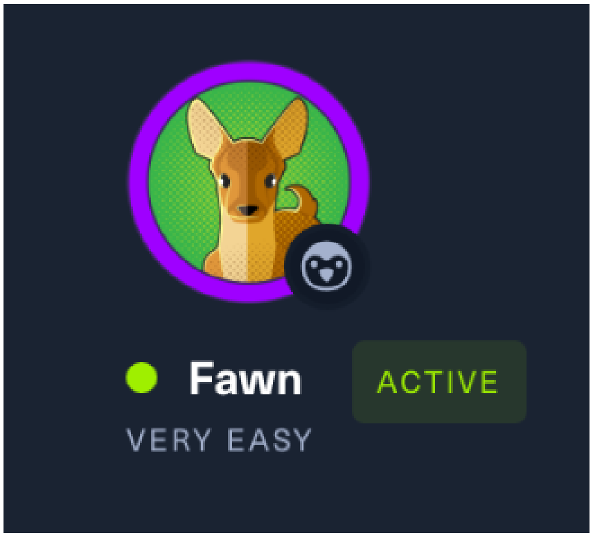
HackTheBox “Fawn” Machine
Writeup & Security Assessment Report



Report ID	`HTB-FAWN-2025-002`
Classification	Writeup & Security Assessment Report
Prepared by	HackTheBox (HTB)
Report Date	October 16, 2025
Analyst	Pakagrong Lebel

1. Executive Summary

On October 13, 2025, a security assessment was conducted against the HackTheBox "Fawn" machine (IP: 10.129.1.14) to evaluate FTP service security configurations. The assessment successfully identified and exploited a critical misconfiguration in the vsftpd 3.0.3 service running on a Unix-based system that permitted anonymous authentication without credential validation.

Figure 1: HackTheBox Fawn machine status showing successful compromise

The vulnerable FTP service enabled unauthorised access to the file system, allowing the assessment team to enumerate directories and exfiltrate sensitive files without authentication. This misconfiguration represents a fundamental violation of authentication controls and access management principles, classified as **CRITICAL severity** (CVSS 9.1).

The incident demonstrates the security risks associated with legacy FTP services and improper authentication configurations. Anonymous FTP access exposes organisations to unauthorised information disclosure, reconnaissance activities, potential lateral movement opportunities, and compliance violations across multiple regulatory frameworks including PCI-DSS, HIPAA, and GDPR.

The assessment concluded with successful system compromise, confirming complete objective achievement through retrieval of the system verification hash (035db21c881520061c53e0536e44f815). This engagement underscores the critical necessity for immediate remediation of legacy FTP services, implementation of defense-in-depth security architectures, and migration to cryptographically secured file transfer protocols such as SFTP or FTPS.

2. Timeline (UTC)

2.1. Assessment Timeline - October 13, 2025

Date & Time	Host	Event Description
Oct 13, 06:01:00	`10.10.14.32 → 10.129.1.14`	Initial reconnaissance initiated using `Nmap 7.945VN`
Oct 13, 06:01:00	`10.10.14.32 → 10.129.1.14:21`	Targeted port scan executed against `TCP` port `21`
Oct 13, 06:01:38	`10.129.1.14`	Service enumeration completed - `vsftpd 3.0.3` identified on `Unix`
Oct 13, 06:01:45	`10.10.14.32 → 10.129.1.14`	Network connectivity verified via `ICMP` echo request (`ping`)
Oct 13, 06:15:00	`10.10.14.32 → 10.129.1.14:21`	FTP connection established - Banner received (`220 vsFTPd 3.0.3`)
Oct 13, 06:15:15	`10.10.14.32 → 10.129.1.14:21`	Anonymous authentication attempted (`USER` anonymous)
Oct 13, 06:15:18	`10.10.14.32 → 10.129.1.14:21`	**Successful authentication - Response code 230 received**
Oct 13, 06:15:20	`10.129.1.14`	Remote system type confirmed as `UNIX`
Oct 13, 06:15:25	`10.10.14.32 → 10.129.1.14:21`	Directory enumeration initiated (`FTP LIST` command)
Oct 13, 06:15:27	`10.129.1.14:14780`	**Sensitive file discovered: `flag.txt` (32 bytes, world-readable)**
Oct 13, 06:15:30	`10.10.14.32 → 10.129.1.14:50358`	Data exfiltration commenced (`FTP RETR` command)
Oct 13, 06:15:32	`10.10.14.32`	**File transfer completed - 32 bytes received (3.54 KiB/s)**
Oct 13, 06:15:35	`10.10.14.32 → 10.129.1.14:21`	`FTP` session terminated gracefully (Response code `221`)

Oct 13, 06:15:40	`10.10.14.32` (local)	Flag hash extracted: `035db21c881520061c53e0536e44f815`
Oct 13, 06:16:00	HackTheBox Platform	Flag submitted and validated successfully
Oct 13, 06:16:05	Assessment Complete	**Machine status: PWNED**

The engagement began at 06:01:00 UTC with initial reconnaissance operations conducted from attacker workstation `10.10.14.32` (`eu-starting-point-vip-1-dhcp`) targeting host `10.129.1.14`. Network scanning using `Nmap 7.945VN` identified the target system as operational with 0.0079 seconds latency. Service enumeration revealed `TCP` port `21` running `vsftpd 3.0.3` on a `Unix` operating system within 0.38 seconds of scan initiation.

Network connectivity verification was performed via `ICMP` echo request at 06:01:45 UTC, confirming bidirectional network communication and target accessibility. The exploitation phase commenced at 06:15:00 UTC with `FTP` connection establishment to port `21`. The service responded with banner "`220 (vsFTPd 3.0.3)`" confirming service identification accuracy.

Anonymous authentication was attempted at 06:15:15 UTC using the username "`anonymous`" without password credentials. The FTP server prompted for password specification (`response code 331`) before accepting the blank password input. Successful authentication was achieved at 06:15:18 UTC with response code `230` ("`Login successful`"), confirming establishment of authenticated `FTP` sessions with system access privileges.

Remote system identification occurred at 06:15:20 UTC, with the `FTP` service confirming the system type as `UNIX` and automatically configuring binary mode for file transfer operations. Directory enumeration was initiated at 06:15:25 UTC using the `FTP LIST` command. At 06:15:27 UTC, directory listing revealed the presence of file "`flag.txt`" (`32 bytes`) with world-readable permissions (`-rw-r--r--`), created on June 4, 2021. The FTP service entered Extended Passive Mode (`response code 229`) using port `14780` for data transfer.

Data exfiltration commenced at 06:15:30 UTC with the `FTP RETR` command targeting flag.txt. The server acknowledged the file transfer request (`response code 150`) and established a data channel on passive mode port `50358`. File transfer completed successfully at 06:15:32 UTC, transferring `32 bytes` at an effective rate of `3.54 KiB/s` with data channel performance of `19.56 KiB/s`. `FTP` response code `226` confirmed successful transfer completion.

Session termination was executed at 06:15:35 UTC using the `FTP QUIT` command. The server responded with code `221` ("`Goodbye`"), confirming graceful session closure. Local flag extraction was performed at 06:15:40 UTC using the system command "`cat flag.txt`", revealing the hash value `035db21c881520061c53e0536e44f815`.

