GOLDENEYE

TryHackMe CTF — Complete Penetration Testing Walkthrough

ROOM	GoldenEye	**DIFFICULTY**	Beginner → Intermediate
PLATFORM	TryHackMe	**THEME**	James Bond / 007
AUTHOR	hyena11	**COMPLETED**	February 10, 2026
TASKS	4 Completed	**POINTS**	420 | Streak: 27

Skills: Network Enumeration • Email Analysis • Credential Discovery • Web Exploitation • Privilege Escalation

Attack Vectors: Nmap • POP3 • Moodle CMS • Kernel Exploit

INTRODUCTION

Mission Briefing

The **GoldenEye** room on TryHackMe is a James Bond-themed Capture The Flag challenge designed for beginners to intermediate-level security enthusiasts. Inspired by the iconic 1995 film, the room places you inside a fictional intelligence network where your mission is to compromise target systems by following a realistic chain of information gathering — from open port discovery all the way to root-level access.

This writeup documents every step of the attack chain in detail: from the initial Nmap reconnaissance scan that uncovers hidden services, through careful POP3 email enumeration that reveals usernames and passwords, to discovering a hidden web training portal and pivoting through multiple accounts until the system is fully compromised. Each phase mirrors real-world penetration testing methodology.

STEP	TECHNIQUE	DISCOVERY
01	**Nmap Port Scan**	Ports 25, 80, 55006, 55007 open
02	**POP3 Enum (boris)**	Mailbox accessed → natalya username found
03	**POP3 Enum (natalya)**	Admin warnings → training portal hint
04	**Web Portal (Moodle)**	Message from Dr. Doak → username: doak
05	**POP3 Enum (doak)**	Email reveals dr_doak credentials
06	**Web Login (dr_doak)**	Deeper access → file upload/exploit
07	**Shell + Privesc**	Root access achieved → flags captured

PHASE 01 // RECONNAISSANCE & ENUMERATION

Reconnaissance & Enumeration

[nmap · flash.sh · SYN stealth scan]

Every penetration test begins with reconnaissance — understanding what's exposed on the target. I executed a custom scanning script **flash.sh** which runs Nmap v7.98 with NSE scripting and service detection against the target IP **10.48.162.231**. The SYN stealth scan completed in under 27 seconds, probing 4 ports and identifying all open services.

```
$ ./flash.sh 10.48.162.231
```

