U.S. Bank Internal Penetration Test Findings

ShadowGuard Security

Secure your digital world with confidence.

MAY 2023

ShadowGuard Security
Authored by: Brandon Williams

Table of Contents

Statement of Confidentiality

The information contained in this report is confidential and intended solely for the use of U.S. Bank. This report is the property of ShadowGuard Security and may not be reproduced, distributed, or disclosed in whole or in part to any third party without the prior written consent of ShadowGuard Security.

This report contains sensitive information related to the security posture of U.S. Bank, and any unauthorized disclosure of this information could compromise the integrity of the network and the security of U.S. Bank.

By accepting this report, U.S. Bank agrees to maintain the confidentiality of this information and take all necessary steps to ensure that the report is only accessed by authorized personnel who have a need to know.

ShadowGuard Security takes all necessary measures to protect the confidentiality of its clients' information, including physical, technical, and administrative safeguards. Any breach of confidentiality should be immediately reported to ShadowGuard Security.

Thank you for your attention to this matter, and we appreciate the opportunity to work with you to improve the security of your organization.

Executive Summary

This report presents the results of the penetration test conducted by ShadowGuard Security on behalf of U.S. Bank. The objective of the test was to identify potential security weaknesses resulting from improper policies, practices, implementation, or patch management. The testing focused on two network segments 192.168.0.0/24 and 10.0.0.0/8. Moreover, the use of social engineering, wireless and physical exploitation were approved for this engagement.

During the testing, our team identified 4 high-risk vulnerabilities, 3 medium-risk vulnerabilities, and 2 low-risk vulnerabilities. The high-risk vulnerabilities identified could potentially be exploited by attackers to gain unauthorized access to sensitive data, and we recommend immediate remediation of these issues.

Our testing methodology included a variety of tools and techniques, including network scanning, vulnerability scanning, and penetration testing. We conducted the testing over 8 weeks and followed industry best practices to ensure the integrity and accuracy of our results.

It is ShadowGuard's professional recommendation that U.S. Bank take immediate action to address the high-risk vulnerabilities identified in this report to improve their overall security posture.

Thank you for the opportunity to conduct this penetration test and provide you with valuable insights into your network security. If you have any questions or concerns, please do not hesitate to contact us.

Reconnaissance

During the reconnaissance phase of the ShadowGuard red team's penetration testing, they utilized open-source intelligence gathering tactics to collect a wealth of information about U.S. Bank and its operations. By employing various OSINT techniques, the team was able to uncover valuable insights into the organization's key personnel, email address formats, affiliates, and job openings, among other areas of interest.

The process of OSINT gathering involves collecting information from publicly available sources, such as social media, company websites, and news articles. This information is then used to gain a better understanding of the target system and to identify potential vulnerabilities that can be exploited. OSINT is a critical component of any penetration testing exercise, as it provides a comprehensive view of the target environment.

To carry out successful OSINT gathering, the red team utilized a range of methods, including searching social media platforms for information, using search engines to find relevant data, investigating job postings and employee profiles, and analyzing information on the target company's website. By applying these techniques, the team was able to build a detailed profile of U.S. Bank, its personnel, and its operations, which in turn enabled them to identify potential attack vectors and vulnerabilities that could be exploited.

Assessment Summary

Based on the findings of the ShadowGuard team's penetration test, a total of 9 key vulnerabilities were discovered that could compromise the confidentiality, integrity, and availability of U.S. Bank and its systems.

There vulnerabilities allowed the team to gain immediate root access to affected systems, and locations. These vulnerabilities include a shell backdoor and misconfigured instances of vsftpd, UnreallRCd, VNC, and LLMNR services/protocols. Additionally, two of the seven high-risk vulnerabilities relate to weaknesses in the areas of U.S. Bank's physical and wireless security measures.

Below are the detailed walkthroughs of the ShadowGuard team's testing with supporting materials. As always please feel free to reach out to the team with any questions or concerns.

Overall, the findings of the penetration test underscore the importance of proactive and ongoing security measures to protect U.S. Bank's assets and sensitive data. By addressing the vulnerabilities identified in this report, U.S. Bank can significantly improve its security posture and reduce the risk of a successful cyber-attack.

Findings and Exploits

Finding 1-Shell Backdoor

During the penetration test, a shell backdoor was discovered on the 192.168.0.239 Metasploitable host using scanning tools.

This allowed for root access to the machine via netcat, leaving the entire system vulnerable to malicious activities.

The screenshot in Figure 1.1 confirms the finding, and Figure 1.2 shows the command used to access the shell. Lastly, figure 1.3 shows the results of an IP address command to confirm the breach.

