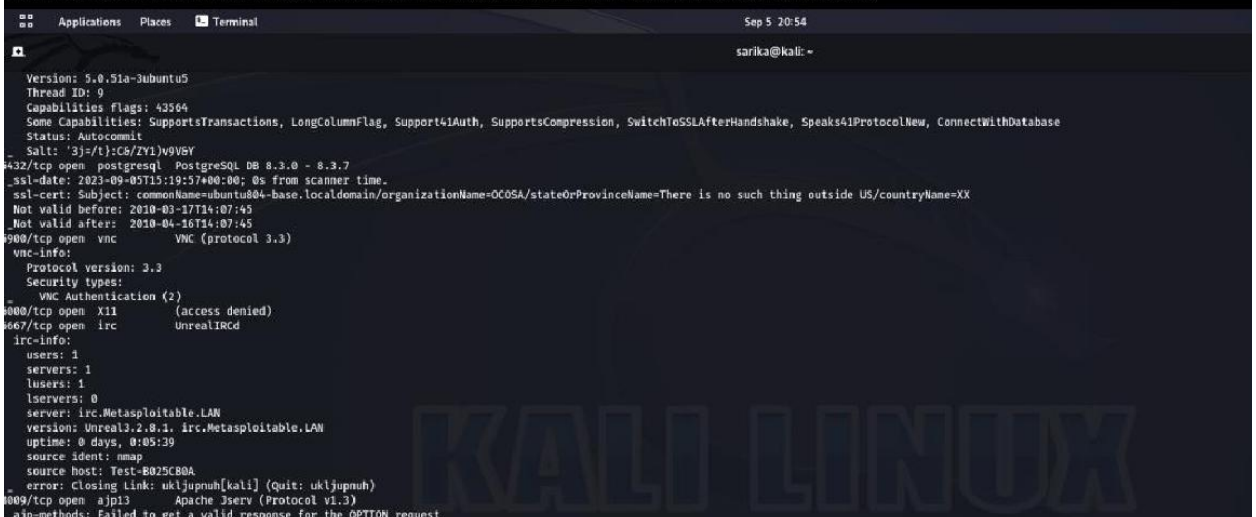
Assignment 2

Penetration Tools in Kali Linux

Sarika V

Nmap


Applications Places Terminal Sep 5 20:53
sarika@kali: ~
| SSL2_DES_64_CBC_WITH_MD5
| SSL2_DES_192_EDE3_CBC_WITH_MD5
| SSL2_RC2_128_CBC_WITH_MD5
| SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_ SSL2_RC4_128_EXPORT40_WITH_MD5
|_ssl-date: 2023-09-05T15:19:57+00:00; 0s from scanner time.
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) DAV/2)
|_http-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp open rpcbind 2 (RPC #100000)
| rpcinfo:
| program version port/proto service
| 100000 2 111/tcp rpcbind
| 100000 2 111/udp rpcbind
| 100003 2,3,4 2049/tcp nfs
| 100003 2,3,4 2049/udp nfs
| 100005 1,2,3 34133/udp mountd
| 100005 1,2,3 53970/tcp mountd
| 100021 1,3,4 34020/udp nlockmgr
| 100021 1,3,4 59339/tcp nlockmgr
| 100024 1 54150/tcp status
|_ 100024 1 54329/udp status
139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp open exec?
513/tcp open login OpenBSD or Solaris rlogind
514/tcp open shell?
| fingerprint-strings:
| NULL:
|_ Couldn't get address for your host (kali)
1099/tcp open java-rmi GNU Classpath grmiregistry
1524/tcp open bindshell Metasploitable root shell
2049/tcp open nfs 2-4 (RPC #100003)
2121/tcp open ftp ProFTPD 1.3.1
3306/tcp open mysql MySQL 5.0.51a-3ubuntu5
| mysql-info:
| Protocol: 10
| Version: 5.0.51a-3ubuntu5
| Thread ID: 9
| Capabilities flags: 43564
| Some Capabilities: SupportsTransactions, LongColumnFlag, Support41Auth, SupportsCompression, SwitchToSSLAfterHandshake, Speaks41ProtocolNew, ConnectWithDatabase
| Status: Autocommit
|_ Salt: '3j=/t}:C6/ZY1)v9V&Y
5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: 2023-09-05T15:19:57+00:00; 0s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX


Applications Places Terminal Sep 5 20:54
sarika@kali: ~
Version: 5.0.51a-3ubuntu5
Thread ID: 9
Capabilities flags: 43564
Some Capabilities: SupportsTransactions, LongColumnFlag, Support41Auth, SupportsCompression, SwitchToSSLAfterHandshake, Speaks41ProtocolNew, ConnectWithDatabase
Status: Autocommit
_ Salt: '3j=/t}:C6/ZY1)v9V&Y
5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7
_ssl-date: 2023-09-05T15:19:57+00:00; 0s 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
5900/tcp open vnc VNC (protocol 3.3)
vnc-info:
Protocol version: 3.3
Security types:
_ VNC Authentication (2)
6000/tcp open X11 (access denied)
6667/tcp open irc UnrealIRCd
irc-info:
users: 1
servers: 1
lusers: 1
lservers: 0
server: irc.Metasploitable.LAN
version: Unreal3.2.8.1. irc.Metasploitable.LAN
uptime: 0 days, 0:05:39
source ident: nmap
source host: Test-B025CB0A
_ error: Closing Link: ukljupnuh[kali] (Quit: ukljupnuh)
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-server-header: Apache-Coyote/1.1
_http-title: Apache Tomcat/5.5
_http-favicon: Apache Tomcat
service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port514-TCP:V=7.94%I=7%D=9/5%Time=64F746D5%P=x86_64-pc-linux-gnu%r(NULL
SF:,2B,"\x01Couldn't\x20get\x20address\x20for\x20your\x20host\x20\(kali\)\
SF:n");
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
Host script results:
smb-security-mode:
account_used: guest
authentication_level: user
challenge_response: supported
_ message_signing: disabled (dangerous, but default)
_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
smb2-time: Protocol negotiation failed (SMB2)

