Cyber Warriors: A Comprehensive Introduction to Cybersecurity Tools and Techniques

June 24-28, 2024

Murtuza Jadliwala

murtuza.jadliwala@utsa.edu

SPrITE LAB

UTSA

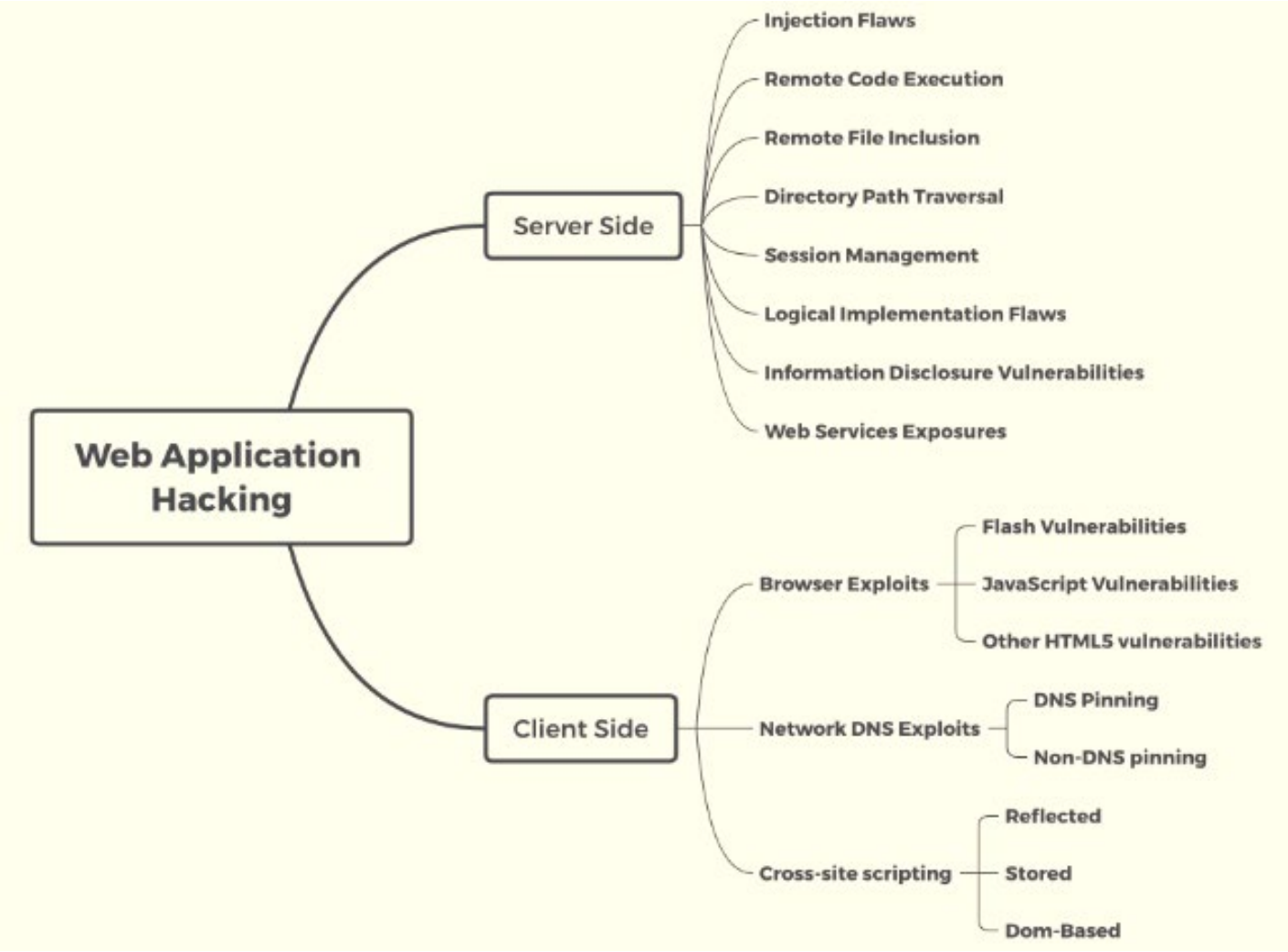
NSF

Introduction to Web & Internet Security

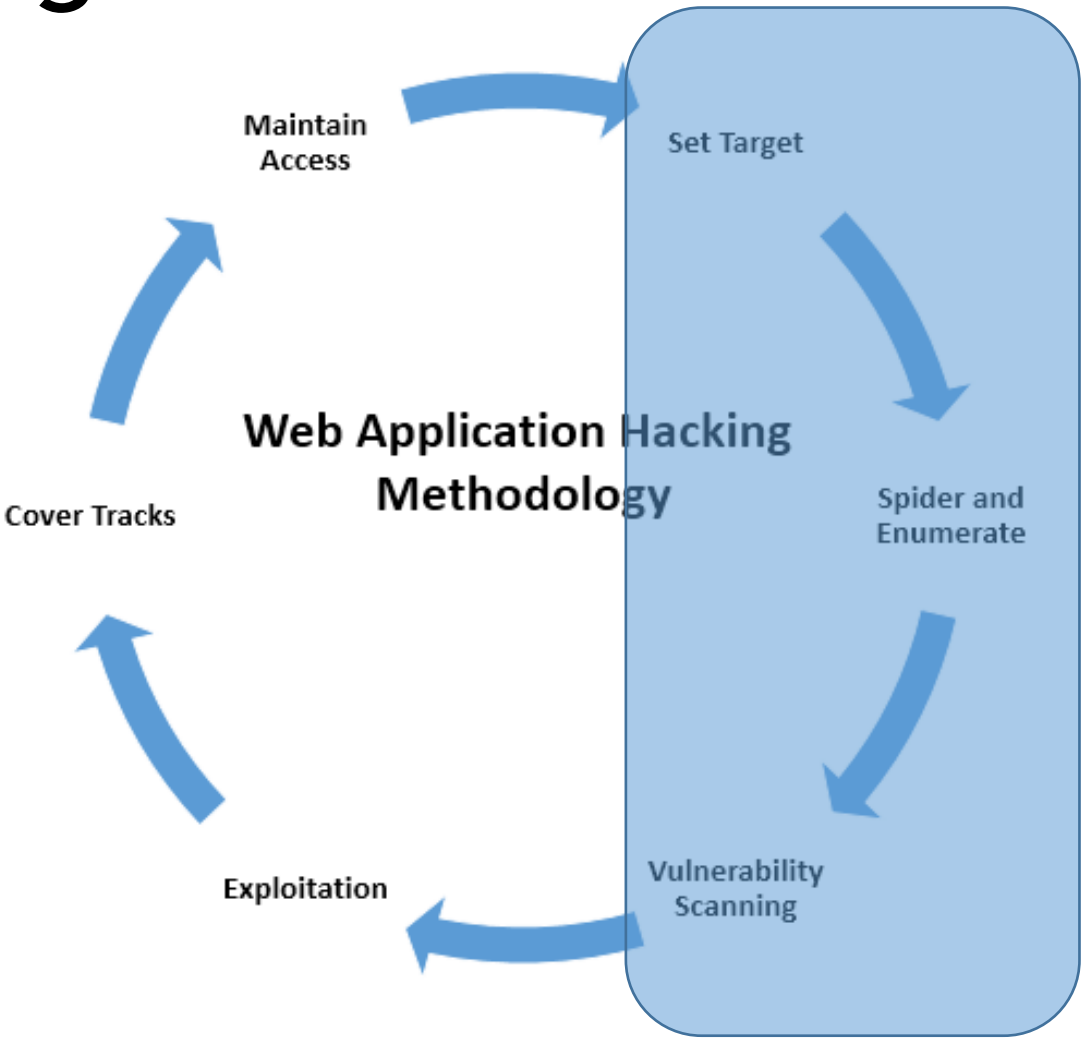
Web Applications

- Web applications are complex Internet services which employ a multi-tiered architecture involving multiple servers:
  - Application and web servers (public facing).
  - Middleware services, backend and data servers (on the internal network).
- Given the complexity of web services, it is important for a hacker or pen-tester to adapt to each site's specific architecture and service parameters.
  - Testing process must also be consistent to ensure that nothing is missed.

Categories of Web Application Hacks



Reconnaissance and Vulnerability Scanning



Reconnaissance and Vulnerability Scanning

- Specific activities related to web application reconnaissance include:
  - Identifying **where and how the target web app** is hosted.
  - Enumerating **target site directory structure** and content management system (CMS), if used, by spidering and offline analysis.
  - Identifying the **authentication and authorization mechanisms** and determining how the session state is maintained during a transaction with that web service. This usually involves analysis of cookies and how they are used, utilizing a proxy tool.
  - Enumerating and evaluating all **forms**. As these are primary means for clients to input data and interact with the web service, they are the location of several exploitable vulnerabilities, such as, SQL/XML/JSON injection attacks and cross-site scripting.
  - Identifying **other areas that accept input**, such as pages that allow for file upload, as well as, any restrictions on accepted upload types.
  - Identifying how **errors are handled**, and the actual error messages that are received by a user; frequently, the error will provide valuable internal information such as the software version used, or internal filenames and processes.