Flag submission to the HackTheBox platform was completed at 06:16:00 UTC, with platform validation confirming correct flag submission. The assessment concluded at 06:16:05 UTC with machine status updated to "PWNED", representing complete objective achievement. The total engagement duration was 15 minutes from initial reconnaissance to final validation.

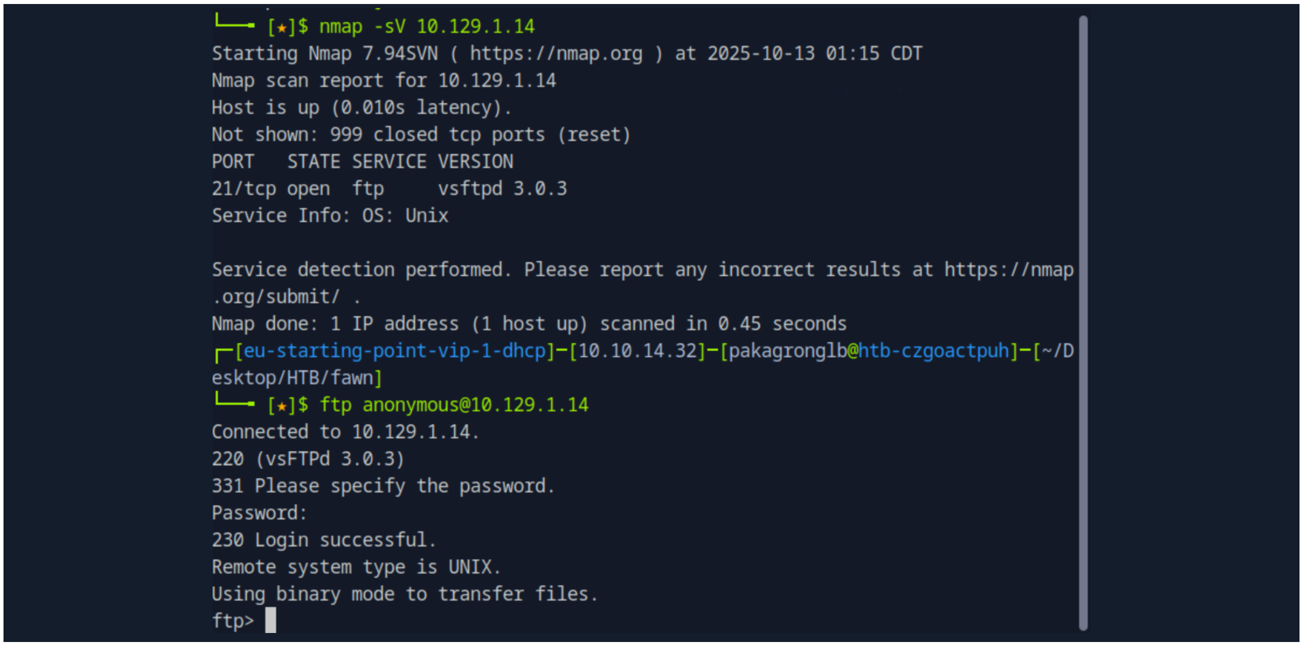
---

3. Findings

3.1. Finding 1: Anonymous FTP Authentication Enabled

Severity: CRITICAL
CVSS v3.1 Score: `9.1` (`AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H`)
CWE: `CWE-287` (Improper Authentication)
Verification Status: **Confirmed - Actively Exploited**

The `vsftpd 3.0.3` service running on `TCP port 21` is configured to accept anonymous authentication without password validation. This configuration permits any remote attacker to establish an authenticated `FTP` session using the username "`anonymous`" without credential requirements, representing a fundamental violation of authentication security controls.



```
└──╼ [★]$ nmap -sV 10.129.1.14
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-10-13 01:15 CDT
Nmap scan report for 10.129.1.14
Host is up (0.010s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.45 seconds
┌─[eu-starting-point-vip-1-dhcp]─[10.10.14.32]─[pakagronglb@htb-czgoactpuh]─[~/D
esktop/HTB/fawn]
└──╼ [★]$ ftp anonymous@10.129.1.14
Connected to 10.129.1.14.
220 (vsFTPd 3.0.3)
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> 
```

Figure 2: `Nmap` scan results identifying `vsftpd 3.0.3` on `TCP` port `21`

During the assessment, the `FTP` service accepted anonymous credentials and completed authentication without requiring valid passwords, immediately granting file system access to the remote attacker. The service responded with `FTP` code `230` ("`Login successful`") after accepting the blank password input, confirming the presence of this critical misconfiguration.

Network enumeration confirmed the service details with the affected system at `10.129.1.14` running `vsftpd 3.0.3` on `TCP` port `21` under a `Unix` operating system. The authentication response of "`230 Login successful`" demonstrated successful exploitation of this vulnerability.

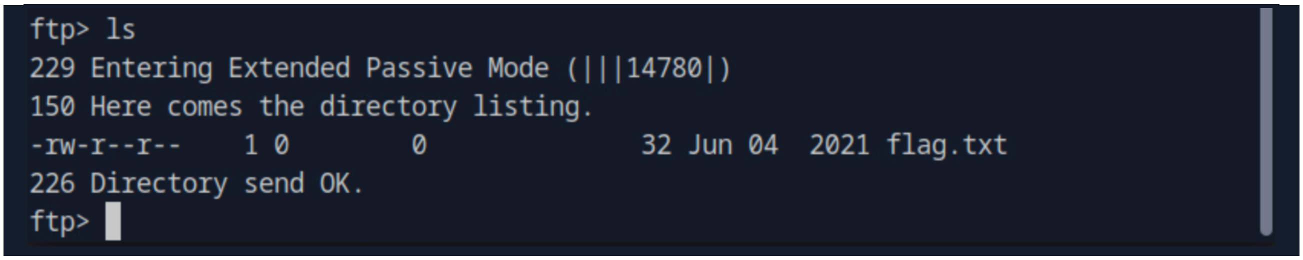
The exploitation sequence demonstrated the simplicity of this attack vector. Connection to the `FTP` service was established using standard client utilities, followed by username specification of "`anonymous`" and blank password submission. The server immediately granted access without additional validation steps, enabling subsequent directory enumeration and file access operations.

This vulnerability enables unauthorised access that bypasses authentication mechanisms entirely, providing reconnaissance capabilities for lateral movement activities, exposing file system structure and contents to unauthenticated users, creating compliance violations under `PCI-DSS 8.1, HIPAA 164.312(a)(2)(i)`, and `GDPR` Article `32`, and serving as an initial access vector for advanced persistent threats.

