**Task Overview**: Develop a process to enumerate all external(public)-facing web servers on blue range

**Potential Task Tools**: NMAP, Vulnerability Scanner (OpenVAS, Nessus), Web Fuzzer (Nikto, OWASP ZAP, DirectoryBuster (DIRB), SQL Map, Hand Jammin’ )

1. **Discovery**
   1. [MITRE ATT&CK **T1595.001**](https://attack.mitre.org/techniques/T1595/001/) Perform light foot-printing on the IP ranges provided to determine what the public facing assets (web servers) are.
   2. nmap -sn x.x.x.x/xx -oA nmapdiscoveryscan | grep for | cut -d ‘ ‘ -f 5
      1. Outputs results in the top three formats for later artifacts, then outputs results to screen in an easy to interpret format.
      2. Copy the IP addresses identified into a target list called “targs”
   3. [MITRE ATT&CK **T1595.002**](https://attack.mitre.org/techniques/T1595/002/) Perform targeted fingerprinting on the devices we identify that are public facing
   4. nmap -Pn -sV -O -sC -iL targs -oA nmapservicescan
      1. Performs a scan on the “targs” list to identify services, operating system, default vuln scripts and outputs the content in the top three formats
   5. [MITRE ATT&CK **T1594**](https://attack.mitre.org/techniques/T1594/) search public facing websites for names of departments/divisions, physical locations, and data about key employees such as names, roles, and contact info. These sites may also have details highlighting business operations and relationships.
2. **Targeted Enumeration**
   1. [MITRE ATT&CK **T1595.002**](https://attack.mitre.org/techniques/T1595/002/) Target the web servers that we’ve identified and initiate differing levels of vulnerability analysis ( in order )
   2. **Nikto**
      1. Intent it to automate a vuln scan on the website and determine attack vector
      2. nikto -host <website url>
   3. **Owasp ZAP**
      1. Intent it to automate a vuln scan on the website and determine attack vector
         1. Use the GUI quick start and target the URLs
      2. ZAP will proceed to crawl the web application with its spider and passively scan each page it finds. Then ZAP will use the active scanner to attack all of the discovered pages, functionality, and parameters.
   4. **Directory Mapping**
      1. Intent it to look for interesting directories / files. Misplaced configuration files or backup files
      2. dirb <website url> /usr/share/wordlists/dirb/<what ever one you want>
         1. directory-list-2.3.-small.txt
   5. **Manual Testing**
      1. Look for comment boxes that allow html taggin <b> </b> these items may be vulnerable to XSS attacks and can run remote code
         1. <script> alert('XSS') </script>
      2. Typically the contacts page has boxes that can be filled out
3. **Exploiting Web Services**
   1. [MITRE ATT&CK **T1190**](https://attack.mitre.org/techniques/T1190/) At this point we’re targeting the information that we’ve gained and attempting to exploit weaknesses / misconfiguration identified in the web server
   2. **Authentication Brute Force** (If there is an authentication / admin CPANEL)
   3. **SQL Mapping** <if we have access OR find a web injection point>
      1. sqlmap -u <http:websiteurl>
   4. **OS Command Injection**
      1. Test to see if vulnerable to OS command injection. Sometimes the file names are in the URL. Perl allows piping (|) data from a process into an open statement.
      2. Example URL before alteration:

<http://sensitive/cgi-bin/userData.pl?doc=user1.txt>

Example URL modified:

<http://sensitive/cgi-bin/userData.pl?doc=/bin/ls|>

This will execute the command /bin/ls.

* 1. **File Upload Misconfiguration**

1. **Post Exploit Enumeration**
   1. System Owner/User Discovery
      1. [MITRE ATT&CK **T1033**](https://attack.mitre.org/techniques/T1033/) Use **whoami** to determine current user and state of admin privileges
      2. [MITRE ATT&CK **T1087.001**](https://attack.mitre.org/techniques/T1087/001/) Local accounts
         1. Get list of users on system using **net user**
         2. Use to get useful information about any particular user **net user <username>**
         3. The above shows a wide range of information such as password changing privileges, account expiration, last logon, when a password was last set, etc.
      3. [MITRE ATT&CK **T1087.002**](https://attack.mitre.org/techniques/T1087/002/) Domain accounts
         1. **net user /domain** will provide a list of domain accounts
         2. You can use this list of accounts as a dump / password spray
   2. [MITRE ATT&CK **T1069**](https://attack.mitre.org/techniques/T1069/001/) Permission Groups Discovery
      1. Local
         1. Use this to possibly identify permissions, ex. Admin privileges to users in the admin group. These users can now be targeted. Type **net localgroup** in the command line
      2. Domain
         1. Use this to possibly identify permissions, ex. Admin privileges to users in the admin group. These users can now be targeted. Type **net group /domain** in the command line
   3. [MITRE ATT&CK **T1018**](https://attack.mitre.org/techniques/T1018/) Remote System Discovery
      1. Execute lateral movement by discovering interconnected systems using **net view**. You can also use local host files ex. **C:\Windows\System32\Drivers\etc\hosts** or **\etc\hosts** to discover hostname to IP address mappings of remote systems.
   4. [MITRE ATT&CK **T1518**](https://attack.mitre.org/techniques/T1518/001/) Software Discovery: Security Software Discovery
      1. Attempt getting a list of security software, configs, defensive tools, etc, such as firewall rules and anti-virus, and shape follow-on behaviors.
      2. Possible commands: **netsh, reg query, dir**.
   5. [MITRE ATT&CK **T0183**](https://attack.mitre.org/techniques/T1083/) File and Directory Discovery
      1. Possible commands: **dir, tree, ls, find, locate**
         1. Use these to navigate the file system and look for potetntially damaging documents, personal, system, or network information that you can exploit
      2. Query remote systems for available shared drives using new view <path of the remote system>
      3. You can also do it locally using net share
   6. Use this to identify potential systems of interest and information pools. As well as potential systems for lateral movement
   7. Ports
      1. Enumerate active ports in windows cmd using **netstat –an**
      2. Use list of open ports to find potential exploits using Nmap Scripts
         1. **If you can download Nmap onto the windows OS -** Once ports are viewable search for the common usage of ports to run Nmap exploitation scripts in /usr/share/nmap/scripts. Common examples:
         2. **Port 80 – HTTP:** sudo nmap –script=http-vuln <IP address>
         3. **Port 135 – RPC:** sudo nmap –script=rpc <IP address>
         4. **Port 445 SMB:** sudo nmap –script=http-smb <IP address>
         5. In the event you get ports open in the range **49152 – 65535** they are usually private ports. If you have time, you can run all the scripts in the Nmap library to find potential vulnerabilities using **sudo nmap –script=vuln\***.