Reconnaissance and Vulnerability Scanning

Detection of Web Application Firewall and Load Balancers

- Identification/Determination of the presence of network-based protective device
  - Imp
- WAFs
- The process of WAF detection can be automated using:

```
root@kali:~# nmap -p 80 --script http-waf-detect.nse www
Starting Nmap 7.70 ( https://nmap.org ) at 2018-12-23 11:10 EST
Stats: 0:00:41 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 0.00% done
Nmap scan report for
Host is up (0.28s latency).
Other addresses for www. (not scanned): 2404:
PORT   STATE SERVICE
80/tcp open  http
| http-waf-detect: IDS/IPS/WAF detected:
|_www.:80/?p4yl04d3=<script>alert(document.cookie)</script>

Nmap done: 1 IP address (1 host up) scanned in 45.61 seconds
```

nmap script http-wafdetect.nse

- The above nmap script identifies that a WAF is present or not; however, it may not always be accurate and the returned results may be too general to guide an effective strategy for firewall bypass.

Reconnaissance and Vulnerability Scanning

Detection of Web Application Firewall and Load Balancers

- Load balancing detector (or lbd) is a Bash shell script that determines whether a given domain uses DNS and/or HTTP load balancing.
- Important information, as it can explain seemingly anomalous results during pen-testing when the load balancer switches requests between multiple servers.
- lbd uses a variety of checks to identify the presence of load balancing.

```
root@kali:~# lbd www.[redacted].com

lbd - load balancing detector 0.4 - Checks if a given domain uses load-balancing.
                                    Written by Stefan Behte (http://ge.mine.nu)
                                    Proof-of-concept! Might give false positives.

Checking for DNS-Loadbalancing: FOUND
www.[redacted].com has address 10[redacted].25
www.[redacted].com has address 10[redacted].25

Checking for HTTP-Loadbalancing [Server]:
 cloudflare
 NOT FOUND

Checking for HTTP-Loadbalancing [Date]: 19:53:50, 19:53:51, 19:53:51, 19:53:51, 19:53:51, 19:53:51, 19:53:51, 19:53:51, 19
:53:51, 19:53:51, 19:53:52, 19:53:52, 19:53:52, 19:53:52, 19:53:52, 19:53:52, 19:53:52, 19:53:52, 19:53:53, 19:53:53, 19:5
3:53, 19:53:53, 19:53:53, 19:53:53, 19:53:53, 19:53:53, 19:53:54, 19:53:54, 19:53:54, 19:53:54, 19:53:54, 19:53:54, 19:53:
54, 19:53:54, 19:53:55, 19:53:55, 19:53:55, 19:53:55, 19:53:55, 19:53:55, 19:53:55, 19:53:55, 19:53:55, 19:53:56, 19:53:56
, 19:53:56, 19:53:56, 19:53:56, 19:53:56, 19:53:56, NOT FOUND

Checking for HTTP-Loadbalancing [Diff]: FOUND
< CF-RAY: 48dd6093b3f86a91-LHR
> CF-RAY: 48dd609463ee360e-LHR

www.[redacted].com does Load-balancing. Found via Methods: DNS HTTP[Diff]
```