Based on this finding, it is recommended that the backdoor be immediately removed from the system to prevent any further unauthorized access. It is also recommended to review the security controls in place and implement measures to prevent similar attacks in the future.

Feel free to look at this external resource on how to remove backdoors to assist the U.S. Bank Team https://www.wordfence.com/learn/finding-removing-backdoors/

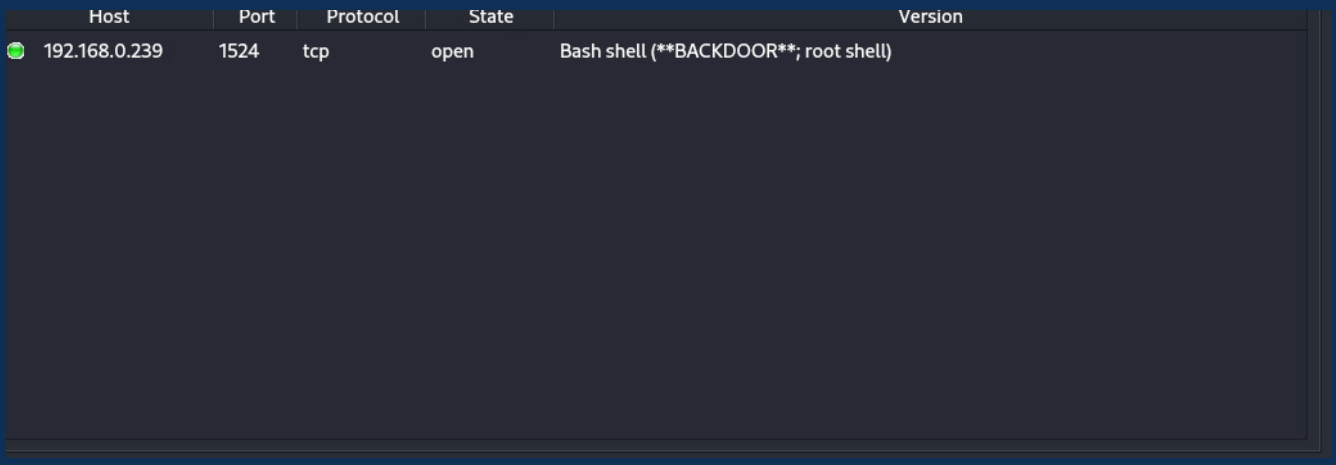


Figure 1.1

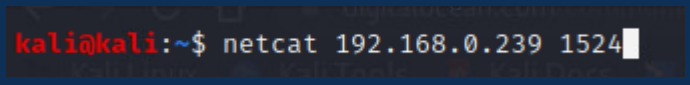


Figure 1.2

```
root@host8:/# ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 00:50:56:98:f3:78 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.239/24 brd 192.168.0.255 scope global eth0
    inet6 fe80::250:56ff:fe98:f378/64 scope link
       valid_lft forever preferred_lft forever
```

Figure 1.3

Finding 2-vsftpd

At the time of this report, the server located at 192.168.0.239 was found to be running VSFTPD version 2.3.4, which was found to have a vulnerability that allowed the ShadowGuard team to access the ftp server and download the system's /etc/shadow file.

This file contains the passwords for all accounts on the system and was later cracked by the team. Additionally, the team was able to create a bash shell with root access to the system.

Figures 2.1, and 2.2 show the attack, the team's accessing the shadow file, and figure 2.3 shows the root shell obtained through the exploitation of this vulnerability.

It is recommended that U.S. Bank update the VSFTPD version to the latest secure version to avoid such vulnerabilities in the future.

According to an article from https://www.rapid7.com/db/modules/exploit/unix/ftp/vsftpd_234_backdoor/ "This backdoor was introduced into the vsftpd-2.3.4.tar.gz archive between June 30th 2011 and July 1st 2011 according to the most up-to-date information available. This backdoor was removed on July 3rd 2011."

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set target 0
target => 0
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.0.239:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.0.239:21 - USER: 331 Please specify the password.
[+] 192.168.0.239:21 - Backdoor service has been spawned, handling...
[+] 192.168.0.239:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.0.0.3:44299 → 192.168.0.239:6200) at 2023-04-25 12:31:34 -0500

ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 00:50:56:98:f3:78 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.239/24 brd 192.168.0.255 scope global eth0
    inet6 fe80::250:56ff:fe98:f378/64 scope link
       valid_lft forever preferred_lft forever
```

Figure 2.1

