# 

# 

# ECorp - Security Report

# Performed by: Pentest R’ Us

# Ethical Hacking - Fall 2022

# 

Group Members: Kamith Mirissage, Joshua Rutherford, Justin James Thomas and Kevin Kalume Umba

# 

# 

# 

# 

# 

# 

# ECorp - “Trusted Manufacturing” - Background

ECorp Industries was founded on February 29th, 2008, by brothers Brad and Julian Thompson in Appleton, Wisconsin. The brothers wanted to put a modern twist on the outdated manufacturing practices of the 20th century. The medium-sized company has been expanding fast into the world of electrical car manufacturing with the rise in demand for EVs across the states. Working as contract manufacturers with big companies like GMC, Ford, and Chevrolet, ECorp has been creating millions of car parts throughout its tenure. As the business expanded, there was more focus on the manufacturing technologies and less on the network system. After hiring a new network administrator last year, ECorp has been modernizing their network technology alongside their manufacturing. The network administrator has hired our ethical hacking team, Pentest’R’us to perform penetration tests on their system to determine any vulnerabilities, security risks, and possible solutions.

# ​​​​Breaking Down The System

Looking at ECorp's network, we see that you have several different device types that you naturally use in your system and multiple different personnel that could interact with them. To start, you have a couple main servers that we will need to make sure are completely up-to-date and free of vulnerabilities. We assume that you will have some employees who work from home or have hybrid style positions, so it is critical that they have proper access protocols or procedures to properly and safely access your network from home. We will require personnel to have secure and up-to-date passwords, not only for your own corporate systems, but also for third-party services such as email or productivity applications. One of the main things we will be searching for are vulnerabilities in your network devices, such as open ports, physical vulnerability such as security gaps and your website [https://www.ecorp.com.](https://www.ecorp.com) In addition to the network side, we will be exploring the physical manufacturing building located in Appleton, Wisconsin and testing out the physical infrastructure of the location. You also have about 20+ workstations that your employees use at the manufacturing plant that we will also want to assess.

# Physical Security - Observed Vulnerabilities and Recommended Solutions (Kamith)

The manufacturing plant located in Appleton is a large rectangle shaped building, measuring 1000m by 400m, is a medium-small sized factory. It has 3 main entrances on the North, South and West side. North and South entrances are RFID key card entrances directly to the manufacturing floor. It’s an enclosed area, a blind spot from the camera. There are big bushes nearby as well that hide part of the vision on the North entrance. The doors themselves are on a piston auto closing door, however take 20-30 seconds to properly close. The west entrance has a small lobby staffed to welcome guests, however we have noticed there have been times when no one was at the welcoming desk, for bathroom breaks or lunch. The entrance to the manufacturing floor itself is behind an unlocked swivel door, easy to open and sneak into. The plant is running 24/7 on shifts, there are small overlap times around 4pm and 8am that have a lot of foot traffic. As for the east entrance, there is another RFID scanned door, however, it’s mainly the semi-truck loading docks. This part of the facility is heavily monitored, probably due to theft but it also helps with security. There is always a forman around monitoring the situation. There aren’t many easy to reach windows as it’s a manufacturing plant. However, some of the windows were left open, albeit 12 feet off the ground. There are service ladders scattered throughout the building, no cameras on them. Roof is fairly standard with exposed vents. The diameter too small for any human to fit through. Inside, the door to the IT team’s office is locked by a standard key lock. The computers and the main server rack are left exposed physically to anyone who can open the door. The server rack is locked by a further deadbolt lock however.

There were multiple security vulnerabilities that could be exploited by a motivated person. The first being the lobby entrance on the west side. As there is no RFID scanned door leading to the manufacturing floor, the only line of defense being a staffed personal who is occasionally away from their post.As for the other entrances, they are all RFID scanned, however, those are still vulnerable. We first recommend moving the camera away from the bushes and into the enclosed area so there is a camera pointing at anyone entering the door. There are hacked RFID scanners that can be placed on top of the existing scanner and create a copy of the RFID scanner (Tatianna,2018). The loading dock is fairly secure but someone could sneak in as it’s a busy location with a lot of moving personnel. The bathroom is inside the building and semi-truck drivers must go inside the plant to use it. The most troubling is the IT office; once someone is able to get into the manufacturing plant, there is a simple door lock standing between them and the company network server rack and admin privileged computers.

