthorized DNS zone transfer	External users could retrieve the complete zone and map internal hostnames and addresses.	**Medium**
Anonymous FTP access	Unauthenticated users could browse and download files from the internal FTP service.	**High**
Plaintext password storage	Password candidates were stored in a readable text file inside an anonymously accessible share.	**High**
Credential reuse	A password disclosed through FTP authenticated successfully to user01's POP3S mailbox.	**High**
Private key transmitted by email	A reusable SSH private key was stored in the mailbox, allowing host access after mailbox compromise.	**High**

Recommended remediation

- Restrict AXFR to explicitly authorized secondary DNS servers using BIND allow-transfer controls and network filtering.
- Disable anonymous FTP. Restrict the service to approved users and trusted management networks, or retire it if unnecessary.
- Remove plaintext password files and rotate all exposed or potentially reused credentials immediately.
- Enforce unique passwords and multi-factor authentication where supported, especially for remote and messaging services.
- Revoke and replace the emailed SSH private key. Store private keys only in approved secret-management systems and distribute public keys instead.

- Review FTP, mail, and SSH logs for unauthorized access and verify whether the exposed credentials or key were used elsewhere.

Key assessment lessons

- Service versions alone did not reveal the intended path; configuration testing was more valuable than searching for a direct OpenSSH exploit.
- TCP/53 was not inherently anomalous, but it provided a protocol-specific enumeration opportunity that exposed useful environmental context.
- A full 1-65535 TCP scan was essential because the decisive anonymous FTP service operated on non-standard port 30021.
- Small weaknesses became critical when chained: information disclosure led to credentials, credentials led to mailbox access, and mailbox access led to SSH access.
- When SSH reports error in libcrypto, validate the local private-key format before assuming the remote server rejected it.

Report note

Document screenshots or command output for the successful AXFR, anonymous FTP listing, Hydra credential validation, POP3S message retrieval, private-key validation, and final SSH session. Do not include the full private key in a client-facing report; record its fingerprint and rotation status instead.