Penetration Test Report

Prepared for Hotel Dorsey

Name: Misty Keefe

Introduction

This report is a summary of the findings of a penetration test conducted for Hotel Dorsey's network. The scope of the penetration test includes the use of a Kali Linux attack machine, with the target being the Metasploitable Linux system. With the Kali Linux machine, Haverbrook Security Lab penetration testers will identify vulnerabilities within the Metasploitable system, exploit these vulnerabilities to gain access to the system, and steal information located on the system.

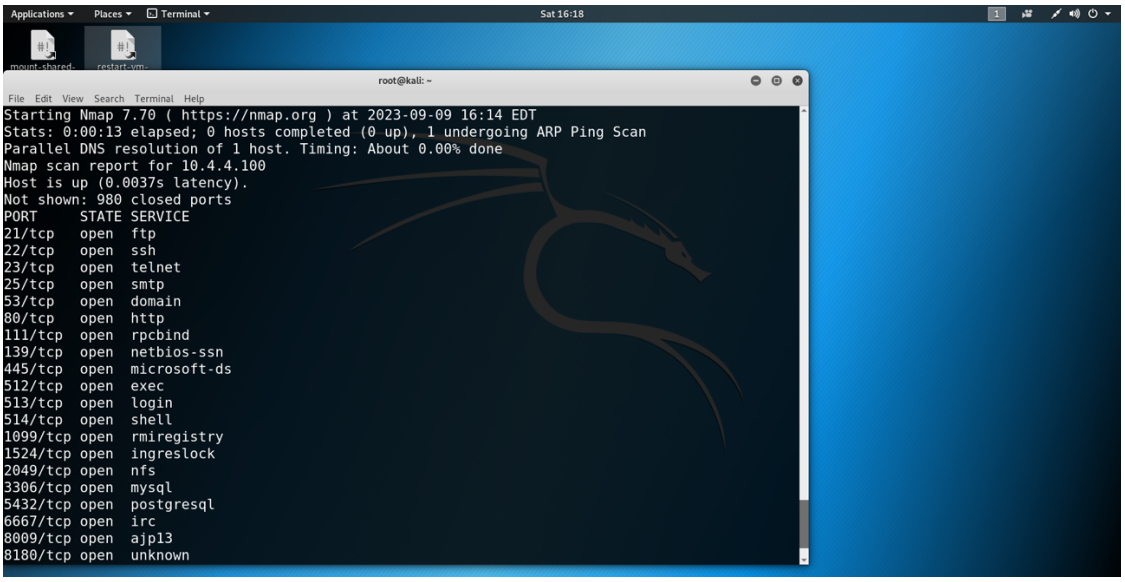
Tools used for this penetration test include the Kali Linux system where all of the actions were performed, terminal windows to execute commands for network reconnaissance and exploitation, and the John the Ripper tool which was used to crack hashes for user credentials. The use of these tools resulted in the successful exploitation and harvesting of user credentials which were thought to be stored securely by the client, as well as the exfiltration of artifacts stored on the system.

The link to the Exploitation Demonstration Video is listed below:

Keefe Exploitation Video.mp4

Target

The target system hostname is Metasploitable, with an IP address of 10.4.4.100. The attack machine hostname is Kali, with an IP address of 10.4.4.50. With conducting a scan of the Metasploitable machine using the "nmap" command, I was able to identify the open ports on the system, along with the services being run on each specified port. The screenshot below displays the results of the Nmap scan. The table below displays the open ports discovered in an Nmap scan, the service being provided on the port, and the description of the service provided.



A screenshot of the results yielded from conducting an nmap scan of the Metasploitable machine.