Reconnaissance and Vulnerability Scanning

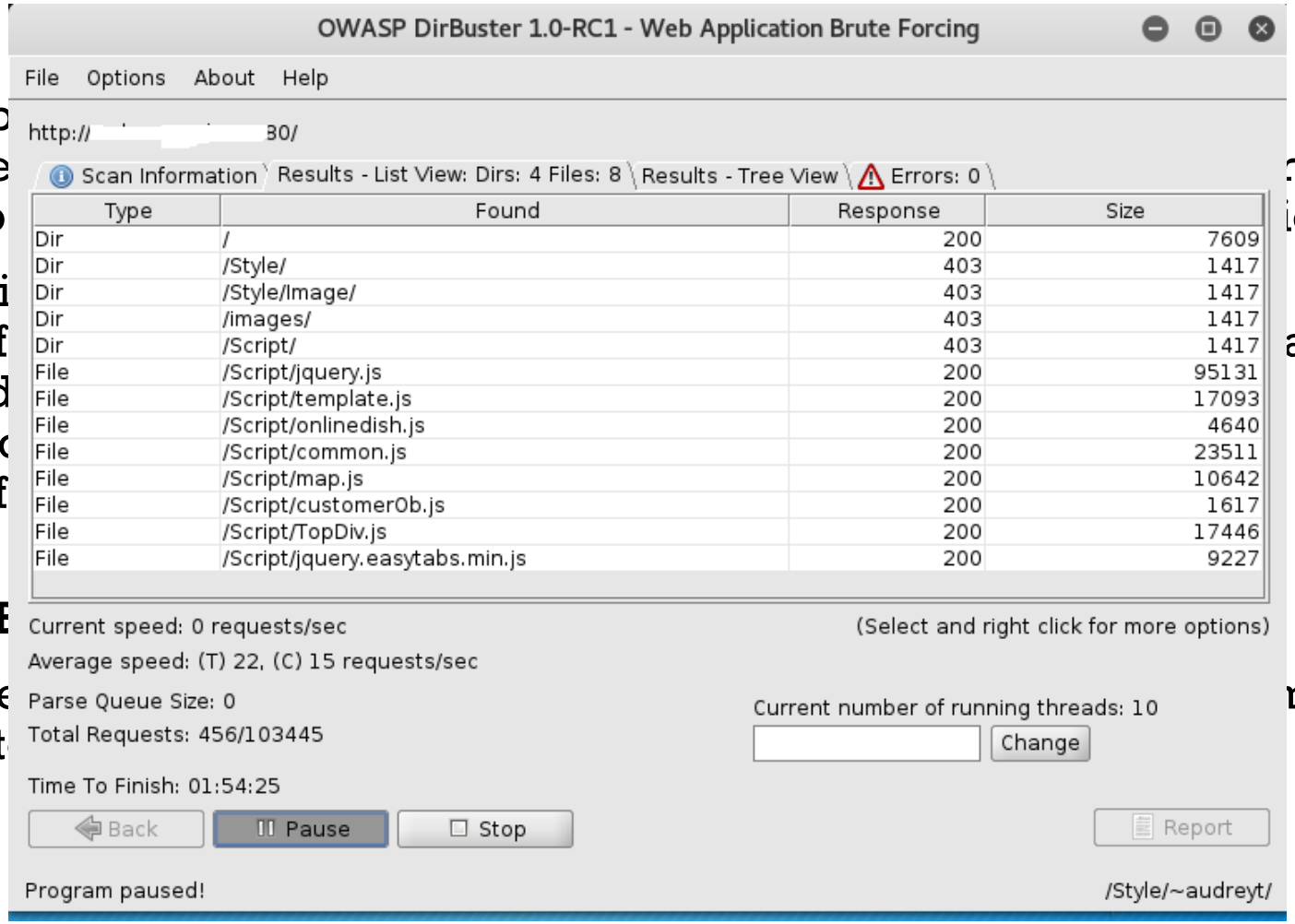
Fingerprinting a Web Application and CMS Detection

- Web Application Fingerprinting: Typically first task in reconnaissance & vulnerability scanning done to find out the version and type of the web server running the application, and the implemented web technologie
  - Allows at xploits.
- One way to nect to the victim host o identify what is bei
- This returns e of web server that ction providing d build the application
- The above information can be used in conjunction with a vulnerability database such as CVE to determine exploitable vulnerabilities: (see https://www.cvedetails.com/vulnerability-list/vendor_id-74/product_id-128/PHP-PHP.html).

```
root@kali:~# nc -vv 192.168.0.101 80
192.168.0.101: inverse host lookup failed: Unknown host
(UNKNOWN) [192.168.0.101] 80 (http) open
HEAD / HTTP/1.0
HTTP/1.1 400 Bad Request
Date: Sat, 15 Dec 2018 23:27:01 GMT
Server: Apache/2.4.37 (Win32) OpenSSL/1.0.2p PHP/5.6.39
Vary: accept-language,accept-charset
Accept-Ranges: bytes
Connection: close
Content-Type: text/html; charset=utf-8
Content-Language: en
Expires: Sat, 15 Dec 2018 23:27:01 GMT
```

Reconnaissance and Vulnerability Scanning

- Web
  dete
  web
- Typi
  conf
  hard
  struc
  conf
- Kali
  DirB
- For e
  brut



Reconnaissance and Vulnerability Scanning

Mirroring a Web Application

- Web Mirroring (Cloning) Applications: Automated crawling tools that make an offline copy of the website.
  - Cloned/downloaded contents of the target site can be used as input to a program such as crunch, which will produce a personalized word list to support password cracking.
- Kali provides an inbuilt application, httrack, which provides the option to download all the contents of a website to the local system.
- httrack is both a command-line and GUI utility. For example, the following command can be used on the terminal:

httrack http://targetwebapp/ -O outputfolder

```
root@kali:~# httrack http://192.168.0.24/vijay -O /root/chap7/
WARNING! You are running this program as root!
It might be a good idea to run as a different user
Mirror launched on Tue, 25 Dec 2018 08:10:27 by HTTrack Website Copier/3.49-2 [XR&CO'2014]
mirroring http://192.168.0.24/vijay with the wizard help..
Done.: 192.168.0.24/manual (282 bytes) - 404
Thanks for using HTTrack!
```