```
root@host8:/# cat /etc/shadow
cat /etc/shadow cat /etc/shadow
root:[redacted]::
daemon:*:14684:0:99999:7:::
bin:*:14684:0:99999:7:::
sys:[redacted]::
sync:*:14684:0:99999:7:::
games:*:14684:0:99999:7:::
man:*:14684:0:99999:7:::
lp:*:14684:0:99999:7:::
mail:*:14684:0:99999:7:::
news:*:14684:0:99999:7:::
uucp:*:14684:0:99999:7:::
proxy:*:14684:0:99999:7:::
www-data:*:14684:0:99999:7:::
backup:*:14684:0:99999:7:::
list:*:14684:0:99999:7:::
irc:*:14684:0:99999:7:::
gnats:*:14684:0:99999:7:::
nobody:*:14684:0:99999:7:::
libuuid:!:14684:0:99999:7:::
dhcp:*:14684:0:99999:7:::
syslog:*:14684:0:99999:7:::
klog:[redacted]::
sshd:*:14684:0:99999:7:::
msfadmin:[redacted]:::
bind:*:14685:0:99999:7:::
postfix:*:14685:0:99999:7:::
ftp:*:14685:0:99999:7:::
postgres:[redacted]:::
mysql:!:14685:0:99999:7:::
tomcat55:*:14691:0:99999:7:::
distccd:*:14698:0:99999:7:::
user:[redacted]::
service:[redacted]:::
telnetd:*:14715:0:99999:7:::
proftpd:!:14727:0:99999:7:::
statd:*:15474:0:99999:7:::
snmp:*:15480:0:99999:7:::
cat: cat: No such file or directory
root:[redacted]::
daemon:*:14684:0:99999:7:::
bin:*:14684:0:99999:7:::
sys:[redacted]::
sync:*:14684:0:99999:7:::
games:*:14684:0:99999:7:::
man:*:14684:0:99999:7:::
lp:*:14684:0:99999:7:::
mail:*:14684:0:99999:7:::
news:*:14684:0:99999:7:::
```

Figure 2.2

```
root@host8:/# cat /etc/shadow
```

Figure 2.3

Finding 3-UnrealIRCd

IRCd, which stands for Internet Relay Chat daemon, is a program that enables users to communicate with each other in real-time over the internet.

While it can be a useful tool for communication, it also has some security risks. One of the main concerns is that IRCd relies on user-created scripts to function. These scripts can be manipulated by attackers to gain access to a system and compromise its security.

Another issue with IRCd is that it can be used to launch distributed denial of service (DDoS) attacks.

It is the recommendation of the ShadowGuard team that this service be removed from use or patched and updated appropriately to prevent future compromise.

The following article can assist U.S. Bank with these remediation recommendations.
https://www.vulnscan.org/improving-irc-security-step-by-step/

Figure 3.1 shows a backdoor execution via IRC that gave full root access to U.S. Bank's systems.

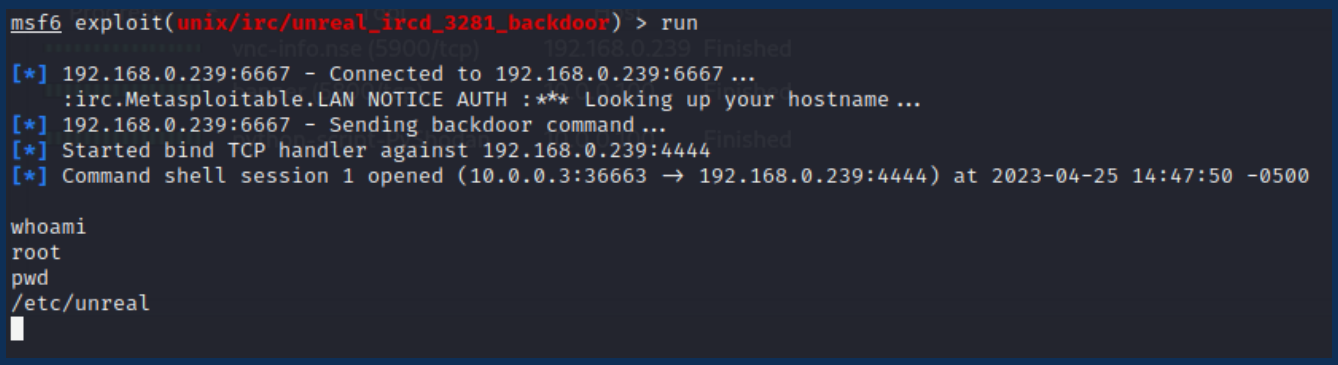


Figure 3.1

Finding 4-VNC

The VNC protocol is being utilized on five hosts within the U.S. Bank network. It is important to note that this protocol is known to be insecure and poses a significant risk to the confidentiality and integrity of sensitive information.

As a result, it is highly recommended that this service be removed from the network to improve the overall security posture of U.S. Bank and safeguard its stakeholders.

The ShadowGuard team was able to successfully execute a Metasploit attack that obtained the VNC server password. Figures 4.1 and 4.2 provide visual evidence of a VNC Client successfully connecting to a compromised server, highlighting the severity of this vulnerability.