Table of Open Port Services and Descriptions

Port	Service	Description
21	ftp	Transport files between computers over the internet
22	ssh	Secure Shell, enables two computers to communicate and share data in a secure connection
23	telnet	Allows collaborative communication between two computers over a non-secure connection
25	Smtp	Primarily used to send and receive email
53	Domain	Used for domain name resolution, translates IP addresses into Domain Names (i.e. google.com)
80	http	Allows data exchange on the web over a non-secure connection

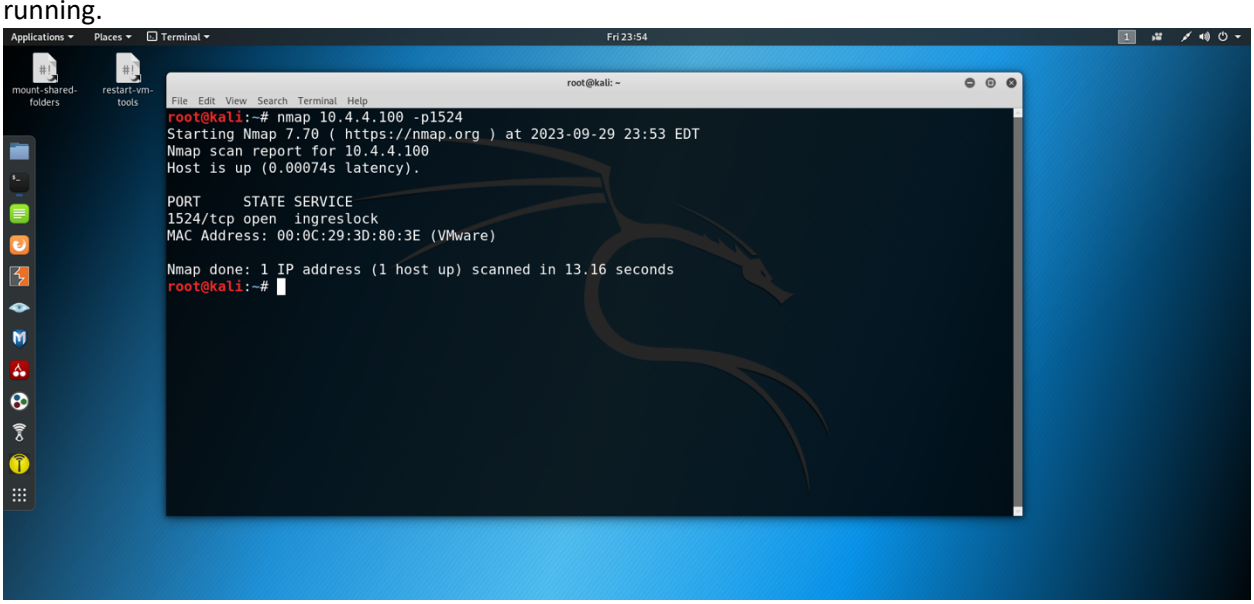
111	Rpcbind	Remote Procedure Call – can request a service from a program located on another computer on a network
139	Netbios-ssn	Connects two computers to transmit heavy data traffic
445	Netbios-ssn	Connects two computers to transmit heavy data traffic
512	Exec	Provides Remote execution with authentication based on usernames and passwords
513	Login	Provides the means to log into a remote system
514	Shell	Provides remote shell connections over a secure connection
1099	Rmiregistry	Software implementation for JAVA programming library
1524	Bindshell	A setup where remote consoles are established with other computers over the network
2049	Nfs	File system that enables the storage and retrieval of data from multiple disks and directories across a network
3306	Mysql	Primarily used for web database
3632	Distccd	Server for the distccd distributed compiler
5432	Postgresql	Used to store and scale complicated data workloads
6667	Irc	Internet Relay Chat – network of internet servers to host real-time online conversations
6697	Irc	Internet Relay Chat – network of internet servers to host real-time online conversations

8009	Ajp13	Proxy inbound requests from a web server through to an application server
8180	http	Open source web server and Servlet container for Java code

Vulnerability

The vulnerability being exploited for this penetration test is the Ingreslock backdoor accessible through port 1524. The Ingreslock backdoor is a vulnerability which was first reported in 2004, which allowed an attacker to gain root access to a system by creating a connection to their target using port 1524. While Ingreslock is a legitimate service used to lock parts of an Ingres database, securing this port when using this service is crucial to ensuring a secure network. By gaining root access, an attacker is able to perform an unlimited number of actions without restrictions including accessing file systems, executing commands, installing files and applications, or exfiltrating data.