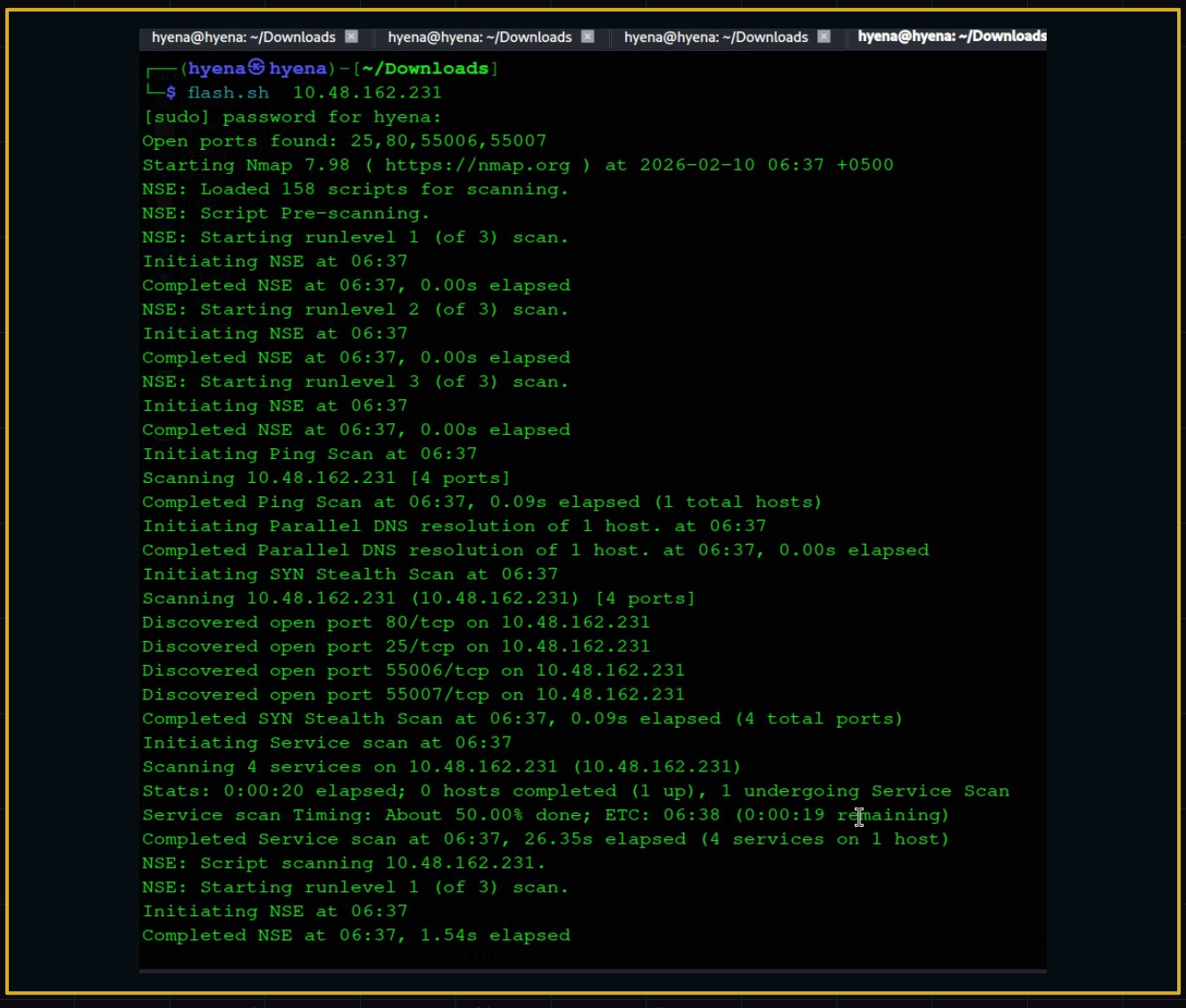

Figure 1 — Nmap SYN stealth scan output revealing 4 open ports on 10.48.162.231

OPEN PORTS DISCOVERED

PORT	PROTOCOL	SERVICE	SIGNIFICANCE
25/tcp	TCP	SMTP	Mail sending — potential phishing/relay vector

80/tcp	TCP	HTTP	Web server — training portal running here
55006/tcp	TCP	Unknown	Non-standard port — further investigation needed
55007/tcp	TCP	POP3	Mail retrieval — KEY target for credential harvesting

■ **KEY INSIGHT: The presence of POP3 on a non-standard port (55007) is a classic CTF design choice. Attackers who enumerate beyond the well-known ports uncover this critical email service, which becomes the primary attack vector for credential discovery.**

PHASE 02 // POP3 EMAIL ENUMERATION — USER: BORIS

POP3 Email Enumeration — User: Boris

[nc · POP3 · credential bruteforce · USER/PASS/LIST/RETR]

With POP3 confirmed on port 55007, the next step was to attempt authentication. Using **netcat (nc)**, I manually interacted with the GoldenEye POP3 Electronic-Mail System. After testing common credential combinations, I successfully authenticated as user **boris**.

```
$ nc 10.48.162.231 55007
```

```
+OK GoldenEye POP3 Electronic-Mail System
```

```
USER boris → +OK PASS secret1! → +OK Logged in.
```