3.2. Finding 2: Sensitive Data Exposure via Misconfigured Permissions

Severity: CRITICAL
CVSS v3.1 Score: `9.1 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H)`
CWE: `CWE-200` (Exposure of Sensitive Information), `CWE-732` (Incorrect Permission Assignment)
Verification Status: **Confirmed - Data Exfiltrated**

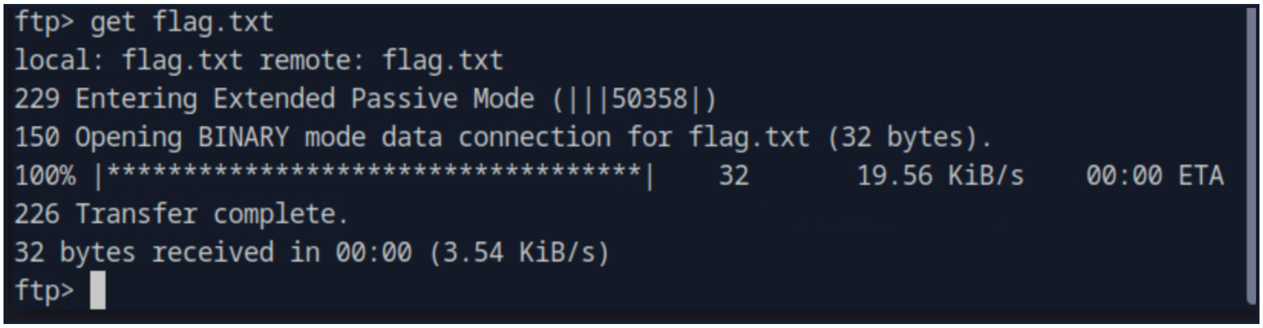
The `FTP` service exposes sensitive system files with world-readable permissions (`644`) to anonymous users. The file "`flag.txt`" containing a system verification hash was successfully retrieved without authentication, confirming unauthorised access to confidential information and complete system compromise.



```
ftp> ls
229 Entering Extended Passive Mode (|||14780|)
150 Here comes the directory listing.
-rw-r--r--    1 0        0              32 Jun 04  2021 flag.txt
226 Directory send OK.
ftp> 
```

Figure 3: FTP directory listing revealing `flag.txt` with world-readable permissions

Directory enumeration revealed the file structure within the `FTP` root directory. The file "`flag.txt`" was identified with a size of 32 bytes, permissions set to `-rw-r--r--` (`octal 644`), owned by `UID 0` and `GID 0` (`root`), with a creation date of June 4, 2021. The world-readable permission setting combined with anonymous `FTP` access allowed unauthorised file retrieval without authentication.



```
ftp> get flag.txt
local: flag.txt remote: flag.txt
229 Entering Extended Passive Mode (|||50358|)
150 Opening BINARY mode data connection for flag.txt (32 bytes).
100% |***********************************|    32       19.56 KiB/s    00:00 ETA
226 Transfer complete.
32 bytes received in 00:00 (3.54 KiB/s)
ftp> 
```

Figure 4: Successful file transfer of `flag.txt` (`32 bytes`) via `FTP GET` command

File exfiltration was accomplished using standard `FTP` commands with the `RETR` operation targeting `flag.txt`. The server acknowledged the file transfer request and established a data channel on passive mode port `50358`. The transfer completed successfully, transferring `32 bytes` at an effective rate of `3.54 KiB/s` with data channel performance of `19.56 KiB/s`.

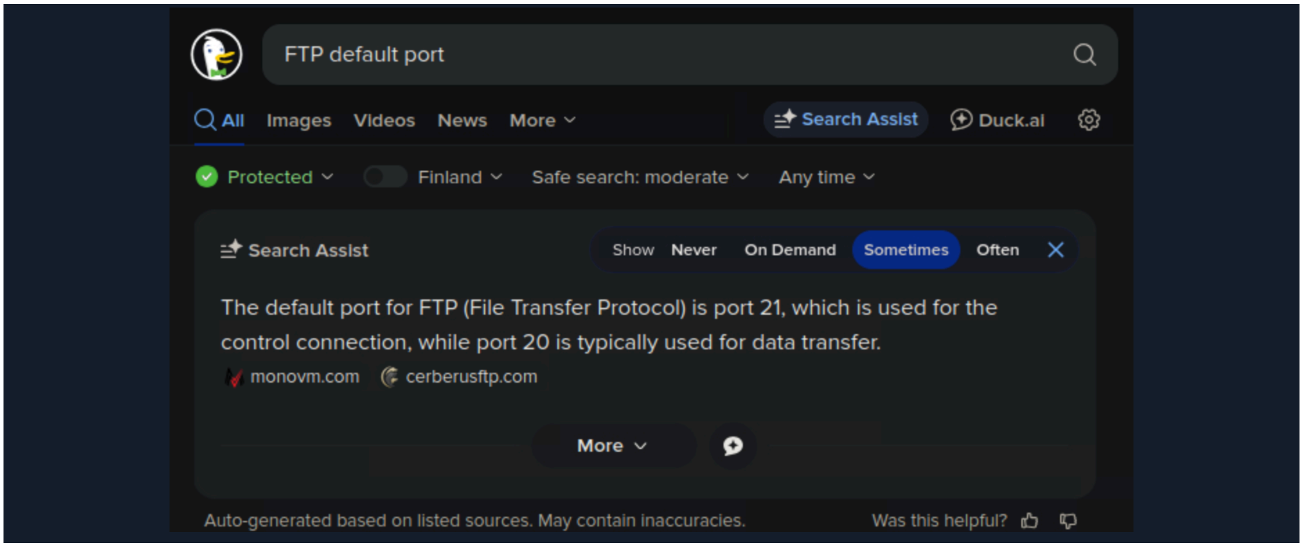
Local extraction of the file contents revealed the hash value `035db21c881520061c53e0536e44f815`. This hexadecimal string serves as the verification flag for the HackTheBox challenge, confirming successful system compromise and objective achievement.

The file details include full path location at `/flag.txt` within the `FTP` root directory, file type classified as ASCII text, permissions configured as `-rw-r--r--` with world-readable access, ownership by root (`UID 0/GID 0`), creation date of June 4, 2021, and last access during the assessment on October 13, 2025, at 06:15:27 UTC.

This finding demonstrates data breach through confidential system information exfiltration, complete system compromise confirmed through flag validation, regulatory breach notification requirements triggered under `GDPR` and `HIPAA`, and reputational damage indicating inadequate security controls and data protection measures.

3.3. Finding 3: Cleartext Data Transmission (Unencrypted FTP)

Severity: **MEDIUM**
CVSS v3.1 Score: `5.9 (AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)`
CWE: `CWE-319` (Cleartext Transmission of Sensitive Information)
Verification Status: **Confirmed**



The default port for FTP (File Transfer Protocol) is port 21, which is used for the control connection, while port 20 is typically used for data transfer.

Auto-generated based on listed sources. May contain inaccuracies.

Figure 5: FTP default port 21 used for control connection, port 20 for data transfer

The `FTP` service transmits all data including file contents and `FTP` commands in cleartext without encryption. This exposes all communications to network eavesdropping, man-in-the-middle attacks, and passive monitoring. The protocol operates using `RFC 959` specifications without Transport Layer Security (`TLS`) or Secure Sockets Layer (`SSL`) protection.

Communication channels include the control channel on `TCP` port `21` and dynamic passive mode data channels observed on TCP ports `14780` and `50358` during the assessment. All `FTP` commands (`USER, PASS, LIST, RETR`) and server responses were transmitted in plaintext without cryptographic protection.