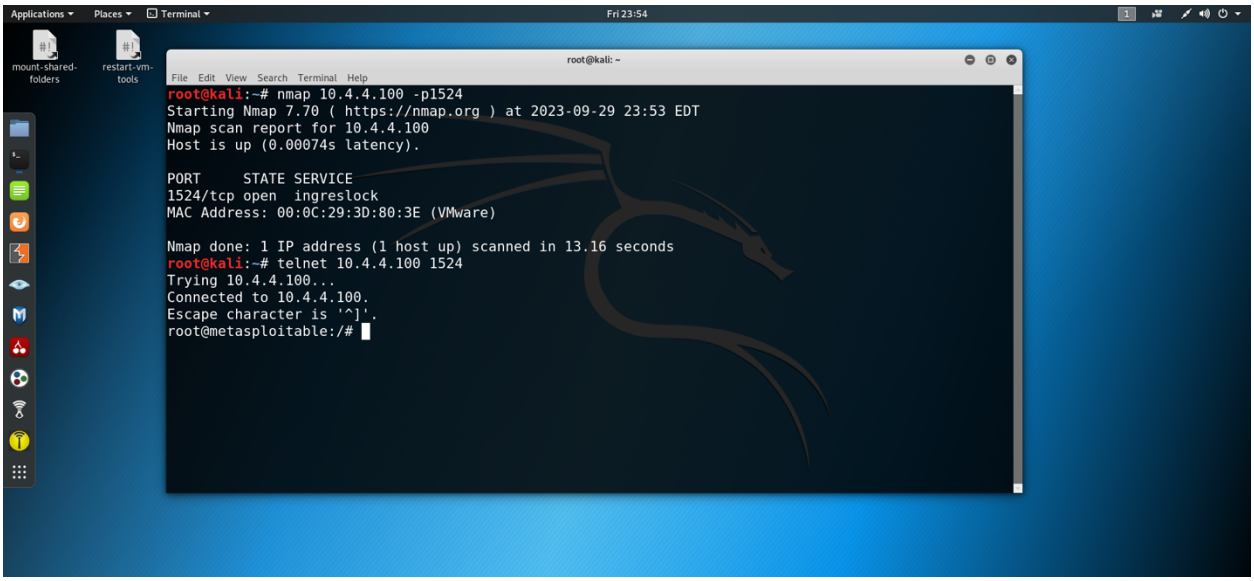
The first step in exploiting this vulnerability is identifying it. This can be accomplished by performing an Nmap scan on the specified port – in this case, port 1524 – to discover if it is open, and the service it is running.



A screenshot of an nmap scan on port 1524 of the Metasploitable target machine. Here, the Ingreslock backdoor is detected by identifying port 1524 is open for the Ingreslock service.

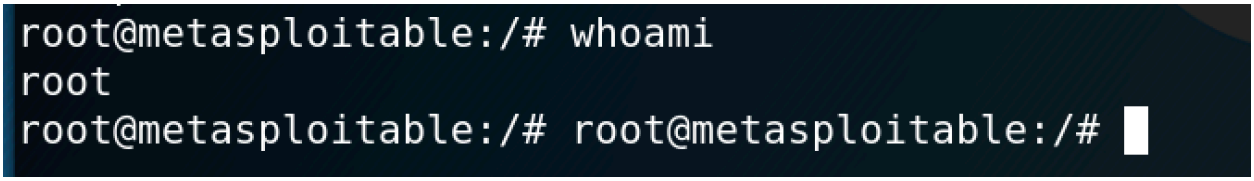
Now that we have identified our way into the system, the next step is to gain access. The Ingreslock backdoor is a particularly alarming vulnerability in the fact that all that is required to gain root access is to establish a telnet connection (a telnet connection is an unsecure remote connection into a host machine) to the target. From discovery of the open port at 23:53 EST, access is gained approximately 30

seconds later with the execution of a single command. The screenshot below shows how this is accomplished.



The telnet command is used in conjunction with the target IP address and desired port to establish a root connection. 10.4.4.100 is our target, and port 1524 is our way into the system.

With this command, root access is gained. We can confirm this using the whoami command to display our current level of access.