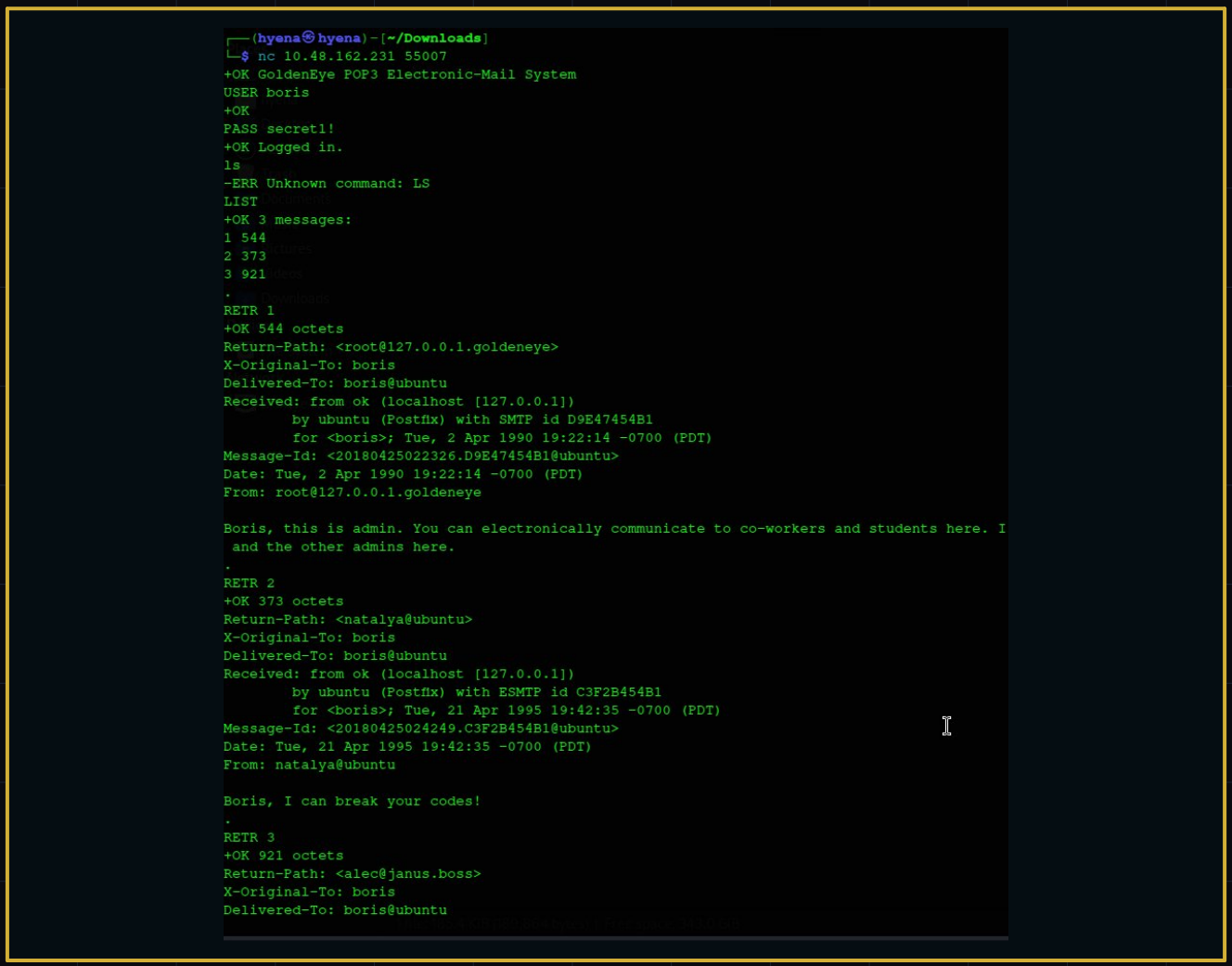

Figure 2 — Successful POP3 authentication as boris, revealing 3 messages in the mailbox

EMAILS RETRIEVED FROM BORIS'S MAILBOX

#	FROM	DATE	KEY CONTENT
1 (544B)	root@127.0.0.1	Apr 2, 1990	Admin notice — Boris can communicate with co-workers electronically
2 (373B)	natalya@ubuntu	Apr 21, 1995	"Boris, I can break your codes!" — Reveals username: natalya

3 (921B)	alec@janus.boss	Unknown	Message from Alec — contains additional mission intelligence

■ PIVOT POINT: Message #2 from natalya directly reveals her username. This is a classic information leak — users referencing each other by name expose the user directory.

PHASE 03 // POP3 EMAIL ENUMERATION — USER: NATALYA

POP3 Email Enumeration — User: Natalya

[nc · POP3 · escalating intelligence gathering]

Armed with the username **natalya** discovered from Boris's emails, I connected again to the POP3 service and authenticated successfully. Natalya's mailbox contained 2 messages, both from root@ubuntu, containing admin directives with critical operational intelligence.