```
msf6 auxiliary(scanner/vnc/vnc_login) > exploit

[*] 192.168.0.239:5900    - 192.168.0.239:5900 - Starting VNC login sweep
[+] 192.168.0.239:5900    - 192.168.0.239:5900 - Login Successful:
[*] 192.168.0.239:5900    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Figure 4.1

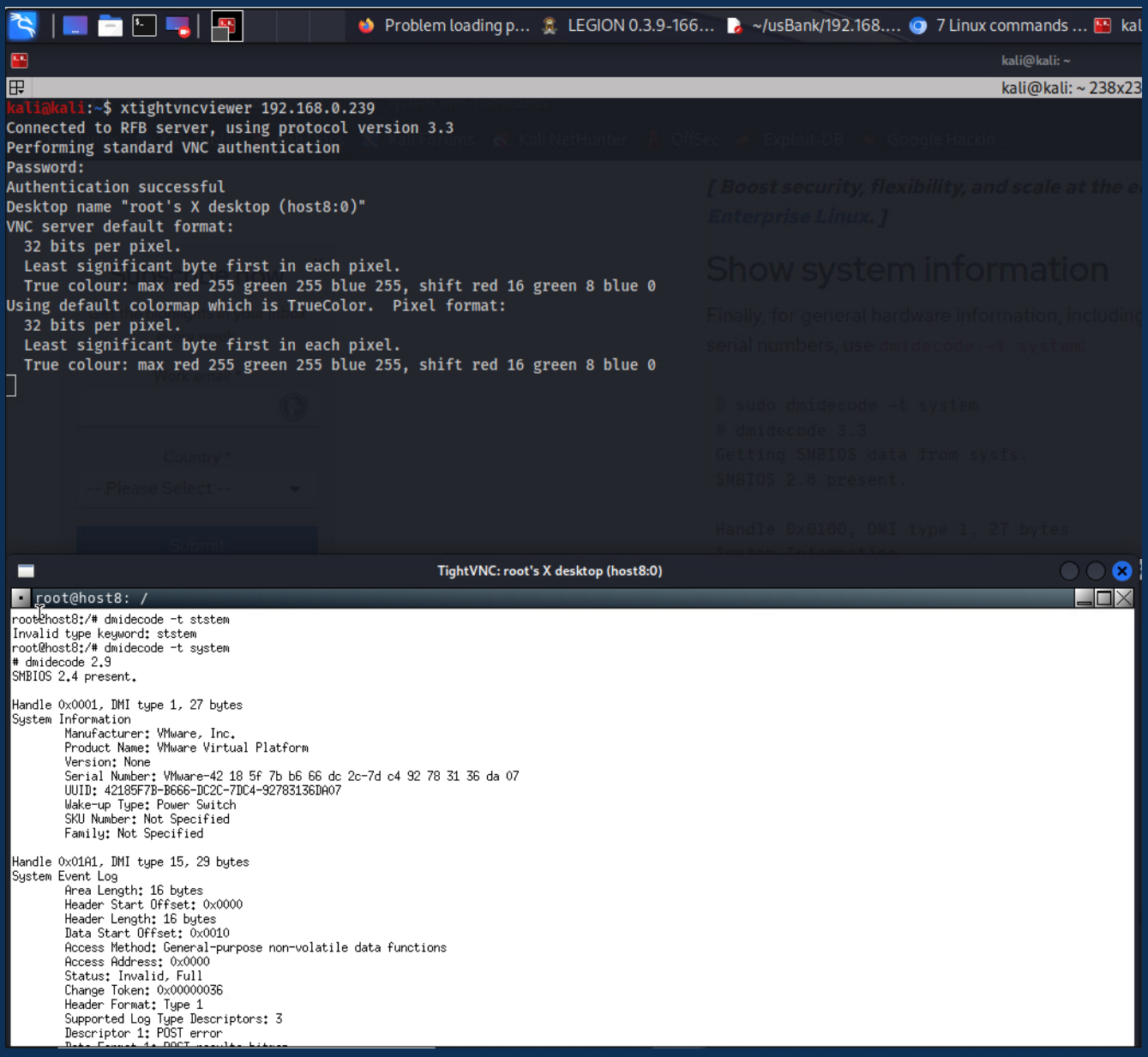


Figure 4.2

It is of utmost importance that the password is changed immediately, especially if the service cannot be removed from U.S. Bank's systems.

Finding 5-LLMNR

LLMNR stands for Link-Local Multicast Name Resolution. It is a protocol used to resolve hostnames to IP addresses in a local network when a DNS server is not available. LLMNR is enabled by default on Windows operating systems from Windows Vista onwards.