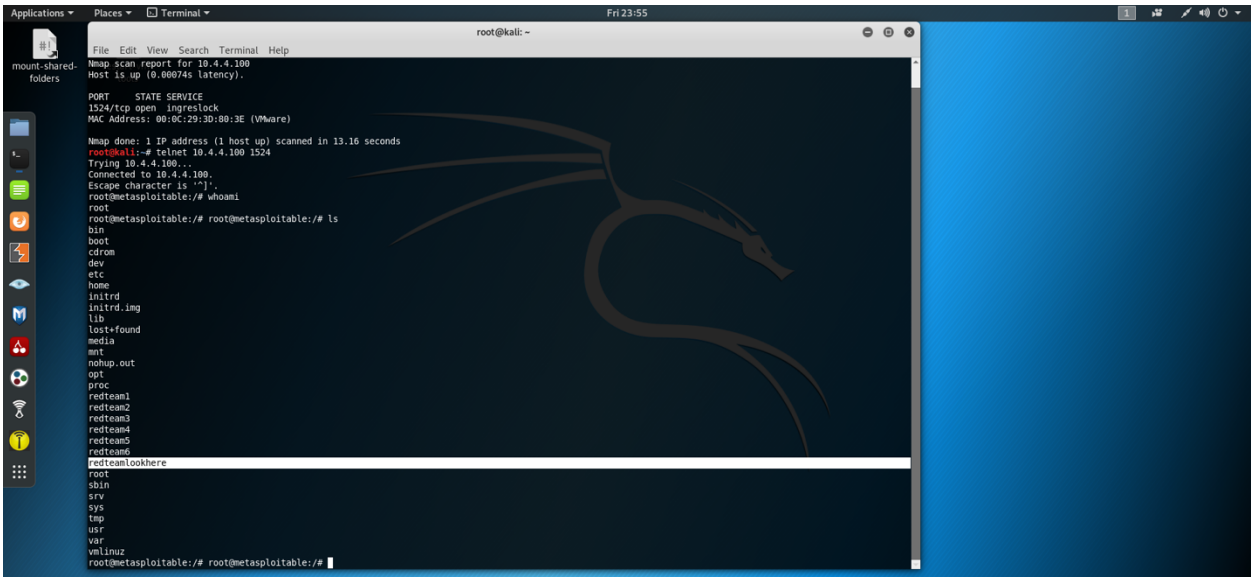


The whoami command yields a "root" response, indicating that we have root access into the target machine.

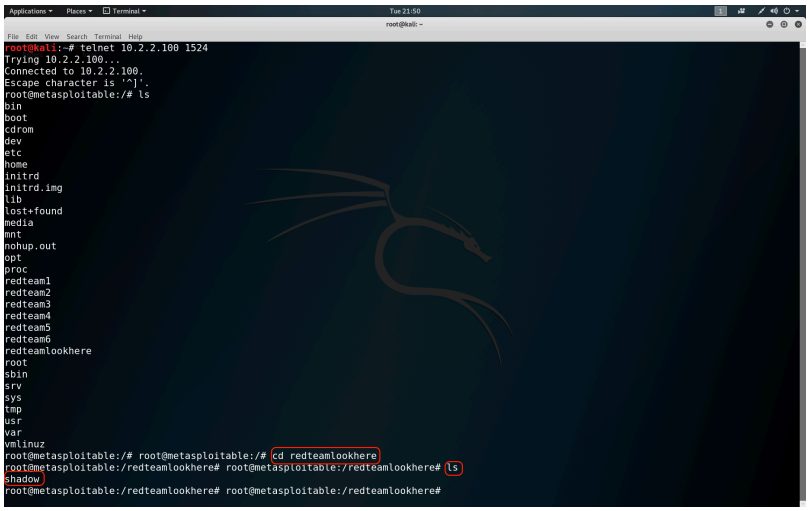
After root access is achieved, the next phase of the penetration test includes navigating through the system to steal information.