## Recommended Solutions for Physical Security Vulnerabilities

We first recommend having badge access to the main entrance, replacing the open door. Installing a camera at the door is also a second good step. There should be a staff replacement at front door security for lunch breaks and bathroom breaks to prevent leaving the lobby unattended. We recommend updating the RFID scanners with a newer technology, as badges can easily be lost or stolen. All doors within the area should be badge access only and have a policy of not letting outside workers enter into the building. We also recommend cutting any bushes or places people can hide nearby to sneak into the plant. Windows should be left closed, if it’s too hot, there should be proper ventilation installed so there is no need for it. All service ladders leading to the roof should have camera and motion detection or have 1 or 2 locations to reach the roof from. The door needs to be replaced with a fast closing door. 20-30 seconds is enough time for someone to sneak right in. To prevent unwanted access, we also recommend that the bathroom for delivery drivers should be outside the main plant area. Finally, the IT office should be badge access only, the server rack should be in its own closed room with very limited badge access. From initial testing, it seemed badge access was universal, anyone can open any door with the same badge, there should be tiered access for certain locations.

# 

# Personnel and Policies – Observed Vulnerabilities and Recommended Solutions (Joshua)

# After spending time observing employees’ workstations and their interactions, we identified several key vulnerabilities related to personnel. Weak passwords and passwords written in plain sight were observed, a critical vulnerability that should be addressed immediately. We also noticed that many employees were using their personal devices to check their email when away from their workstations; BYOD is an area of increasing concern for many businesses, and this can be a vulnerability without proper precautions. In addition, we observed several employees visiting suspicious websites on their workstations and opening spam emails, both of which can lead to malware infections that could compromise the system. Finally, in discussions with employees, we learned that no required information security awareness training is in place to educate employees about current risks.

# 

# Passwords

# First, we noticed that many employees had their passwords attached to their monitors with sticky notes, meaning that anyone with physical access to a workstation would have access to the password required to access it. Observed passwords ranged from "ecorp123" to "password" to "1234567" implying that there was no requirement to combine alphanumeric characters, passwords were not case sensitive, and there was no required password length. Even if the passwords had not been visible at the workstations, all of the observed and revealed passwords would be vulnerable to brute force attacks (*Estimating Password Cracking Times*, n.d.). In addition, there was no requirement for multi-factor authentication, which would require a second form of verification in addition to the password; often, MFA services will send a text message with a one-time login code that employees would enter after entering their password, as a secondary security measure to prevent suspicious logins.

# 

## Recommended solutions to Password Vulnerabilities

# It would be advisable to implement a strong password policy for ECorp. As mentioned above, there did not appear to be any requirements for password length, including special characters, or case sensitivity, all of which are strongly recommended in discussions for improving password security against brute-force attacks (*Estimating Password Cracking Times*, n.d.). Many tools are available to test password security, so it could be beneficial to ask employees to test their passwords using a tool prior to setting them for their accounts. Kaspersky, for example, offers this service on their website at<https://password.kaspersky.com/> (*Kaspersky: Secure Password Check*, n.d.). We would also recommend adding a multi-factor authentication service to your system in order to further prevent suspicious logins; we noted that you’re using Microsoft systems and wanted to mention that Microsoft Authenticator is an option that could be easily implemented in conjunction with existing services at ECorp (Microsoft, n.d.). Microsoft’s documentation on password policies also makes a number of recommendations that should be considered when establishing a password policy, which we have summarized in the checklist below (Microsoft, 2022):

# 

# · Don’t use the same password for multiple sites

# · Don’t use personal information in your password

# · Make sure your password is long – the more characters, the harder to crack

# · Use characters outside of alpha-numeric.

# · Consider using a phrase that you’ll always remember, but would be hard to guess

# · Consider using a password manager

# · Use multi-factor authentication when possible

# 

## Personal Devices (BYOD)

## We noticed that employees were using their personal devices to access work emails and other work-related websites and applications. When we asked employees about the requirements for using personal devices, they said that they just needed to log in, and they were able to access the websites on their personal devices, implying that there was no required VPN to connect to company services or other protections in place. Bring-your-own-device policies are becoming increasingly common and should be considered when allowing employees to use personal devices. Employees are more likely to connect to insecure networks outside of work on their personal devices, so if they have access to ECorp resources and documents on these devices, this increases the risk of these files being compromised. Similarly, employees commonly misplace their devices, or they can be stolen, both of which could lead to a compromised system.