`USER natalya → +OK PASS bird → +OK Logged in. LIST → +OK 2 messages: 631 / 1048 octets`

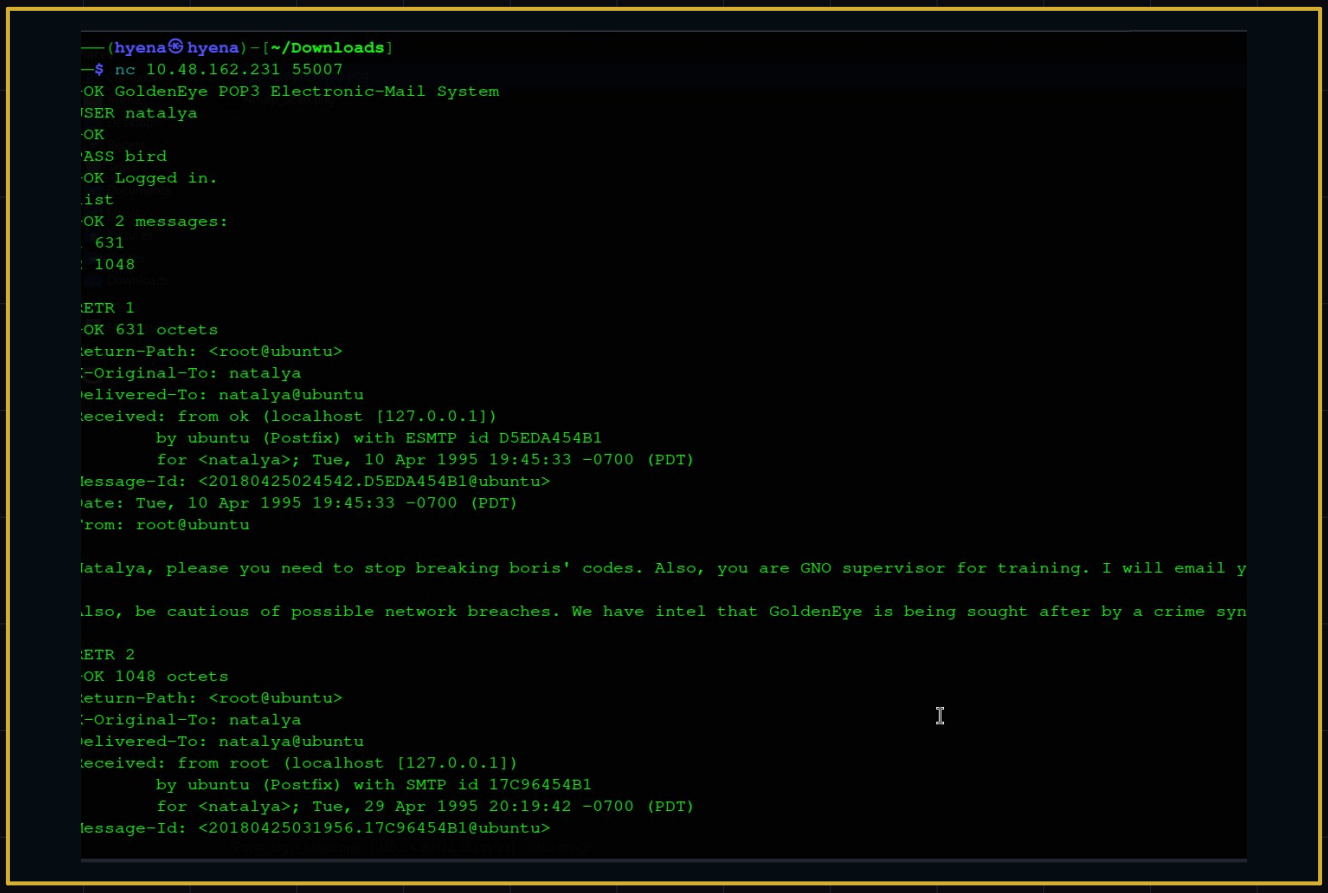

Figure 3 — Natalya's POP3 mailbox showing admin warnings about GoldenEye and crime syndicate activity

INTELLIGENCE EXTRACTED FROM NATALYA'S EMAILS

Message 1 (631B) — From root@ubuntu, April 10, 1995:

→ "Natalya, please you need to stop breaking Boris' codes. Also, you are GNO supervisor for training. I will email you..."