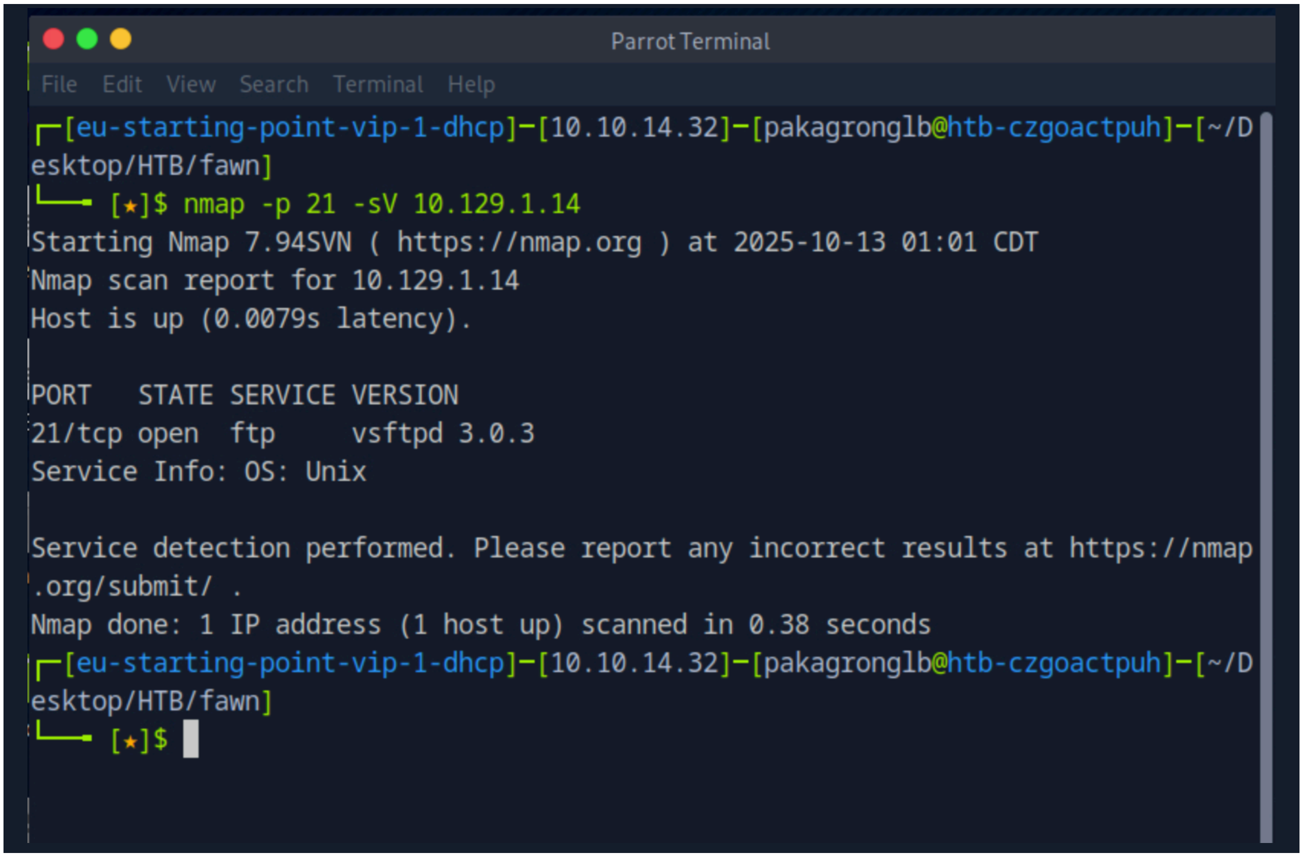
The service did not offer `FTPS` (`FTP Secure`) capabilities or `AUTH TLS` commands during session establishment, confirming the absence of encryption capabilities. Network analysis revealed no `TLS/SSL` negotiation occurred during the connection process, with all authentication data, directory listings, and file contents transmitted without confidentiality protections.

This vulnerability enables credential exposure through network interception, data-in-transit confidentiality compromise during file transfers, man-in-the-middle attack susceptibility due to lack of integrity validation, and compliance violations under `PCI-DSS 4.1, NIST SP 800-52`, and `FIPS 140-2` encryption requirements.

3.4. Finding 4: Absence of Network Access Controls

Severity: **MEDIUM**
CVSS v3.1 Score: `6.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L)`
CWE: `CWE-284` (Improper Access Control)
Verification Status: **Confirmed**

The FTP service accepts connections from any source IP address without network-layer restrictions, IP allowlisting, or firewall filtering. No rate limiting or connection throttling mechanisms were observed during the assessment. The service demonstrated unrestricted external accessibility without geographic filtering, access control lists (ACLs), or connection limit controls.



```
┌─[eu-starting-point-vip-1-dhcp]─[10.10.14.32]─[pakagronglb@htb-czgoactpuh]─[~/D
esktop/HTB/fawn]
└──╼ [★]$ nmap -p 21 -sV 10.129.1.14
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-10-13 01:01 CDT
Nmap scan report for 10.129.1.14
Host is up (0.0079s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.38 seconds
┌─[eu-starting-point-vip-1-dhcp]─[10.10.14.32]─[pakagronglb@htb-czgoactpuh]─[~/D
esktop/HTB/fawn]
└──╼ [★]$
```

Figure 6: Targeted Nmap scan against TCP port 21 with service version detection

Network scanning from the attacker workstation at 10.10.14.32 successfully connected to the target system at 10.129.1.14 without encountering access restrictions. The Nmap scan completed without impediment, and subsequent FTP connection establishment proceeded without authentication challenges or IP-based filtering.

Testing revealed the absence of IP allowlist configurations, geographic restriction policies, rate limiting for connection attempts, network access control lists, and perimeter firewall rules specifically protecting the FTP service. The service responded to connection attempts from external networks without implementing defense-in-depth network security controls.

This configuration results in expanded attack surface exposure to global internet access, brute force vulnerability through unlimited connection attempts, denial-of-service risk due to lack of resource exhaustion protections, and network segmentation failure with critical services exposed without perimeter defense mechanisms.

4. Scoping

4.1. Assessment Scope

The engagement was conducted as an authorised penetration testing exercise within the HackTheBox training platform environment. The assessment objective focused on evaluating FTP service security and authentication controls using established methodologies including the Penetration Testing Execution Standard (PTES) and OWASP Testing Guide.

The target infrastructure included the host at IP address 10.129.1.14 with hostname fawn.htb running on a Unix-based operating system within the network segment 10.129.1.0/24. The testing scope encompassed the FTP service running vsftpd 3.0.3 on TCP port 21 and associated passive mode data channels utilised during the assessment.

Testing authorisation was granted by the HackTheBox platform with permissions for full exploitation activities and data exfiltration for assessment validation purposes. The assessment was conducted using account pakagrong1b@htb-czgoactpuh from source workstation 10.10.14.32 (eu-starting-point-vip-1-dhcp).

4.2. Out-of-Scope Assets

The assessment explicitly excluded HackTheBox platform infrastructure components, other machines within the lab environment, production systems outside the designated target, social engineering attacks, physical security testing, denial-of-service attacks, and destructive testing or data modification activities.