ftp service version: vsftpd 2.3.4
Vulnerabilitites of using the version:
VSFTPD v2.3.4 Backdoor Command Execution
Description
This module exploits a malicious backdoor that was added to the VSFTPD download archive. This backdoor was introduced into the vsftpd-2.3.4.tar.gz archive between June 30th 2011 and July 1st 2011 according to the most recent information available. This backdoor was removed on July 3rd 2011.
On analyzing the server status, the control connection is plain text, which means it is not encrypted and can be easily read by anyone who can access the packets.

Ssh version OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
SSH User Code Execution
This module connects to the target system and executes the necessary commands to run the specified payload via SSH. If a native payload is specified, an appropriate stager will be used.

telnet version Linux telnetd
Linux BSD-derived Telnet Service Encryption Key ID Buffer Overflow
This module exploits a buffer overflow in the encryption option handler of the Linux BSD-derived telnet service (inetutils or krb5-telnet). Most Linux distributions use NetKit-derived telnet daemons, so this flaw only applies to a small subset of Linux systems running telnetd.

MySQL version

MySQL < 5.0.51a / 5.1.23 / 6.0.4 Multiple vulnerabilities

An attacker may be able to cause the federated handler and daemon to crash when the federated engine issues a SHOW TABLE STATUS LIKE query by having a malicious server return a response with less than 14 columns.
(MySQL bug #29801 / CVE-2007-6304)
It fails to update the DEFINER value of a view when that is altered, which could allow an authenticated user to gain additional access through the ALTER VIEW. (MySQL bug #29908 / CVE-2007-6303)

Solution

Upgrade to MySQL version 5.0.51a / 5.1.23 / 6.0.4 or later.

Password cracking

1. Single-crack mode

John takes a string and generates variations of that string to generate set of passwords.
Ex, if username is “stealth” and password id “StEaLtH”, we use single mode of John to generate password variations (STEALTH, Stealth, Stealth,….).

```
stealth:d776dd32d662b8efbdf853837269bd725203c579
```

“format” flag is used to specify hash type and “single” flag to let John know we want to use single crack mode. Create Text.txt with username and hash value of password.

```
$ john --single --format=raw-sha1 crack.txt
```

```
└─$ cat Test.txt
stealth:d776dd32d662b8efbdf853837269bd725203c579


┌──(sarika㉿kali)-[~/Desktop]
└─$ john --single --format=raw-sha1 Test.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-SHA1 [SHA1 256/256 AVX2 8x])
Warning: no OpenMP support for this hash type, consider --fork=3
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 4 candidates buffered for the current salt, minimum 8 needed for performance.
StEaLtH          (stealth)
1g 0:00:00:00 DONE (2023-09-06 13:41) 100.0g/s 36800p/s 36800c/s 36800C/s StEaLtH..stealh
Use the "--show --format=Raw-SHA1" options to display all of the cracked passwords reliably
Session completed.
```

2. Dictionary mode

We provide John with list of passwords. John generates hashes for these on fly and compare with password hash. Create a wordlist, (generally collected using info about user). John will generate hashes for these on fly and compare them with password hash.

In Kali, you can find it at /usr/share/wordlists/rockyou.txt. We will also have a crack.txt file with just the password hash.

```
edba955d0ea15fdef4f61726ef97e5af507430c0
```

```
$ john --wordlist=/usr/share/wordlists/rockyou.txt --format=raw-sha1 crack.txt
```

```
┌──(sarika㉿kali)-[~/Desktop]
└─$ echo "edba955d0ea15fdef4f61726ef97e5af507430c0" > crackdict.txt

┌──(sarika㉿kali)-[~/Desktop]
└─$ john --wordlist=../wordlist.txt --format=raw-sha1 crackdict.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-SHA1 [SHA1 256/256 AVX2 8x])
Warning: no OpenMP support for this hash type, consider --fork=3
Press 'q' or Ctrl-C to abort, almost any other key for status
password5        (?)
1g 0:00:00:00 DONE (2023-09-06 14:04) 50.00g/s 1550p/s 1550c/s 1550C/s j..hb
Use the "--show --format=Raw-SHA1" options to display all of the cracked passwords reliably
Session completed.
```

3. Incremental mode

Incremental mode is the most powerful mode provided by John. It tries all possible character combinations as passwords. The cracking can go on for a long time if the password is too long or if it's a combination of alphanumeric characters and symbols. This mode is rarely used, a combination of Social Engineering attacks and wordlist mode will help you crack most of the hashes.

```
$ john -i:digits passwordfile.txt
```