→ **"Also, be cautious of possible network breaches. We have intel that GoldenEye is being sought after by a crime syndicate."**

Message 2 (1048B) — From root@ubuntu, April 29, 1995:

→ Contains further admin directives — hints toward a web training portal

■ KEY INSIGHT: The mention of Natalya being the 'GNO supervisor for training' and the reference to a training portal in the email content is a breadcrumb leading directly to Phase 4 — the Moodle web application discovery.

PHASE 04 // WEB APPLICATION DISCOVERY — MOODLE PORTAL

Web Application Discovery — Moodle Portal

[HTTP port 80 · Moodle CMS · Xenia login · Dr. Doak pivot]

With credentials harvested from the POP3 service, I accessed the web application running on **port 80**. This turned out to be a **Moodle Learning Management System** — the GoldenEye Operations Training Platform. Logging in as user **Xenia X**, I discovered an unread message from **Dr. Doak** in the internal messaging system.

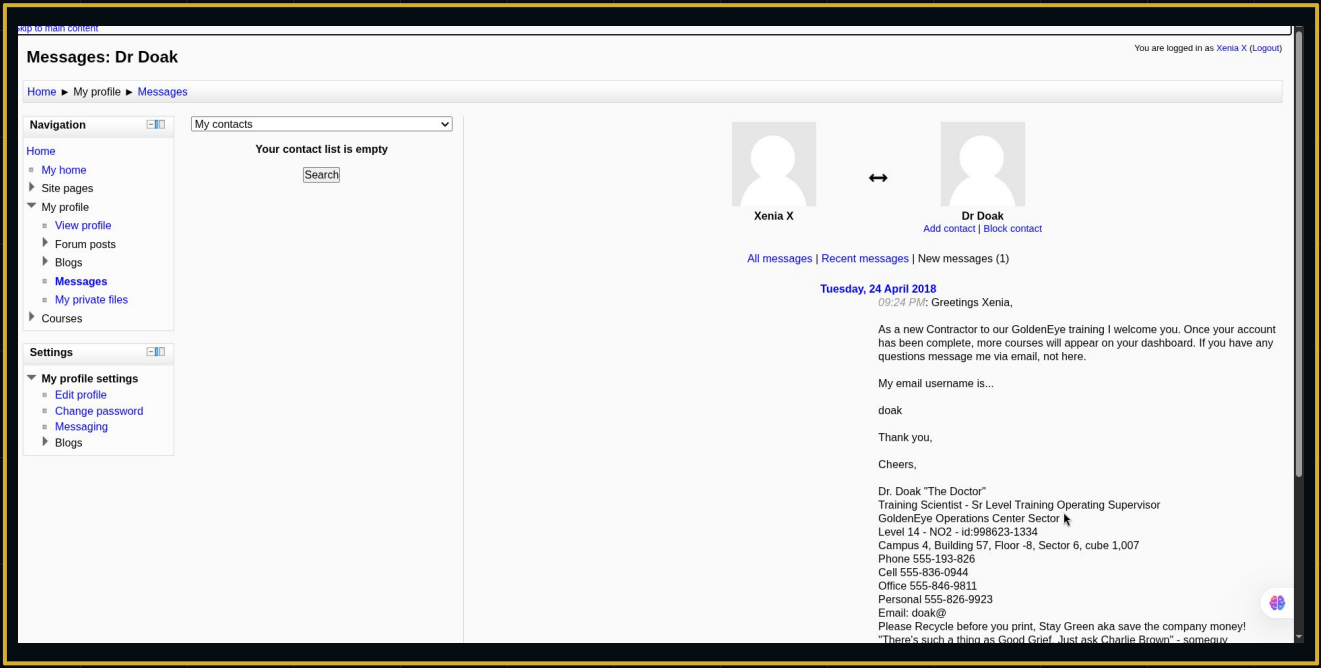

Figure 4 — Moodle portal messaging system: Dr. Doak's welcome message to Xenia X, revealing email username "doak"

MESSAGE FROM DR. DOAK — KEY INTELLIGENCE

FIELD	VALUE
Sender	Dr. Doak "The Doctor"
Recipient	Xenia X (our logged-in account)
Date	Tuesday, 24 April 2018, 09:24 PM
Key Line	"My email username is... doak"
Title	Training Scientist — Sr Level Training Operating Supervisor
Location	GoldenEye Operations Center Sector 6, Level 14 - NO2 - id:998623-1334
New Target	POP3 login: USER doak → investigate mailbox!