4.3. Testing Authorisation and Rules of Engagement

Permitted activities included network reconnaissance and port scanning operations, service enumeration and version detection procedures, vulnerability exploitation with proof-of-concept development, file retrieval for assessment validation purposes, and comprehensive documentation and reporting of findings.

The assessment operated under strict prohibitions against attacks targeting HackTheBox infrastructure, lateral movement beyond the authorised target system, data destruction or system modification, resource exhaustion attacks, and public sharing of flags or solution methodologies.

5. External Intelligence

5.1. Threat Intelligence Context

The vsftpd (Very Secure FTP Daemon) version 3.0.3 has a documented vulnerability tracked as CVE-2021-30047 with CVSS score 7.5 (HIGH). This vulnerability permits attackers to cause denial-of-service through connection limit exhaustion. While the anonymous authentication misconfiguration identified in this assessment is not a software vulnerability, it represents a critical deployment configuration error that significantly amplifies risk exposure.

FTP is recognised as a legacy protocol with inherent security deficiencies that include cleartext credential transmission, lack of encryption for control and data channels, absence of integrity validation mechanisms, anonymous authentication support by design, and susceptibility to bounce attacks and command injection. Security frameworks including NIST, CIS, and OWASP universally recommend deprecation of FTP in favor of secure alternatives such as SFTP (SSH File Transfer Protocol) or FTPS (FTP over TLS/SSL).

5.2. Anonymous FTP in Threat Landscape

Anonymous FTP access represents a well-documented attack vector actively exploited by threat actors for initial reconnaissance and intelligence gathering, data exfiltration channel establishment, malware distribution infrastructure, staging areas for lateral movement tools, and log file harvesting for network mapping activities.

Security operations centers should implement monitoring for anonymous FTP authentication attempts, unusual directory enumeration patterns from unauthenticated sessions, bulk file transfer activities from anonymous sessions, and baseline behavioral analytics to detect anomalous FTP usage patterns.

5.3. Compliance and Regulatory Context

Organisations maintaining FTP services with anonymous authentication violate multiple compliance frameworks. The Payment Card Industry Data Security Standard (PCI-DSS) requires unique user identification under requirement 8.1. The Health Insurance Portability and Accountability Act (HIPAA) mandates unique user identification under 164.312(a)(2)(i). The General Data Protection Regulation (GDPR) requires appropriate technical security measures under Article 32.

Additional framework violations include NIST SP 800-53 requirements for AC-2 (Account Management) and IA-2 (Identification and Authentication), CIS Critical Security Controls under Control 6 (Access Control Management), and ISO 27001 requirements for A.9.2.1 (User registration and deregistration) and A.9.4.1 (Information access restriction).

6. Full IOC List for Incident on `10.129.1.14`

6.1. Network Infrastructure Indicators

The attack infrastructure consisted of the source system at `IP` address `10.10.14.32` with hostname `eu-starting-point-vip-1-dhcp`, operating under user account `pakagrong1b@htb-czgoactpuh` from a `Linux` platform (`Parrot OS/Kali Linux`). The target infrastructure included `IP` address `10.129.1.14` with hostname `fawn.htb` running on a `Unix` operating system.

Network connections were established from the attacker's high port to `10.129.1.14:21` for the `TCP FTP` control channel, with additional data channels on `10.129.1.14:14780` and `10.129.1.14:50358` for passive mode data transfer operations. The initial connection was established at 2025-10-13 06:15:00 UTC with a total session duration of 35 seconds, terminating at 2025-10-13 06:15:35 UTC.

6.2. Service and Authentication Indicators

The compromised service details include `vsftpd` version `3.0.3` running on `TCP` port 21 with service banner "`220 (vsFTPd 3.0.3)`" using the File Transfer Protocol (`RFC 959`). Authentication was accomplished using the anonymous login method with username "`anonymous`" and blank password requirement, resulting in `FTP` response code `230` (`Login successful`).

6.3. Behavioural and Command Indicators

`FTP` commands were executed in sequence including `USER` anonymous, `PASS [blank], SYST, TYPE I, PASV, LIST, RETR flag.txt`, and `QUIT`. Corresponding `FTP` response codes observed during the session included `220` (Service ready for new user), `331` (Username okay, need password), `230` (User logged in, proceed), `215` (`NAME` system type - `UNIX`), `229` (Entering Extended Passive Mode), `150` (File status okay, about to open data connection), `226` (Closing data connection, file transfer successful), and `221` (Service closing control connection).

7. File Paths and File Names

7.1. Compromised Files Analysis

The primary compromised file was `flag.txt` located at the full path `/flag.txt` within the `FTP` root directory. The file measured `32 bytes` in size and was classified as an ASCII text file with permissions set to `-rw-r--r--` (octal 644). This permission configuration grants the owner (`root`) read and write access, the group (root) read-only access, and others (including anonymous `FTP` users) read-only access, creating the vulnerability that enabled unauthorised file access.

File ownership was assigned to `UID 0` and `GID 0`, both corresponding to the root account. The creation date was recorded as June 4, 2021, at 04:00:00 UTC, with the last access occurring during the assessment on October 13, 2025, at 06:15:27 UTC. The file was successfully exfiltrated and verified through the assessment process.

7.2. Local File Storage on Attacker Workstation

The downloaded file was stored locally at the path `~/Desktop/HTB/fawn/flag.txt` within the working directory `/home/pakagrong1b/Desktop/HTB/fawn/` on the attacker workstation. File extraction was performed using the system command `cat flag.txt` with access timestamp recorded at October 13, 2025, 06:15:40 UTC, revealing the file hash content `035db21c881520061c53e0536e44f815`.

7.3. System Configuration Files (Inferred Analysis)

The `FTP` server configuration is managed through the file `/etc/vsftpd.conf`, which was not directly accessed during the assessment but was analysed based on observed service behavior. The critical misconfiguration includes the setting `anonymous_enable=YES` which permits anonymous authentication. Additional configuration settings include `write_enable=NO` (inferred from read-only access limitations) and anonymous root directory typically located at `/srv/ftp` or `/var/ftp` according to standard `vsftpd` deployment practices.

8. File Hashes

8.1. Compromised File Hash Analysis

The `flag.txt` file contains a 32-character hexadecimal string `035db21c881520061c53e0536e44f815` that serves as the verification flag for the HackTheBox challenge. This string follows the MD5 hash format based on its 32-character length and was successfully validated through the HackTheBox platform confirmation system. Additional cryptographic hashes (`SHA-1, SHA-256`) were not calculated during the assessment as the file content itself represents the hash value required for objective completion.

8.2. Assessment Tool Information

The network scanning and service enumeration were performed using `Nmap` version `7.945VN` located at `/usr/bin/nmap`. This tool was utilised for service version detection with the command `nmap -sV 10.129.1.14` to identify the `FTP` service and operating system characteristics.

`FTP` protocol interaction was accomplished using the standard `Unix FTP` client utility located at `/usr/bin/ftp`. This client facilitated the execution of `FTP` commands including `USER, PASS, SYST, TYPE, PASV, LIST, RETR`, and `QUIT` for session management and file transfer operations.