While LLMNR can be useful in certain scenarios, it can also be a security risk. Attackers can exploit LLMNR to perform a type of attack called "name poisoning". This involves responding to LLMNR queries with a fake IP address, which can redirect traffic to a malicious server as seen in figure 5.1.

Once the redirected traffic was captured the red team was able to make use of the hashcat utility to crack the administrator password of U.S. Bank's domain controller gaining access to the systems file shares. The cracked password can be seen in figure 5.2.

To mitigate this risk, it is recommended to disable LLMNR in environments where a DNS server is available. This can be done through Group Policy or by editing the registry on Windows computers. The following link from Black Hills Information Security can assist U.S. Bank with this process. https://www.blackhillsinfosec.com/how-to-disable-llmnr-why-you-want-to/

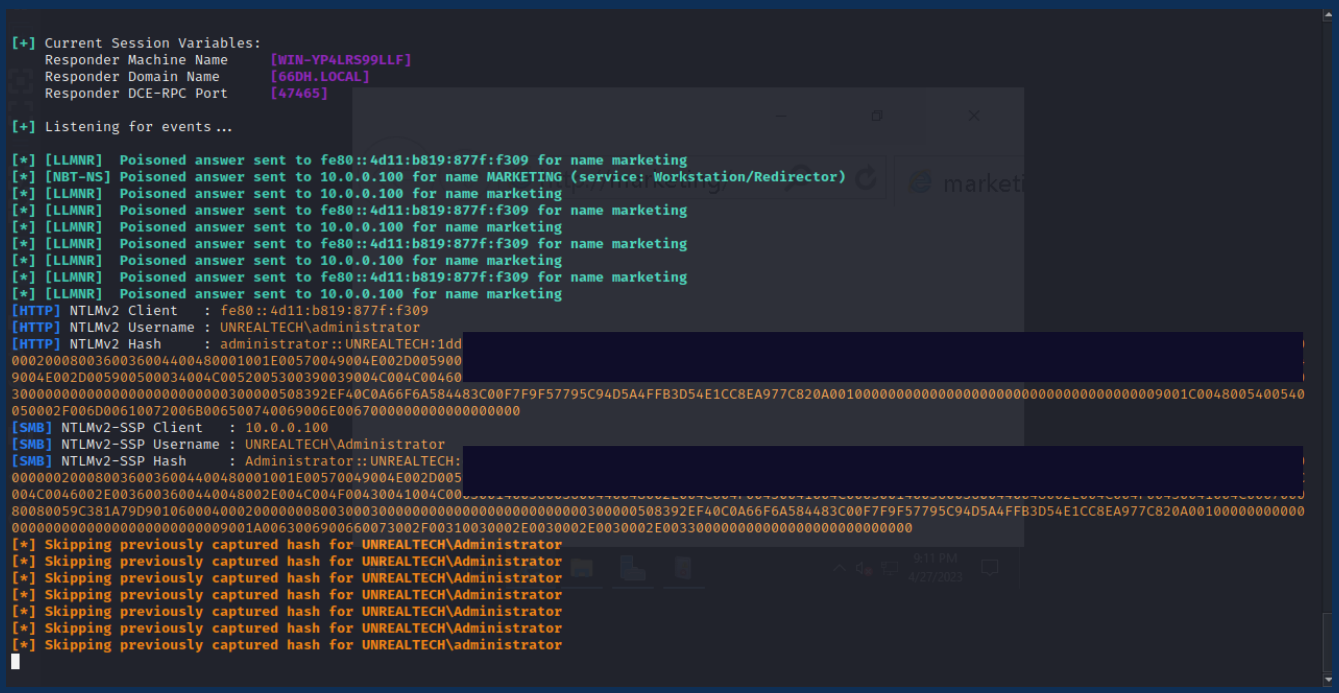


Figure 5.1

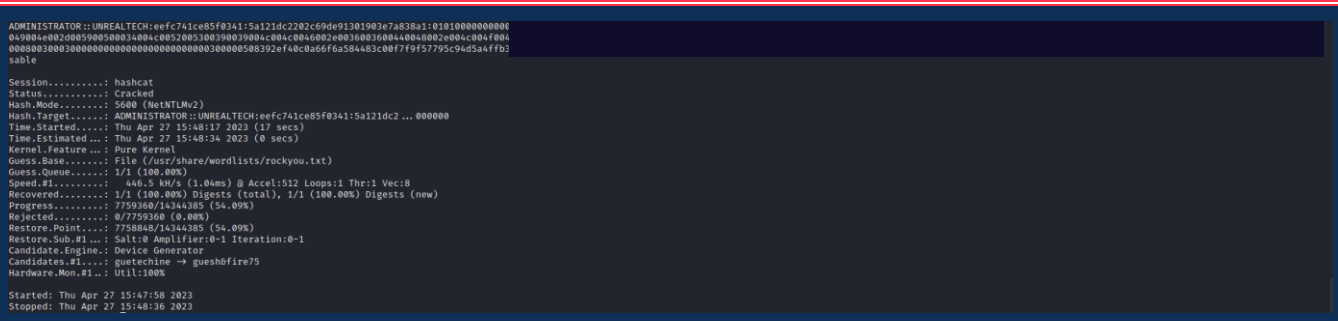


Figure 5.2

Finding 6-Wireless

During the assessment conducted by ShadowGuard Security, the red team successfully cracked the WEP key of a U.S. Bank branch, which poses a significant security concern. WEP is an outdated and vulnerable protocol that is easily exploited by attackers. As a result, the red team was able to gain unauthorized access to the bank's wireless network and potentially sensitive information.

To address this issue, it is strongly recommended that the bank upgrade their wireless security to a more secure protocol, such as WPA2. This would provide stronger encryption and better protection against potential attackers. In addition, implementing strong password policies and regularly changing passwords can also help prevent unauthorized access to the network. To further enhance network security, regular monitoring for any suspicious activity and prompt investigation of potential security breaches are also essential. The following article showcases what WEP is and why it shouldn't be used in production. https://www.oreilly.com/library/view/80211-security/0596002904/ch01s07.html

Figure 6.1 shows the ShadowGuard's cracking of the key.

