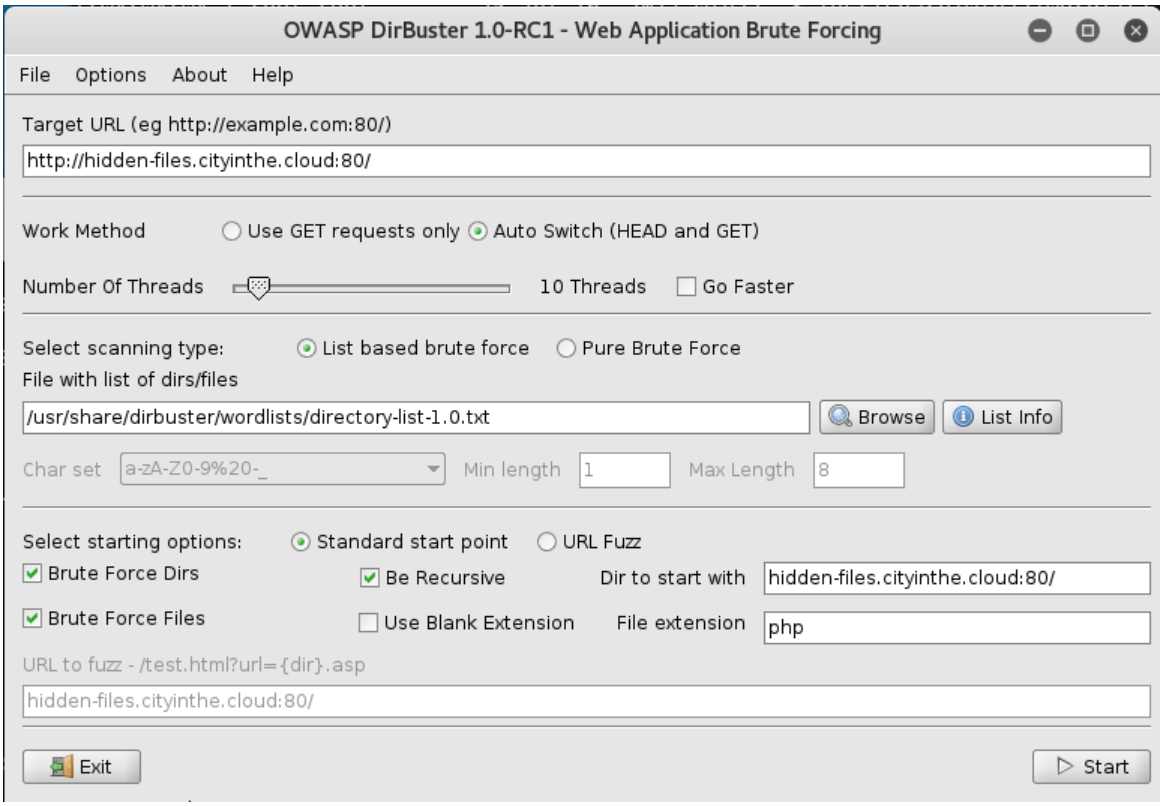
# CS5781 Special Project 2024 (due Nov 18 – Dec 4, 2024) ver1.7

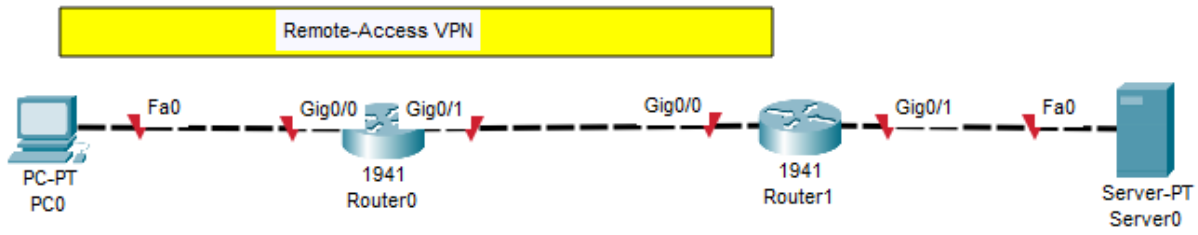
Each group (up to 3 students) is to do any one of the following projects or propose a security-related project that has not been assigned to another group (check with instructor). The deliverable report shall comprise of a 10 to 15-minute Zoom presentation describing the installation, configuration, and live demonstration of the working project. Projects already assigned will be marked with red **X.** Projects that are still available will be marked **O**.