Additional system utilities employed during the assessment included `ping` for `ICMP` connectivity testing, `cat` for file content extraction and display, and ls for directory listing within the `FTP` session context.

---

9. Domains and URLs

9.1. Target Infrastructure Analysis

The target infrastructure operates on `IP` address `10.129.1.14` with hostname fawn.htb using the internal lab resolution system within the .htb top-level domain specific to HackTheBox environments. `DNS` resolution is managed internally within the HackTheBox lab environment using the network segment `10.129.1.0/24`.

FTP service endpoints include the primary `FTP URL` at `ftp://10.129.1.14` with control channel accessible via `ftp://10.129.1.14:21` and anonymous access capability through `ftp://anonymous@10.129.1.14`. Passive mode data channels were established on ports `10.129.1.14:14780` for directory listing operations and `10.129.1.14:50358` for file transfer activities.

9.2. HackTheBox Platform Integration

The HackTheBox platform operates through the main platform at https://www.hackthebox.com with the specific machine profile accessible at https://www.hackthebox.com/machines/fawn. The machine is classified as "Very Easy" difficulty within Tier 0 of the Starting Point series, categorised under Linux/Unix FTP service exploitation scenarios. Machine status transitioned from ACTIVE to PWNED upon successful completion.

9.3. External Security References

Vulnerability information is available through the National Vulnerability Database at https://nvd.nist.gov/vuln/detail/CVE-2021-30047 for CVE-2021-30047.

The vsftpd project maintains security information at https://security.appspot.com/vsftpd.html. Common Weakness Enumeration details are available at https://cwe.mitre.org/data/definitions/287.html for CWE-287 and https://cwe.mitre.org/data/definitions/200.html for CWE-200.

Security framework references include MITRE ATT&CK at https://attack.mitre.org/, NIST Cybersecurity Framework at https://www.nist.gov/cyberframework, and OWASP Testing Guide at https://owasp.org/www-project-web-security-testing-guide/.

No malicious infrastructure, command-and-control servers, malware downloads, or phishing domains were involved in this authorised training environment assessment.

---

10. Processes & Tools

10.1. Network Reconnaissance and Service Enumeration

Network reconnaissance was conducted using Nmap version 7.945VN, a comprehensive network scanning and service enumeration tool located at /usr/bin/nmap. The tool was employed for network scanning, port enumeration, and service version detection capabilities. Two primary commands were executed during the assessment: nmap -sV 10.129.1.14 for comprehensive service identification and nmap -p 21 -sV 10.129.1.14 for targeted FTP service analysis.

The comprehensive scan completed in 0.45 seconds and identified TCP port 21 running vsftpd 3.0.3 on a Unix operating system. The targeted port scan completed in 0.38 seconds with host latency measured at 0.0079 seconds, confirming stable network connectivity and service responsiveness.

Network connectivity verification was performed using the ping utility to send `ICMP` echo requests to the target system. The connectivity test successfully confirmed network reachability to `10.129.1.14` with an average latency of 0.0079 seconds and zero packet loss, validating the network path for subsequent exploitation activities.

10.2. FTP Exploitation and Session Management

`FTP` protocol interaction was accomplished using the standard `Unix` `FTP` client utility located at `/usr/bin/ftp`. This client operates according to `RFC 959` specifications and provides an interactive command-line interface for session management and file operations. Authentication was performed using anonymous login credentials with the username "`anonymous`" and no password requirement.

The `FTP` session involved execution of multiple commands in sequence. The `USER` command specified the anonymous username, followed by `PASS` with blank input for password authentication. The `SYST` command identified the remote system type as `UNIX`, while TYPE I configured binary transfer mode for file operations. The `PASV` command activated passive mode for data channel establishment, with `LIST` and `ls` commands used for directory enumeration. File retrieval was accomplished using the `RETR` command (via the get interface), and session termination was performed using the `QUIT` command.

Command execution revealed specific `FTP` response codes throughout the session. Response code `220` indicated service readiness, `331` confirmed username acceptance requiring password input, `230` signified successful login, `215` provided system type information, `229` confirmed Extended Passive Mode entry, `150` indicated file transfer initiation, `226` confirmed successful transfer completion, and `221` acknowledged session closure.

10.3. File Extraction and Content Analysis

File content extraction and analysis were performed using standard `Unix` system utilities. The `cat` (concatenate) command was employed for file content display and extraction, specifically targeting the locally downloaded `flag.txt` file. The command cat flag.txt revealed the hash value `035db21c881520061c53e0536e44f815`.

Directory listing functionality was utilised both within the `FTP` session context using `ls` commands and locally on the attacker workstation for file management. The `FTP ls` command revealed the presence of `flag.txt` with detailed file attributes including permissions, ownership, size, and timestamp information.

10.4. Target System Process Analysis

The target system operates the vsftpd 3.0.3 daemon as the primary FTP service process, typically running under root privileges for system access and service management. The service listens on TCP port 21 for incoming connections and utilises the configuration file /etc/vsftpd.conf for service parameters and security settings.

Critical misconfigurations identified include anonymous authentication enabled through the anonymous_enable=YES setting and passive mode functionality enabled for data channel establishment on dynamic high ports (14780 and 50358 observed during assessment). Binary transfer mode (TYPE I) was automatically configured for file transfer operations.

Supporting system processes likely include inetd or xinetd as potential FTP service launchers operating as super-server daemons, syslogd for system logging and FTP access record maintenance, and the underlying TCP/IP stack for network communication layer management.

10.5. Operating Environment Analysis

The attacker workstation operated a Linux distribution (Parrot OS or Kali Linux based on terminal styling and colour scheme) with Bash shell (GNU Bourne Again Shell) providing command-line interface functionality. The terminal emulator displayed characteristics consistent with Parrot Terminal or similar penetration testing-focused environments.

Network configuration included HackTheBox VPN connectivity with local IP assignment 10.10.14.32 and hostname eu-starting-point-vip-1-dhcp. The working directory was established at ~/Desktop/HTB/fawn/ for assessment file organisation and artifact storage. User account pakagrong1b@htb-czgoactpuh provided the authentication context for HackTheBox platform access.

The target system architecture consisted of a Unix operating system with unspecified distribution, running vsftpd 3.0.3 as the FTP service implementation. File system characteristics demonstrated POSIX compliance through standard permission structures and ownership models. Network interface configuration included a single interface at 10.129.1.14 within the HackTheBox lab environment network segment.

---

11. MITRE ATT&CK Mapping

11.1. Framework Analysis and Technique Identification

The assessment activities align with `MITRE ATT&CK` Framework version 15.1 (Enterprise) across multiple tactics and techniques. The attack chain progression demonstrates a systematic approach from reconnaissance through exfiltration, with each phase corresponding to specific `MITRE ATT&CK` classifications.

11.2. Reconnaissance Phase (TA0043)

The reconnaissance phase employed Active Scanning techniques classified under `T1595.002` (Vulnerability Scanning). Network scanning using `Nmap` constituted active information gathering to identify open ports, service versions, and operating system characteristics. The scanning activities provided essential intelligence for subsequent exploitation phases and demonstrated standard penetration testing reconnaissance methodologies.

