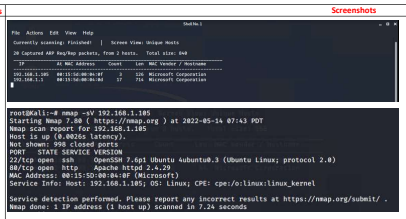
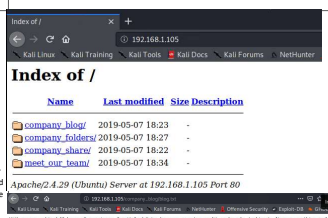
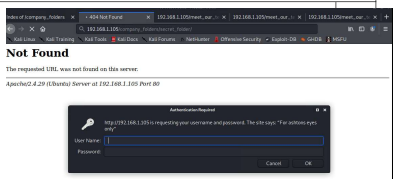
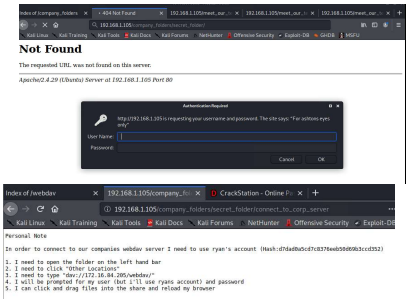
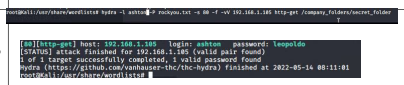
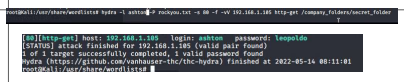
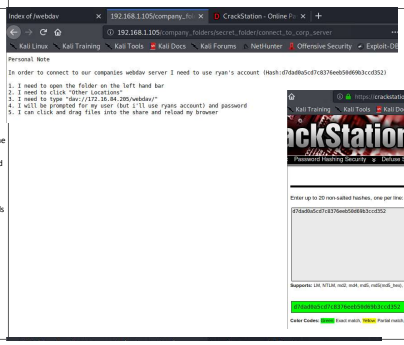
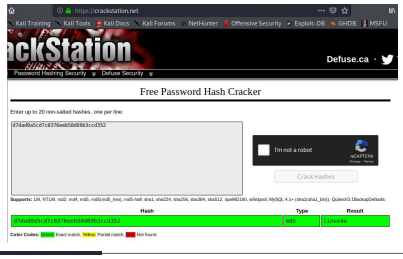
Vulnerabilities	Description	Impact	Tools & Processes	Achievements	Screenshots
Port 80 Open CVE-2019-6579	Open Port 80 can give attackers network access to the webserver	The attacker is able to use Port 80 to gain administrative priveleges and execute malicious code	Netdiscover was used to gather network information and clients connected to it. That was followed with a nmap scan to identify ports open on the target machine.	found that Port 80 was open an was able to access the web server	
Path Traversal to Access Secret Files CVE-2021-41773	The attacker is able to search for directories outside of root by using the URL to search for specific directories	The attacker can gain access to sensitive data that is not in the root folder	Once inside one of the visible directories on the web server, the URL was changed to the secret_folder directory	I able to gain access to the login page of the secret_folder which verified that existence of a private company folder.	 
Sensitive Data Exposure	Sensitive Data is exposed to authorized and unauthorized parties	The attacker is able to easily access sensitive data that they are looking for or information on how to gain priveleged access to the information that they are looking for	Searched the IP address on firefox which led the web server. Many of the files on the webserver talked about a secret_folder. Through Path Traversal and hydra I was able to gain access to the directory. The login page also gave away the account username to access the directory. The secret_folder also exposed the CEO's webdav password	found out how to access the webdav which further led to shell access to the CEO's account and capture the flag	
Weak Password CVE-2019-4067	The password policy for a given account does not require users to create complex passwords	Password can be easily guessed allowing attackers access to the account	Hydra was used easily bruteforce and guess the password of ashton's account	Uncovered ashton's credentials which lead to the CEO's Hashed Password	
Bruteforce Vulnerability CWE-307: Improper Restriction of Excessive Authentication Attempts	When no restriction is placed on the amount of time a log in can be attempted before an Account Lock-out	Attackers can continue to use bruteforce attacks until they are able to gain access to the account	Hydra was used to bruteforce the account without being locked out at any point for too many failed attempts	Uncovered ashton's credentials which lead to the CEO's Hashed Password	 
CWE-759: Use of a One-Way Hash without a Salt	A given software uses hashes on it's passwords but does not salt them	If computing resources are available, an attacker is able to crack the password either locally or through an online software very easily. If salts are used by the software, it becomes more difficult of the attacker to crack it since the salt string is unique to the software	crackstation was used on the hash to reveal the CEO's webdav password	uncovered the CEO's password and was able to access the webdav with his credentials	 

Cross site Scripting PHP remote file Inclusion CVE-2006-2849	Remote attackers are able to upload php code to the webserver and execute it	The attacker is able to get shell access to the vulnerable machine	msfvenom was used to create a PHP reverse shell payload. This was then uploaded to the webdav. Metasploit was used to execute the payload.	I was able to start a meterpreter session and shell into the CEO's webdav account to where I can view all of his directories and capture the flag