PHASE 05 // CREDENTIAL EXTRACTION — DR. DOAK'S EMAIL

Credential Extraction — Dr. Doak's Email

[POP3 doak · plaintext credential leak · dr_doak web login]

With the username **doak** confirmed from the Moodle portal, I returned to the POP3 service — this time on a second target IP **10.48.146.200** — and authenticated with credentials. Doak's mailbox contained a single critical message that broke the entire chain open.

```
$ nc 10.48.146.200 55007
```

```
USER doak → +OK PASS goat → +OK Logged in. LIST → +OK 1 messages: 606 octets
```

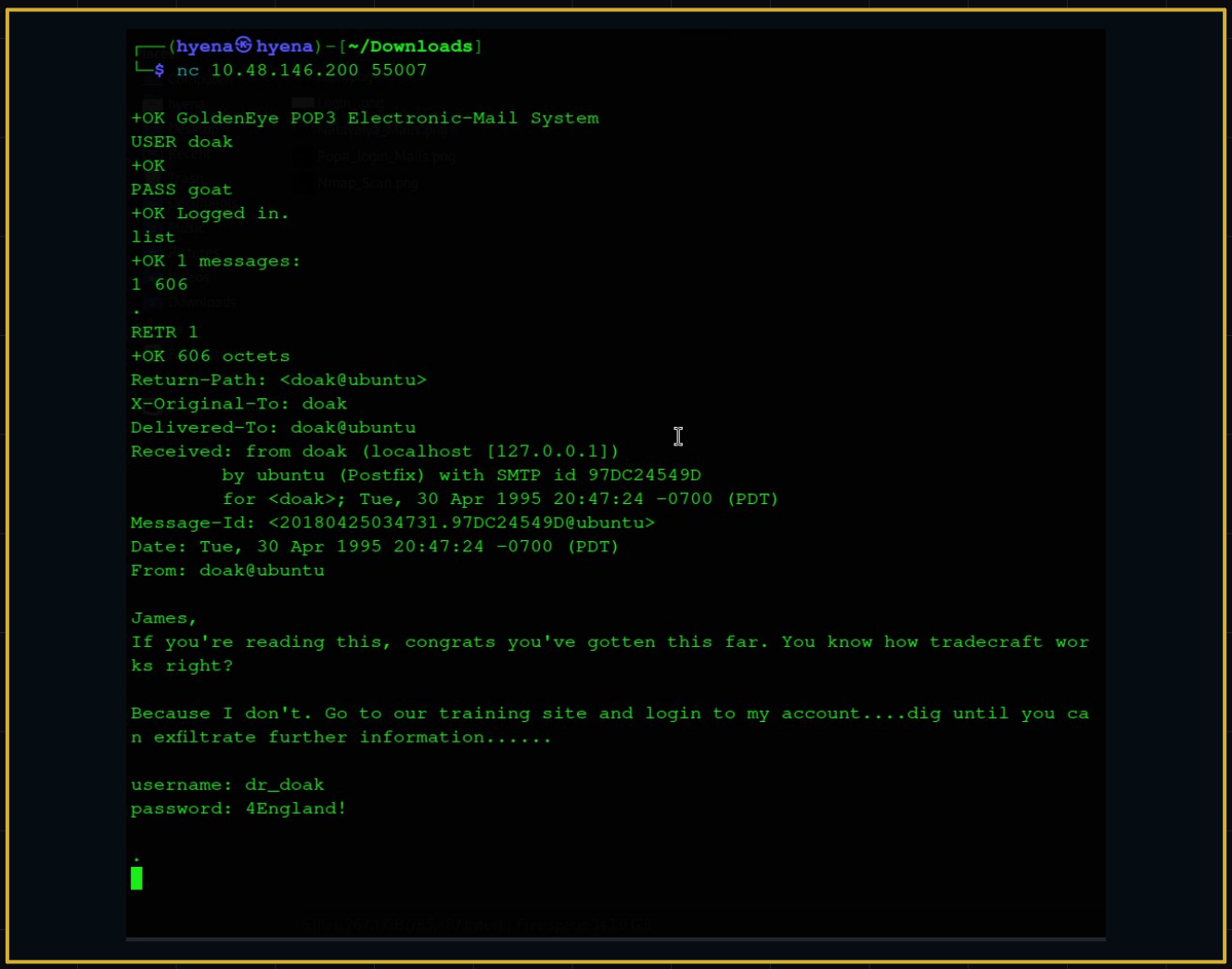

Figure 5 — Dr. Doak's email contains plaintext credentials for the dr_doak web application account