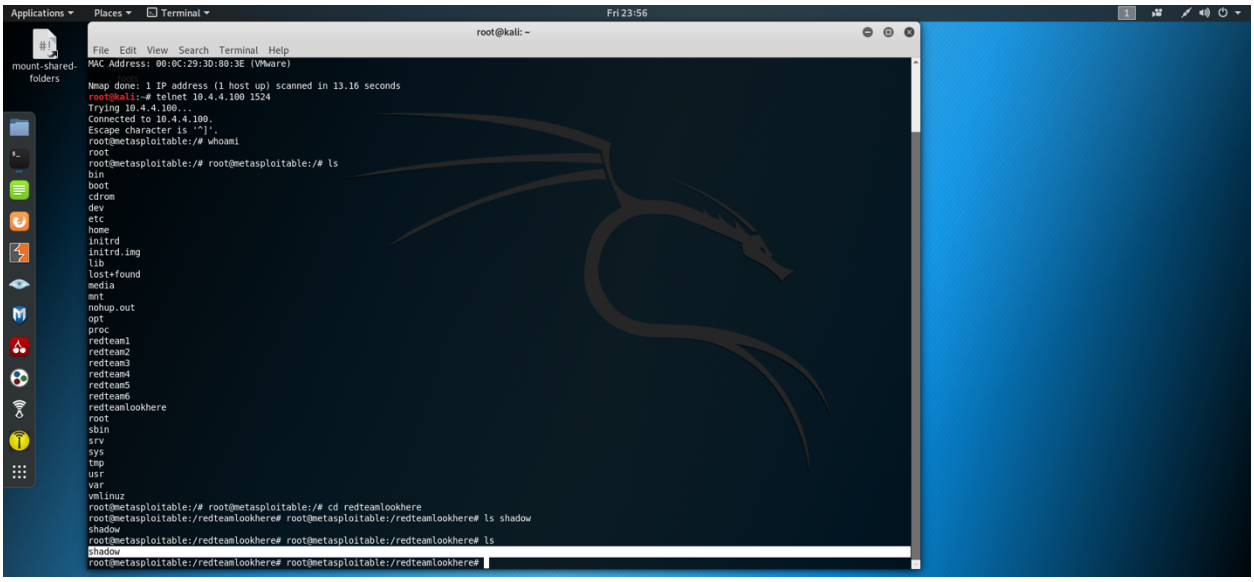
Data Exfiltration

With root access, an attacker is able to navigate themselves through directories with no restrictions or limitations. This is the method that was used to discover the target file containing the user credentials we are stealing and cracking for this penetration test. Screenshots and steps of this process are detailed below.

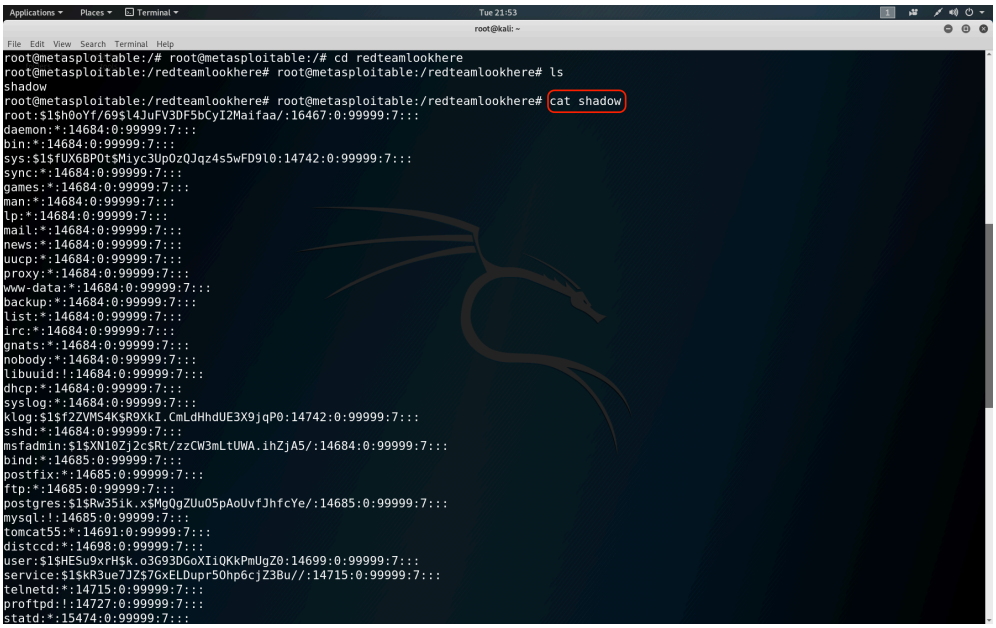


With root access, the ls command lists all of the contents and directories located within a location. Here, we can discover the "redteamlookhere" folder.