# 

# Recommended Solutions for Personal Device (BYOD) Vulnerabilities

# Personal devices can be a serious vulnerability because there is less control over where the device will be taken, what networks it may connect to, and what will happen if the device is lost or stolen; there are measures that can be taken to minimize these risks, however. A good precaution to take is requiring a VPN for employees to log in to company-associated sites and applications on their personal device; VPNs can encrypt the device's IP address, making it less likely to be compromised if the employee is using an insecure network outside of work (Din, 2022; Lawson, 2018). If there is concern that employee devices may contain sensitive data that could compromise ECorp if the device was stolen, the company should consider implementing a personal device management solution that is capable of remotely wiping devices in case they are stolen. Mobile Device Management platforms, such as *gurumobility*, offer employers the ability to manage which devices have access to what information, give administrators the ability to locate missing devices and remove sensitive information, and even allow employers to control which applications can be installed on devices (GadellNet, 2022).

# Technological solutions, though, are only effective when bolstered with BYOD policies; ECorp should also establish policies that hold employees accountable and fill in gaps left by software’s limitations (Chouffani & Wigmore, 2021). Policies should cover significant details, like approved devices, acceptable use of devices, password requirements, measures to be taken in the case of a lost or stolen device, and plans for how to handle an employee leaving their position (Chouffani & Wigmore, 2021).

# 

## Suspicious Web Traffic and Spam Emails

# We observed several employees visiting websites with gratuitous pop-up advertisements; we asked a couple of employees and they informed us that they were visiting websites to watch movies for free. We also observed several employees checking their inboxes, and noticed that employees were receiving spam emails, and often were willing to open attachments and click on links in these emails. Malicious websites are a serious risk to the systems of ECorp; hackers commonly use websites with free content, such as movies, to incentivize individuals to click on links and download files, and often these files are laden with malware which could lead to an attack on the business, such as Ransomware (Minhas, 2021). Likewise, emails that send links to similar types of websites or include suspicious attachments are becoming an increasingly common attack leveraged by hackers (*How to Recognize and Avoid Phishing Scams,* 2022). Generally, companies use information security awareness trainings to educate employees on the risks associated with websites and emails like these, but after asking around, we discovered that there were no information security trainings currently being offered at ECorp (*What Is Security Awareness Training and Why Is It Important?*, n.d.).

# 

# Recommended solutions to Web and Phishing Vulnerabilities

# 

# Our first recommendation related to these vulnerabilities would be that ECorp implement a mandatory information security awareness training for all employees; not only can these trainings stand as a platform to educate your personnel on the risks of suspicious websites and phishing emails, but these trainings are often used to reinforce policy decisions relating to other identified vulnerabilities, such as passwords and use of personal devices (*What Is Security Awareness Training and Why Is It Important?*, n.d.). Trainings should be offered annually at a minimum, though we would encourage holding them more regularly, and offering supplemental materials in employee newsletters to ensure that cybersecurity risks remain on the mind of your employees (*8 Tips for Developing a Security Awareness Program*, 2019).

# 

# In addition to security awareness trainings, we would advise ECorp to implement some measures for web traffic control. Firewalls are an excellent option for a business of your size; they can protect your systems from malicious software, prevent employees from visiting suspicious websites, limit the use of bandwidth on devices to minimize employees streaming movies, and can even provide VPN services, which would help enhance security on personal devices (Maxwell, 2022).