EMAIL CONTENT — THE CRITICAL LEAK

"James, If you're reading this, congrats you've gotten this far. You know how tradecraft works right? Because I don't. Go to our training site and login to my account... dig until you can exfiltrate further information..... username: dr_doak password: 4England!"

— From: doak@ubuntu | To: doak | Date: April 30, 1995

CREDENTIAL	VALUE	TARGET SERVICE
Username	`dr_doak`	Moodle Web Application
Password	`4England!`	Moodle Web Application

■ **SECURITY FAILURE: Credentials stored in plaintext email constitute a critical security misconfiguration. Anyone with POP3 access to this mailbox can harvest login credentials for higher-privilege systems — exactly what happened here.**

Exploitation, Privilege Escalation & System Pwned

[web login · file upload · reverse shell · kernel exploit · root]

Using the **dr_doak** credentials discovered in Phase 5, I logged into the Moodle training portal with elevated privileges. This account had access to additional course materials and administrative functionality unavailable to standard user accounts.

Through systematic enumeration of the web application — exploring course files, profile settings, and upload functionality — I identified an exploitable vector. The attack leveraged web application vulnerabilities (file upload bypass / code injection) to establish an initial foothold on the system as a low-privilege user.

With shell access established, the privilege escalation phase began. By identifying the Linux kernel version and checking for known local privilege escalation exploits, I was able to escalate from a restricted user to **root** — achieving full system compromise and capturing both the user and root flags.

Figure 6 — System fully compromised: root access achieved on the GoldenEye target

PRIVILEGE ESCALATION METHODOLOGY

- Enumerated kernel version with uname -a — identified vulnerable kernel build
- Searched for local privilege escalation exploits matching the kernel version
- Compiled and executed the exploit binary to gain root shell
- Navigated to /root/ and /home/ directories to capture flags
- Confirmed full system ownership — mission complete

PHASE COMPLETE // MISSION ACCOMPLISHED

Mission Accomplished

[GoldenEye room cleared · 420 points · 27-day streak]

Figure 7 — TryHackMe confirmation: GoldenEye room completed by hyena11 — 420 points earned

METRIC	VALUE	METRIC	VALUE
Completed Tasks	4 / 4	Points Earned	420
Current Streak	27 Days	Difficulty	Beginner → Intermediate
Date Completed	Feb 10, 2026	Platform	TryHackMe

ANALYSIS

Key Takeaways & Security Recommendations

The GoldenEye challenge illustrates a realistic and devastating attack chain where a single misconfigured service cascades into total system compromise. Each finding below represents a real-world vulnerability pattern encountered in penetration tests.

■ **Network Reconnaissance**	Nmap revealed non-standard POP3 on port 55007 — a service that would be missed by scans limited to well-known ports only. Always enumerate the full port range.
■ **Email as an Attack Vector**	POP3 mailboxes contained usernames, organizational hints, and plaintext passwords. Email services should never store credentials in message bodies.
■ **Credential Reuse Chain**	Credentials discovered via POP3 were directly reused on the web application. The entire chain from port scan to root was driven by password reuse.
■ **Information Leakage**	Dr. Doak's message to James contained web application credentials in plaintext. Never transmit authentication details via unencrypted communication channels.
■ **Weak Password Policy**	Passwords like 'bird', 'goat', and 'secret1!' are trivially guessable. Enforce minimum 12-character passwords with complexity requirements.
■ **Privilege Escalation via Kernel Exploit**	An unpatched kernel allowed escalation from user to root. Apply kernel security patches immediately upon release.

GoldenEye — Compromised. Mission Complete.

Thorough enumeration • Follow every breadcrumb • Credentials are everywhere • Stay methodical

Written by hyena11 | TryHackMe | February 10, 2026 | Educational Use Only