1. **X** Describe and demonstrate how you can use aircrack-ng program to crack WEP and WPA/WPA2-PSK keys of WiFi traffic.
2. **X** Demonstrate how any of the Kali password attack tools can be used to successfully crack a Microsoft Windows server and Linux server user account password files.
3. **X** Demonstrate how any of the Kali reverse engineering tools can be used to reverse engineer an executable file.
4. **X** Configure 2-factor authentication on any server and demonstrate how login requires user credentials and another form of authentication.
5. **X** Show how Amazon AWS security features can be used to secure access to a server hosted on Amazon AWS
6. **X** Show how Microsoft Azure security features can be used to secure access to a server hosted on Microsoft Azure.
7. **X** Discuss how various anonymous messaging app(s) are architected to bypass government surveillance. Provide a demonstration of one such app.
8. **X** Install and configure Samba service on Kali VM and demonstrate how files can be easily shared between Windows OS and Kali VM.
9. **X** Set up a Honeypot server to monitor malicious activity
10. **X** Log Snort output to MySQL database and query database via ACID
11. **X** Configure a Apache web server to support SSL protocol ( http://www.apache-ssl.org ) for secure communication between a web browser and web server. Generate a server certificate and install onto web server.
12. **X** Set up demonstrate how PGP (Pretty Good Privacy) can be use to encrypt and decrypt email.
13. **O** Set up a Kerberos server (http://web.mit.edu/kerberos/www/ ) and demonstrate how it is used in authentication
14. **O** Set up a firewall using Linux Ipchains/iptables with 2 network interfaces
15. Set up a Cisco switch that can support 802.1x port authentication via a RADIUS server. Verify by connecting a client computer whose network interface is configured to use 802.1x user authentication.
16. **X** Show how Volatility tool can be used for conducting memory forensics analysis
17. **X** Run dirbuster (installed on Kali) to perform brute force attack against a web server such as http://hidden-files.cityinthe.cloud to find listing of valid folders on web server using one

of dirbuster's wordlists containing popular folder names.




18. X Use Cisco Packet Tracer to demonstrate how a computer can use a vpn client software application to remotely establish a IPSec VPN tunnel to a company's border router and access an internal server. Show vpn-related configuration settings on PC0 and Router1. To show that VPN connection is up, run command (i) "ipconfig /all" and tracert to server0 on PC0, (ii) "show isakmp sa" and "show ipsec sa" on Router1.




19. X Install and configure a Rootkit and demonstrate how it hides existence of files, processes, and open TCP ports. Describe and demonstrate techniques that can be used to detect that a system has been rootkitted.

20. X Since the use of usernames and passwords can be compromised, discuss the use of passwordless authentication as an alternative and provide a live demo of its use.

21. X Explain how the architecture of Bitcoin addresses various security concerns, such as authentication, confidentiality, data integrity, and non-repudiation. Provide a demonstration showing the ease of buying and selling Bitcoins.

22. X Discuss the architecture of Tor (the onion router) and how it supports anonymous communication. Provide a demonstration how the Tor browser can be used to access the Dark Web.

23. X Discuss and demonstrate how Wireshark can be used to capture and decode https traffic generated by a web browser and web server.

24. O Show how Mimikatz hacker tool can be used to steal clear-text user credentials.

25. O Explain how Eduroam works and provide screenshots, packet captures, and traceroute showing how you were able to (i) use your CalStateLA's user account credentials to connect and authenticate to another Eduroam member institution's wifi network, or (ii) connect to CalStateLA's "eduroam" SSID using credentials belonging to another university.

26. X Explain how single sign-on works and provide a live demonstration how user authentication to two separate applications can be achieved by having user provide credentials only once.

27. O Install Cisco ASA firewall binary executable onto GNS3 and show how Cisco ASA firewall can be configured and monitored using its graphical user interface in lieu of command line interface.

28. X Discuss how you are able to solve a challenging question in each of the following four modules within NCL Fall 2024 Gymnasium: forensics, wireless access exploitation, and web application exploitation.

29. O Explain how RadSec is more secure than Radius. Show how to set up a RadSec server such as freeRADIUS (https://www.freeradius.org/documentation/freeradius-server/3.2.7/howto/protocols/proxy/enable_radsec.html ) and configure a test RadSec client. Capture and decode RadSec packets.

30. O Propose a security related project that is acceptable to instructor.