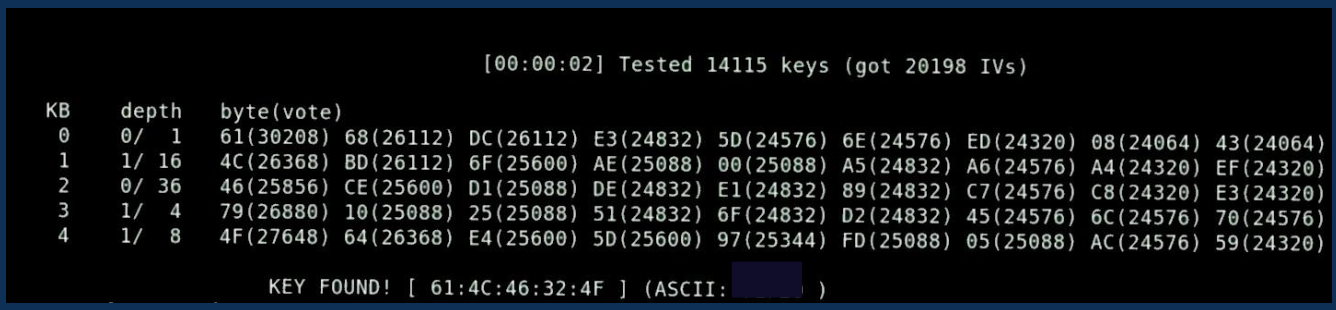


Figure 6.1

Finding 7-Physical

During the physical aspect of ShadowGuard Security's assessment, our red team members successfully gained access to a local branch office using social engineering tactics and locksmith tools. This highlights the importance of ensuring that sensitive information is not discussed in areas where it can be overheard, especially during normal business hours. We recommend implementing policies and procedures to reinforce this and conducting regular training sessions for all employees.

To improve physical security, we recommend upgrading the locks on external and some internal doors to more tamper-resistant and potentially electronic options. In addition, installing additional security cameras throughout the branch office will provide an extra layer of security and help monitor employee behavior to prevent unauthorized access.

Figure 7.1 shows a photograph taken from the second floor of the local branch office accessed by the team.

Figure 7.1

Finding 8-Telnet

Telnet is a network protocol that allows remote access to a server. However, it is an insecure protocol that transmits all data, including sensitive information such as usernames and passwords, in plain text over the network. This makes it easy for attackers to intercept and steal this information.

To address this security risk, it is strongly recommended to use a more secure protocol such as SSH (Secure Shell) instead of Telnet. SSH provides encryption for all data transmitted over the network, making it difficult for attackers to intercept and steal sensitive information. It is also important to keep all software up to date with the latest security patches to prevent any vulnerabilities that could be exploited by attackers. The following link can assist U.S. Bank with creating SSH keys to begin phasing telnet out of use.
https://gist.github.com/brando5393/cbda30c65267d1afcf680d23579b3b33

During an active Telnet session, the red team captured a TCP stream, as shown in Figure 8.1. This highlights the importance of implementing secure protocols and regularly assessing network traffic to identify and address potential vulnerabilities.