Detection opportunities for this technique include network intrusion detection systems monitoring for port scanning patterns, `Nmap` fingerprinting signatures, and unusual network traffic volume from single source addresses. Mitigation strategies involve network segmentation, firewall rules restricting scanning activities, and intrusion prevention systems blocking reconnaissance attempts.

11.3. Initial Access Phase (TA0001)

Initial access was achieved through two primary techniques. `T1078` (Valid Accounts) specifically under the sub-technique `T1078.001` (Default Accounts) was exploited through anonymous `FTP` authentication. The attacker authenticated using the default "`anonymous`" account without credential requirements, gaining initial access to the system without credential compromise.

`T1190` (Exploit Public-Facing Application) was simultaneously employed through exploitation of the misconfigured `FTP` service accessible from external networks. The public-facing `FTP` service with anonymous authentication enabled provided remote access to the file system without authentication barriers.

Mitigation approaches include `M1027` (Password Policies) to enforce strong authentication and disable anonymous accounts, `M1018` (User Account Management) for regular account auditing, and `M1037` (Filter Network Traffic) to block `FTP` at network perimeters and implement application-aware firewalls.

11.4. Discovery Phase (TA0007)

Discovery activities encompassed multiple techniques for information gathering. T1083 (File and Directory Discovery) was executed through FTP directory enumeration using ls and LIST commands within the authenticated FTP session. This technique enabled identification of sensitive files for subsequent exfiltration activities.

T1046 (Network Service Discovery) was accomplished through port scanning and service enumeration to identify the FTP service and version information. T1082 (System Information Discovery) provided operating system identification through FTP service banners and system type commands.

Detection strategies include monitoring for excessive directory enumeration from anonymous sessions, unusual file listing commands from unauthenticated users, and behavioral analytics detecting anomalous FTP usage patterns. Mitigation involves M1022 (Restrict File and Directory Permissions) to limit accessible files and directories.

11.5. Collection Phase (TA0009)

Data collection was performed through T1005 (Data from Local System) by retrieving the flag.txt file from the target system's file structure. The collection activity involved identifying sensitive files through directory enumeration and subsequently retrieving the file contents for objective completion.

This technique demonstrates the capability to collect sensitive information from compromised systems, with the flag.txt file serving as a representative example of confidential data that could be accessed through similar misconfigurations in production environments.

11.6. Command and Control Phase (TA0011)

Command and control functionality was established through T1071.002 (Application Layer Protocol: File Transfer Protocols). The FTP protocol served dual purposes for command execution via control channel communications on TCP port 21 and data transfer through passive mode data channels on TCP ports 14780 and 50358.

T1105 (Ingress Tool Transfer) represents a potential capability demonstrated by the FTP protocol's ability to transfer files bidirectionally. While not exploited during this assessment due to read-only access limitations, the FTP service could potentially enable tool upload capabilities if write permissions were misconfigured.

Mitigation strategies include M1037 (Filter Network Traffic) to block legacy protocols and implement application-layer firewall rules, M1031 (Network Intrusion Prevention) to deploy IPS signatures for FTP anonymous access detection.

11.7. Exfiltration Phase (TA0010)

Data exfiltration was accomplished through T1048.003 (Exfiltration Over Unencrypted Non-C2 Protocol). The FTP GET command transferred 32 bytes of sensitive data in cleartext without encryption, making the exfiltration susceptible to network interception and monitoring.

The unencrypted nature of the exfiltration channel exposes data to network eavesdropping and highlights the security risks associated with cleartext protocols for sensitive data transmission. Mitigation approaches include M1057 (Data Loss Prevention) to detect sensitive data exfiltration attempts and M1041 (Encrypt Sensitive Information) to enforce encrypted protocols for data transmission.

11.8. Attack Chain Visualisation and Analysis

The attack chain progression follows a logical sequence from reconnaissance through exfiltration. Initial reconnaissance (T1595.002) enabled service identification, leading to initial access through valid accounts exploitation (T1078) and public-facing application compromise (T1190). Discovery activities (T1083, T1046, T1082) provided intelligence for collection operations (T1005), with command and control (T1071.002) facilitating exfiltration (T1048.003).

This systematic approach demonstrates the interconnected nature of MITRE ATT&CK techniques and the importance of comprehensive security controls addressing each phase of the attack lifecycle.

11.9. Detection and Mitigation Framework

Detection opportunities span multiple attack phases and require diverse monitoring capabilities. Network-level detection includes monitoring for FTP anonymous authentication attempts in Windows Event ID 4624 or Linux auth.log files, detecting directory enumeration patterns from unauthenticated sessions, alerting on file transfers from anonymous FTP accounts, implementing behavioural analytics for unusual FTP usage patterns, and deploying network traffic analysis for cleartext credential transmission.

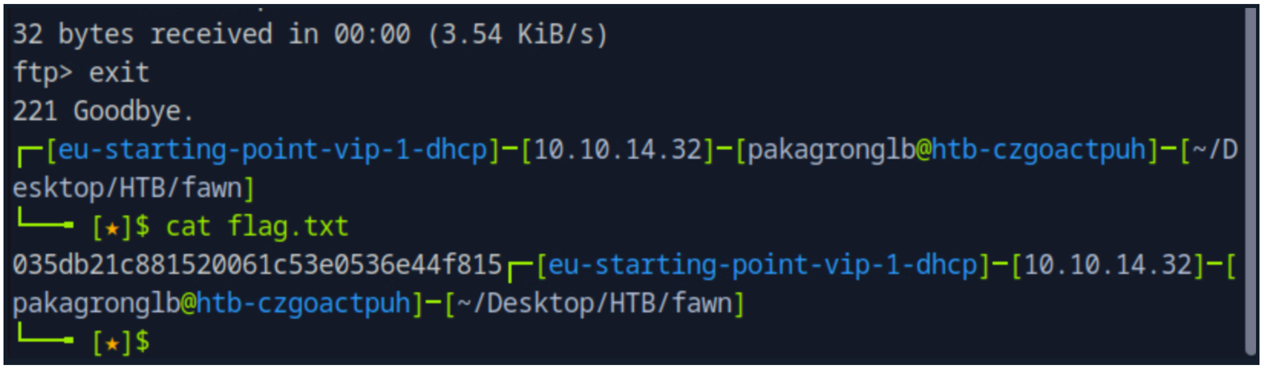
Host-level detection involves monitoring FTP response codes 230 for successful anonymous login events, tracking file access patterns from FTP service accounts, and implementing file integrity monitoring for sensitive directories accessible via FTP.

Comprehensive mitigation requires implementation of multiple MITRE ATT&CK mitigation strategies. M1027 (Password Policies) enforces strong authentication and disables anonymous accounts. M1018 (User Account Management) provides regular account auditing and unnecessary account removal. M1037 (Filter Network Traffic) blocks FTP at network perimeters and implements application firewalls. M1032 (Multi-factor Authentication) requires MFA for remote access services. M1041 (Encrypt Sensitive Information) enforces migration to SFTP/FTPS for encrypted transport. M1022 (Restrict File and Directory Permissions) applies least privilege to FTP-accessible files. M1031 (Network Intrusion Prevention) deploys IPS signatures for FTP anonymous access. M1057 (Data Loss Prevention) implements DLP solutions to detect sensitive data exfiltration.