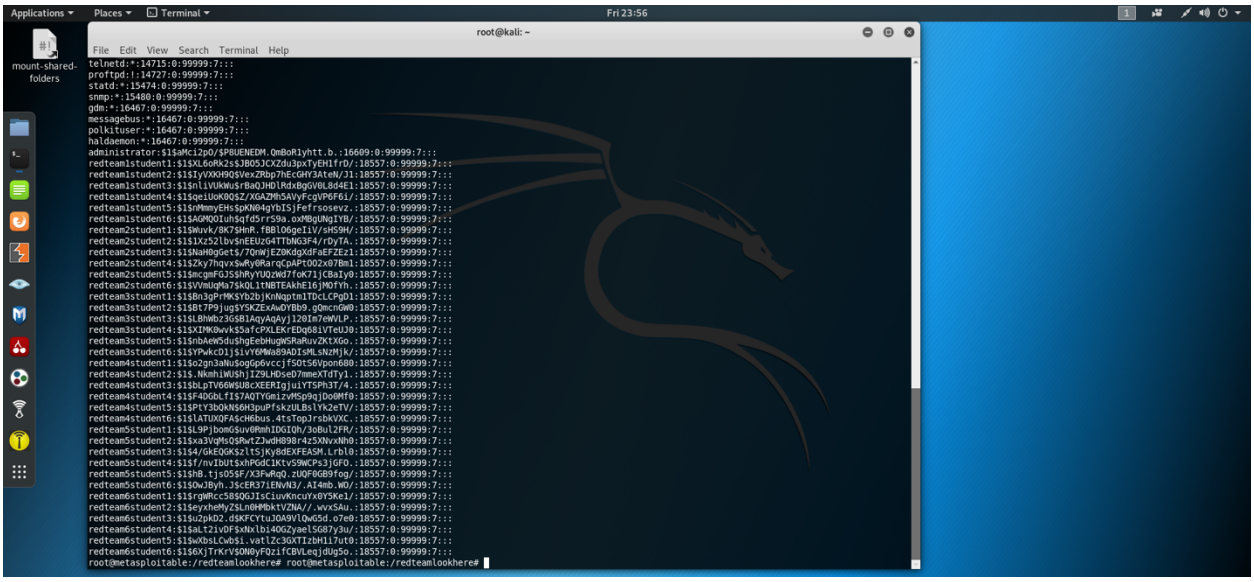




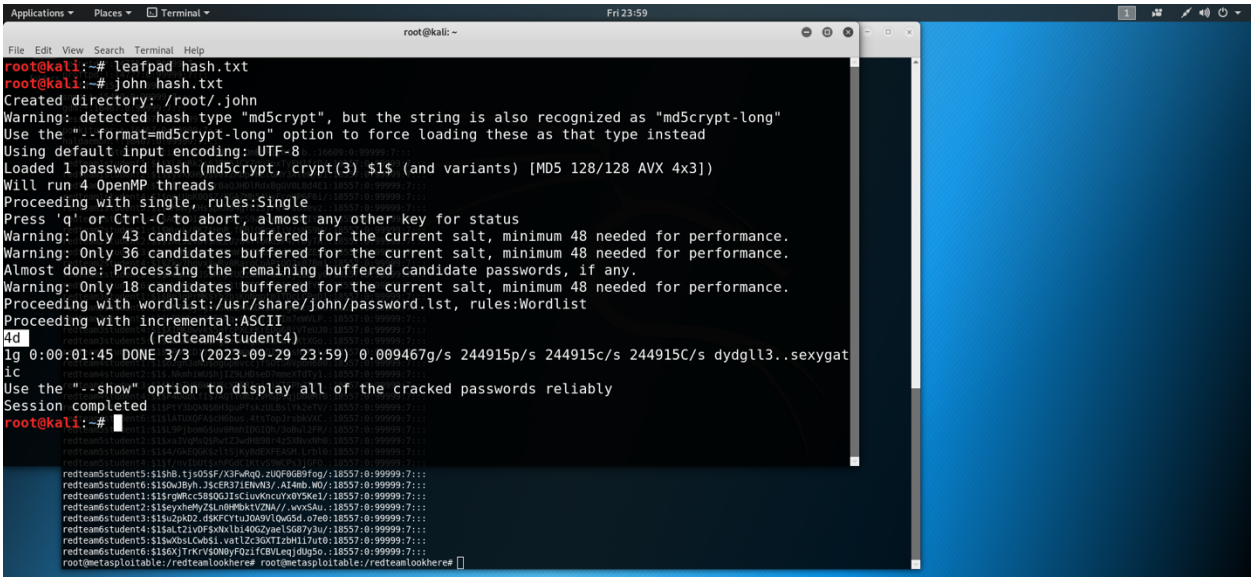
By changing directories to the "redteamlookhere" folder and listing its contents, we discover the "shadow" file.