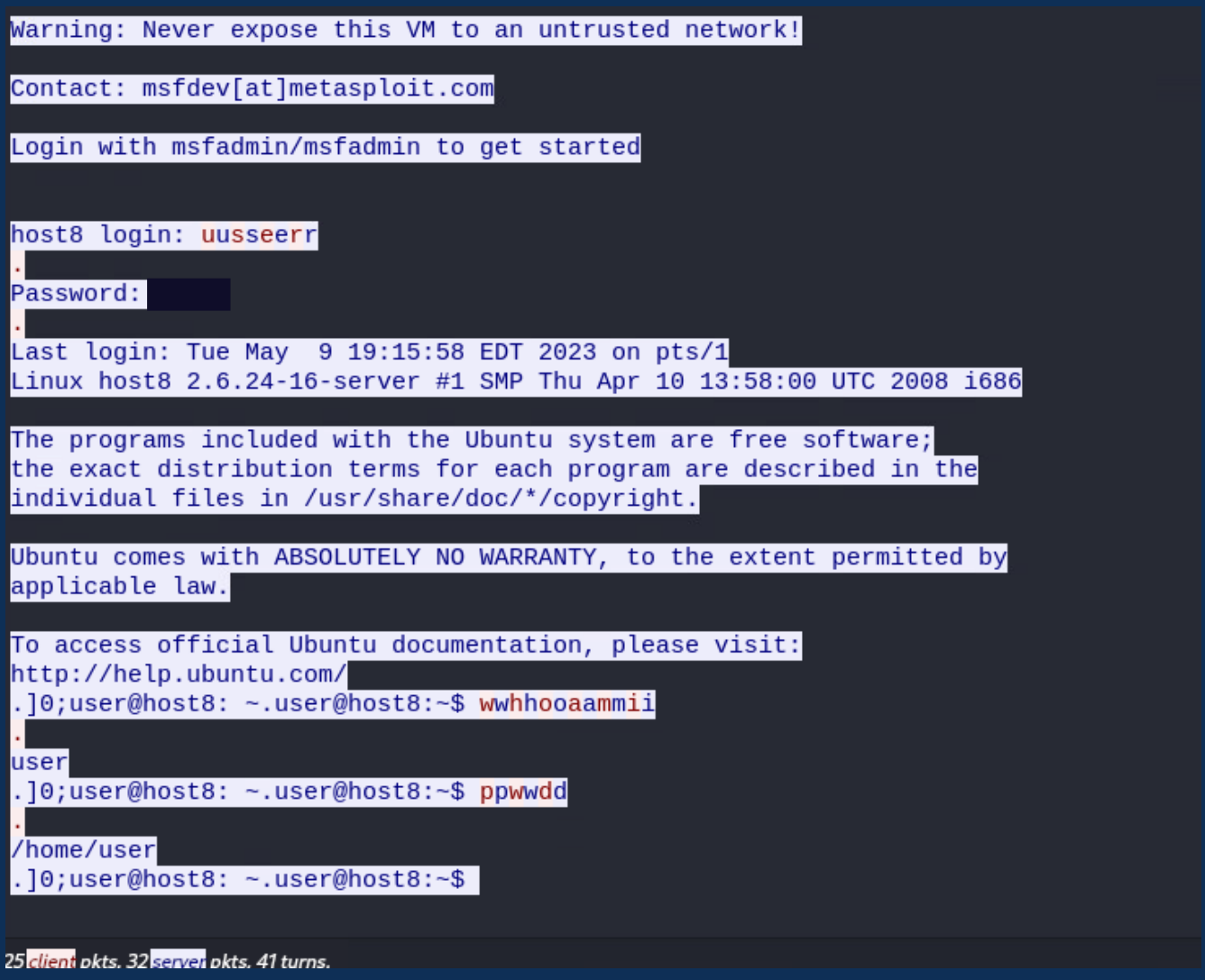


Figure 8.1

Finding 9-Firewall Access

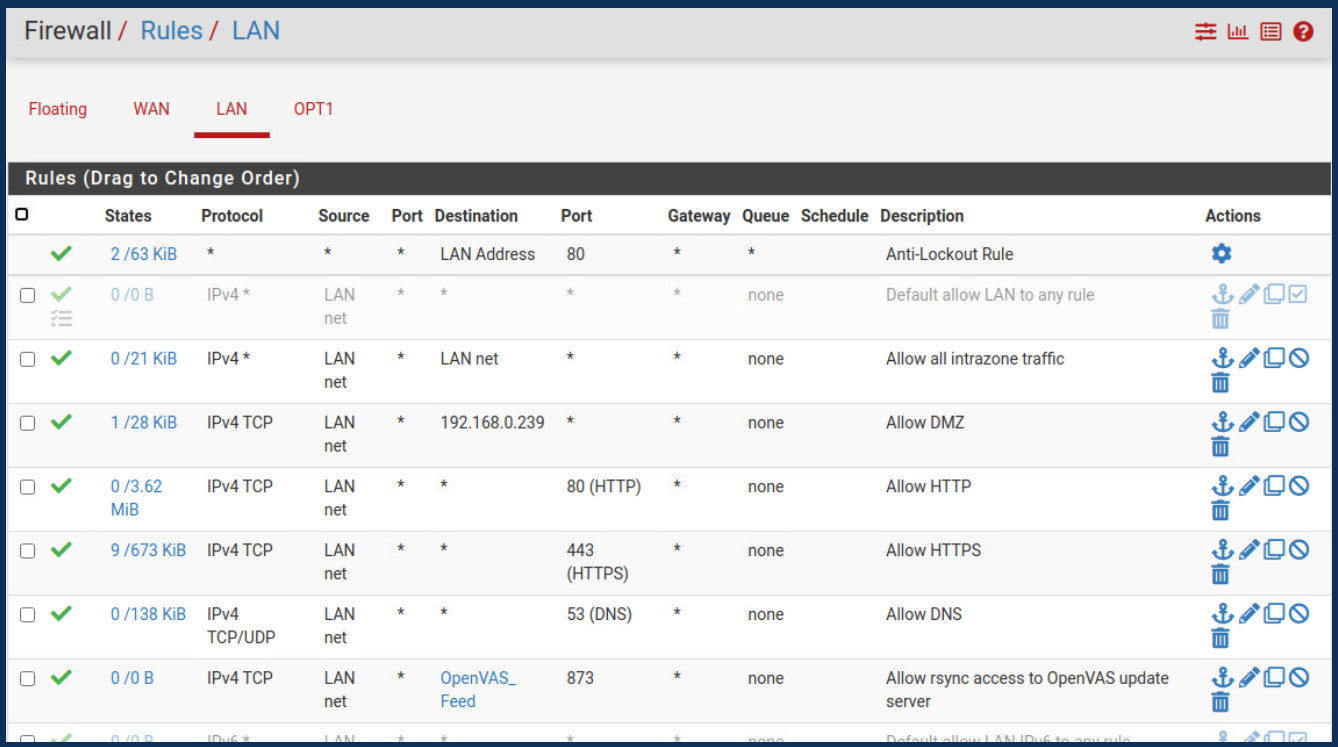
Shortly after the physical portion of ShadowGuard's engagement, team members were able to access the firewalls on U.S. Bank's network. This was made possible due to employees discussing

passwords in common areas openly, which highlights the critical role that employee education plays in maintaining strong information security practices. The use of weak passwords and discussing them openly in public spaces is a significant security risk, as it makes it easier for attackers to gain unauthorized access to sensitive systems and data.

These appliances were found to be pfSense firewalls, which are a popular choice for both home and enterprise users due to their ease of use, flexibility, and advanced features such as traffic shaping, VPN support, and intrusion detection and prevention. However, even the most secure and advanced firewalls are only as strong as their weakest link, which in this case was the weak passwords used to secure them.

It is the recommendation of ShadowGuard Security that the passwords on these firewalls be changed immediately, and that U.S. Bank implement an employee education program focused on information security to raise awareness about the importance of strong passwords and