Reconnaissance and Vulnerability Scanning

Other Web Application Vulnerability Scanners on Kali

Application	Description
Arachnid	An open source Ruby framework that analyzes HTTP responses received during scanning to validate responses and eliminate false positives.
GoLismero	A scanner that maps web applications and detects common vulnerabilities. The results are saved in TXT, CVS, HTML, and RAW formats.
Nikto	A Perl-based open source scanner that allows IDS evasion and user changes to scanned modules. This original web scanner is beginning to show its age, and is not as accurate as some of the more modern scanners.
Skipfish	A scanner that completes a recursive crawl and dictionary-based crawl to generate an interactive site map of the targeted website, annotated with the output from additional vulnerability scans.
Vega	A GUI-based open source vulnerability scanner. As it is written in Java, it is cross-platform (Linux, macOS, and Windows) and can be customized by the user.
w3af	A scanner that provides both a graphical and command-line interface to a comprehensive Python testing platform. It maps a target website and scans for vulnerabilities. This project has been acquired by Rapid7, so there will be closer integration with the Metasploit framework in the future.
Wapiti	A Python-based open source vulnerability scanner.
Webscarab	OWASP's Java-based framework for analyzing HTTP and HTTPS protocols. It can act as an intercepting proxy, a fuzzer, and a simple vulnerability scanner.
Webshag	A Python-based website crawler and scanner that can utilize complex IDS evasion.
WebSploit	An advanced man-in-the-middle (MiTM) framework, useful in wireless and Bluetooth attacks.

Application-specific Attacks

Brute-forcing Access Credentials of a Web Application

- **What is a access authentication brute-force attack against a website or its services**?: Guessing username and password to access the website or service.
- This attack has a high success rate because users tend to select easy-to-remember credentials or reuse credentials, and also because system administrators frequently don't control multiple access attempts.
- Kali comes with hydra, a command-line tool, and hydra-gtk, which has a GUI

```
root@kali:~/chap7# hydra -l admin -P passlist.txt 192.168.0.101 http-post-form "/mutillidae/index.php?page=login.php:userr
ame=^USER^&password=^PASS^&login-php-submit-button=Login:Not Logged In"
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purp
oses.

Hydra (http://www.thc.org/thc-hydra) starting at 2018-12-23 15:11:02
[DATA] max 6 tasks per 1 server, overall 6 tasks, 6 login tries (l:1/p:6), ~1 try per task
[DATA] attacking http-post-form://192.168.0.101:80//mutillidae/index.php?page=login.php:username=^USER^&password=^PASS^&lo
gin-php-submit-button=Login:Not Logged In
[80][http-post-form] host: 192.168.0.101   login: admin   password: adminpass
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2018-12-23 15:11:18
```

```
hydra -l admin -P passlist.txt 192.168.0.101 http-post-form
"/mutillidae/index.php
page=login.php:username=^USER^&password=^PASS^&login-php-
submitbutton=Login:Not Logged In"
```

Application-specific Attacks

Injection Attacks: Command Injection in Web Applications

- Command Injection: Pass malicious "values" or "commands" to vulnerable web applications through HTTP Post method or as URL parameters. These malicious "commands" are then executed by the target OS (through the vulnerable web application) resulting in an privilege escalation or unauthorized access/execution!
  - Primarily caused due to insufficient input validation.
- **Command injection exploiter (commix)** is an automated tool written in Python (precompiled in Kali) used for testing command injection vulnerabilities in web applications.
- The command injection attacks are independent of the operating system in use. They can target Linux, Unix, and Windows as well. They are also independent of the programming languages used as they can inject themselves into many programming languages including C, C++, PHP, Python, and Java.

Application-specific Attacks

Injection Attacks: Command Injection in Web Applications

- Commix (https://github.com/commixproject/commix) also comes as an additional plugin in various penetration testing frameworks such as TrustedSec's Penetration Testers Framework (PTF) and OWASP's Offensive Web Testing Framework (OWTF).
- Attackers may use all the functionalities provided by commix by entering commix -h in the Terminal.
- Commix website has links to various test pwnable (compromisable) VMs and testbeds, usage examples and several cool demos!
- A useful demo of a command injection using commix: https://www.youtube.com/watch?v=A57pbJA706U

Questions