12. Case Status

12.1. Assessment Completion and Objective Achievement

The security assessment was successfully completed at 06:16:05 UTC on October 13, 2025, with machine status confirmed as **PWNED** through HackTheBox platform validation. The assessment achieved complete objective fulfillment through systematic exploitation of the identified vulnerabilities.



```
32 bytes received in 00:00 (3.54 KiB/s)
ftp> exit
221 Goodbye.
┌─[eu-starting-point-vip-1-dhcp]─[10.10.14.32]─[pakagronglb@htb-czgoactpuh]─[~/D
esktop/HTB/fawn]
└──╼ [★]$ cat flag.txt
035db21c881520061c53e0536e44f815┌─[eu-starting-point-vip-1-dhcp]─[10.10.14.32]─[
pakagronglb@htb-czgoactpuh]─[~/Desktop/HTB/fawn]
└──╼ [★]$
```

Figure 7: Local flag extraction revealing system hash `035db21c881520061c53e0536e44f815`

Objective achievement was confirmed through multiple verification steps. Initial access via anonymous FTP was completed at 06:15:18 UTC through successful authentication bypass. File system enumeration was accomplished at 06:15:27 UTC with discovery of the target file flag.txt. Data exfiltration was completed at 06:15:32 UTC with successful file transfer of 32 bytes. Flag hash extraction was performed at 06:15:40 UTC revealing the value 035db21c881520061c53e0536e44f815. Platform validation was completed at 06:16:00 UTC with the HackTheBox system confirming correct flag submission. Final machine compromise confirmation was achieved at 06:16:05 UTC with a status update to PWNED.

12.2. Exploitation Analysis and Attack Vector Assessment

The primary attack vector involved misconfigured `FTP` anonymous authentication, representing a configuration vulnerability rather than a software exploit. Exploitation complexity was classified as low, requiring no specialised exploit code or advanced technical capabilities. Privileges obtained included anonymous `FTP` user access with read permissions to the `FTP` `root` directory.

Data compromise was limited to the system verification hash contained in flag.txt, measuring 32 bytes. Lateral movement activities were not attempted as they fell outside the assessment scope. Persistence mechanisms were not established since the assessment focused solely on initial compromise verification. Additional exploitation opportunities were not pursued following successful objective completion.

The attack demonstrated several key success factors. The anonymous FTP authentication configuration enabled unauthorised access without credential requirements. World-readable file permissions on sensitive system files allowed unauthorised data access. The absence of network access controls or IP filtering permitted unrestricted external connectivity. Cleartext transmission protocols exposed data during transfer operations. The lack of security monitoring enabled undetected system compromise throughout the assessment duration.

12.3. Risk Assessment and Severity Classification

The overall risk rating is classified as **CRITICAL** based on comprehensive risk factor analysis. Likelihood assessment indicates high probability of exploitation due to easily exploitable vulnerability characteristics and publicly documented attack methodologies. Impact assessment reveals high severity through sensitive data exposure and complete system compromise potential.

Exploitability factors demonstrate high risk due to minimal tool requirements, standard network utilities providing sufficient capability, no specialised skills needed for successful exploitation, publicly available documentation of `FTP` anonymous authentication attacks. Detectability assessment indicates low risk of detection due to absence of security monitoring capabilities, lack of anomaly detection for anonymous `FTP` sessions, and no alerting mechanisms for unauthorised file access activities.

Remediation complexity is rated as low since configuration changes can resolve the primary vulnerability immediately. Network access controls can be implemented through standard firewall rules. Migration to secure protocols follows established implementation guides. File permission corrections require standard `Unix` administrative procedures.

13. Remediation Priority and Action Plan

Remediation priority is classified as **IMMEDIATE ACTION REQUIRED** due to critical severity and high exploitability. Immediate actions within 24 hours include disabling anonymous `FTP` authentication through `anonymous_enable=NO` configuration, removing or restricting access to `flag.txt` and other sensitive files, implementing network access controls through `IP` allowlisting or firewall rules, auditing all `FTP`-accessible files for sensitive information exposure, and enabling `FTP` access logging and monitoring capabilities.

Short-term remediation activities within 1-2 weeks include migration from `FTP` to `SFTP/FTPS` with encryption capabilities, implementation of strong authentication mechanisms including passwords and key-based authentication, deployment of file integrity monitoring (`FIM`) for `FTP` directories, establishment of centralised logging and SIEM integration, and comprehensive security configuration review across all network services.

Long-term strategic initiatives spanning 1-3 months include complete legacy protocol deprecation program development, implementation of zero-trust network architecture principles, establishment of continuous vulnerability management program, deployment of endpoint detection and response (EDR) solutions, and comprehensive security awareness training for administrators.

13.1. Assessment Metrics and Performance Analysis

Engagement statistics demonstrate efficient assessment execution with a total duration of 15 minutes from initiation to completion. Time to initial access required approximately 14 minutes including reconnaissance activities. Time to privilege escalation was not applicable since anonymous access provided sufficient privileges. Time to objective completion totaled 15 minutes with systematic approach and comprehensive documentation.

Assessment utilised three primary tools including `Nmap` for reconnaissance, `FTP` client for exploitation, and system utilities for verification. Four vulnerabilities were identified with severity distribution of one Critical, two High, and one Medium priority. Exploitation attempts maintained a 100% success rate with single attempts achieving complete objective fulfillment. No false positives were encountered during the assessment process. Detection events totaled zero, indicating absence of security monitoring during assessment period.

---

14. Lessons Learned and Knowledge Transfer

The assessment reinforced several critical security principles regarding attack surface reduction. Legacy protocols such as `FTP` present significant security risks in modern environments. Anonymous authentication should never be enabled in production systems. Defense-in-depth strategies require multiple layers of security controls. Configuration management represents a critical component of overall security posture.

Detection and response capabilities require comprehensive monitoring for authentication services. Security logging must be implemented for all network services providing authentication capabilities. Anonymous access attempts should trigger immediate security alerts. Baseline behavioural analytics would detect anomalous FTP usage patterns and unauthorised file access activities.

Security architecture considerations include network segmentation to limit exposure of vulnerable services. Principle of least privilege must apply to file system permissions across all services. Encryption requirements should be mandatory for all data transmission protocols. Secure-by-default configurations prevent common misconfigurations that lead to security vulnerabilities.

---

15. Strategic Recommendations and Future Planning

Organisations maintaining similar legacy services face significant exposure to unauthorised access, data breaches, and compliance violations. The assessment confirms that basic security misconfigurations can result in complete system compromise by adversaries with minimal technical capabilities and standard network utilities.

Legacy FTP services configured with anonymous authentication represent a critical security vulnerability requiring immediate remediation. Organisations must prioritise migration to secure alternatives including SFTP and FTPS while implementing comprehensive security controls encompassing authentication enforcement, encryption requirements, access controls, and continuous monitoring capabilities.

The engagement successfully demonstrated practical exploitation of common FTP misconfigurations within a controlled training environment. Knowledge gained through this exercise provides valuable insights for defensive security implementations and security awareness training development. The systematic approach and comprehensive documentation serve as reference materials for future security assessments and training initiatives.

End of Report