other security best practices. This education program should include regular training sessions and reminders about the risks associated with weak passwords and the potential consequences of a data breach.

Figure 9.1 shows the firewall rules currently in place for U.S. Bank's LAN, which serves as a starting point for assessing the overall security of the network. However, it is essential to keep in mind that firewall rules alone are not sufficient to protect against all possible threats. It is crucial to regularly review and update firewall rules and implement other security measures, such as intrusion detection and prevention systems, to provide multiple layers of defense against evolving threats.



	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓	2 /63 KiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
✓	0 /0 B	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	
✓	0 /21 KiB	IPv4 *	LAN net	*	LAN net	*	*	none		Allow all intrazone traffic	
✓	1 /28 KiB	IPv4 TCP	LAN net	*	192.168.0.239	*	*	none		Allow DMZ	
✓	0 /3.62 MiB	IPv4 TCP	LAN net	*	*	80 (HTTP)	*	none		Allow HTTP	
✓	9 /673 KiB	IPv4 TCP	LAN net	*	*	443 (HTTPS)	*	none		Allow HTTPS	
✓	0 /138 KiB	IPv4 TCP/UDP	LAN net	*	*	53 (DNS)	*	none		Allow DNS	
✓	0 /0 B	IPv4 TCP	LAN net	*	OpenVAS_ Feed	873	*	none		Allow rsync access to OpenVAS update server	

Figure 9.1