The "cat" command allows the attacker to see the contents of the shadow file. The results yielded are shown here.



Within the contents of the shadow file, we identify our target password hash.



By taking the hash of the user credentials, we can use the John the Ripper tool to crack the hash. The results of the hash cracking is shown in the format of "username:password." For this instance, our username was "redteam4student4" and "4d" was the cracked hash for the password.

This process shows an extremely concerning level of vulnerability for the client's network and systems. The process of reconnaissance, exploitation, infiltration, and data exfiltration in total took less than 10 minutes for the user credentials targeted in this demonstration. With root access, attackers are given a golden ticket to perform any actions they desire with absolute autonomy of their desires. This can include stealing highly sensitive information and selling it to competitors, locking users and administrators out of the system and holding it hostage for ransom, and many more functions. The Ingreslock backdoor alone displays the exceptional amount of work needed to be done to secure the network and protect it from threat actors.

Recommendations

The Ingreslock backdoor creates a critical vulnerability to the system and significantly weakens its ability to defend itself from attackers. To mitigate this vulnerability, the TCP port on port 1524 should be locked down to prevent remote access from this port. In locking down port 1524, remote connections will not be able to be established, and thus prevent attackers from gaining entry to the system using this method.

Hotel Dorsey's network security posture severely lacks the safeguards necessary to ensure data confidentiality and integrity. Significant improvement of network management is required, and would best be provided through the employment of two full-time staff members: a database administrator and a network engineer. A database administrator's role will be to ensure that the database runs efficiently and securely. They will be responsible for establishing organization to the systems in compartmentalizing information in a way that ensures authorized users only access information that is necessary to perform their duties. A network engineer's role will primarily focus on maintaining the network within the organization. Beyond this, they also provide services to users to include troubleshooting outages, monitoring the network for suspicious activity, and resolving issues as they arise.

References

Alshawish, Ali, et al., *A Model-Based Time-to-Compromise Estimator to Assess the Security Posture of Vulnerable Networks.* 2019 International Conference on Networked Systems, IEEE, 2019.

Dimitrova, M. (2022, December 30). *Remove Ingreslock backdoor and lock TCP 1524*. How to, Technology and PC Security Forum | SensorsTechForum.com. https://sensorstechforum.com/remove-ingreslock-backdoor-and-lock-tcp-1524/

Ingreslock vulnerability - squarespace. (n.d.). https://static1.squarespace.com/static/5ba4e5c87a1fbd36d01467bc/t/5c1cc92588251b338fea2d12/1545390373629/Ingreslock+Vulnerability.pdf

Schrader, D., & Dirk Schrader Dirk Schrader is a Resident CISO (EMEA) and VP of Security Research at Netwrix. A 25-year veteran in IT security with certifications as CISSP (ISC2) and C. (n.d.). *Handling open ports secure and finding vulnerabilities*. Netwrix Blog. https://blog.netwrix.com/2022/08/16/open-network-ports/

Wang, Bolun, et al., *Neural Cleanse: Identifying and Mitigating Backdoor Attacks in Neural Networks.* IEEE Symposium on Security and Privacy (SP), 2019.