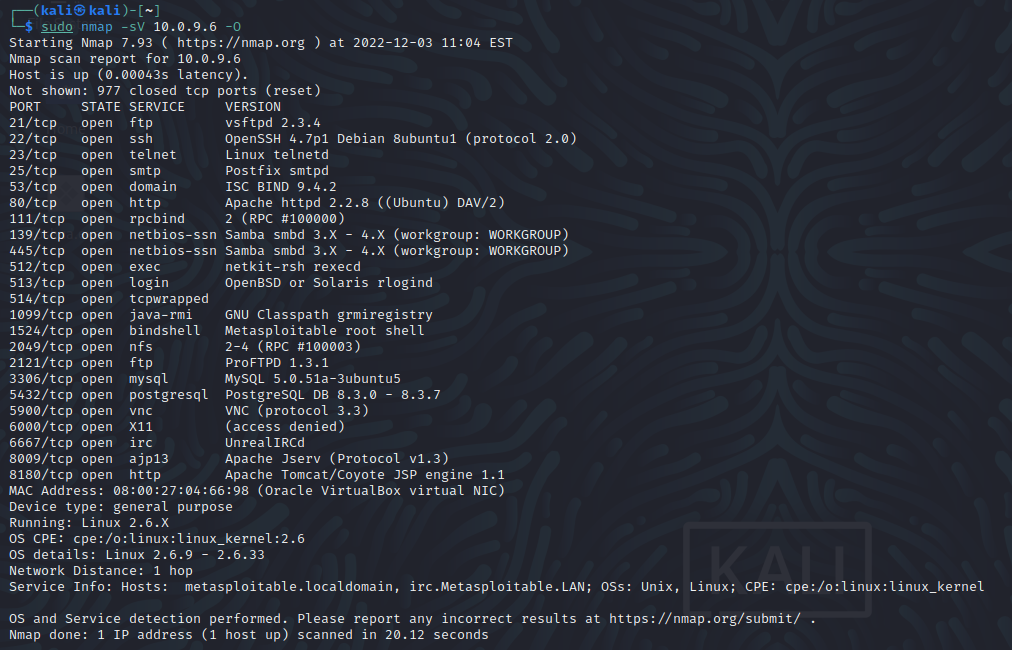
# 

# Systems - Tested Vulnerabilities and Potential Solutions

**Tools used**: nmap and Metasploit Framework

**Vulnerabilities Found**: FTP (port 21), OpenSSH (port22), postgresql (port 5432), VNC (port 5900)

Our group ran nmap to discover vulnerabilities in ECorp’s systems and devices (Figure 1), and used Metasploit Framework to find available exploits on the known open ports to gain root access through both FTP and VNC, and establish a meterpreter shell using postgresql. In addition, we were able to use a brute force attack to identify the password for OpenSSH, allowing unfettered remote access to systems.

****

**Figure 1: nmap port scan of company’s systems, revealing open ports.**

# FTP - Port 21(Joshua)

To exploit FTP, I searched in Metasploit Framework for “vsftpd,” the version of FTP being used by the target system. Metasploit Framework found one exploit was available: /exploit/unix/ftp/vsftpd\_234\_backdoor. I configured the required RHOSTS parameter with the target system’s IP address and ran the exploit (Figure 1). The exploit was able to create a shell, and I ran “whoami” to find out I had root access.

## Recommended Solutions for FTP Vulnerabilities

The penetration test revealed that the FTP port on this server was open, but also that it was not secured with encryption or users/passwords; as a result, when accessing through FTP, I was able to achieve root access on the system. To address this, at the very least, FTP needs to be set up to support encryption, authenticate by username and strong password, and/or use an IP address whitelist to prevent easy intrusion (*10 Essential Tips for Securing FTP and SFTP Servers*, n.d.). FTP is over 30 years old, and as with any older protocol many vulnerabilities have been discovered over time. While there are ways of encrypting FTP sessions and adding an access list of users with passwords, ultimately, I would advise switching to a more secure protocol. The SANS whitepaper on Securing FTP Authentication (2002) suggests implementing SSH or SFTP can help secure this type of connection: SSH Tunnels can be used as a proxy service to encrypt data being transferred through FTP and SFTP is essentially a version of FTP enhanced with SSH features which authenticates connections before transferring data (Gromek, 2002, p.11).

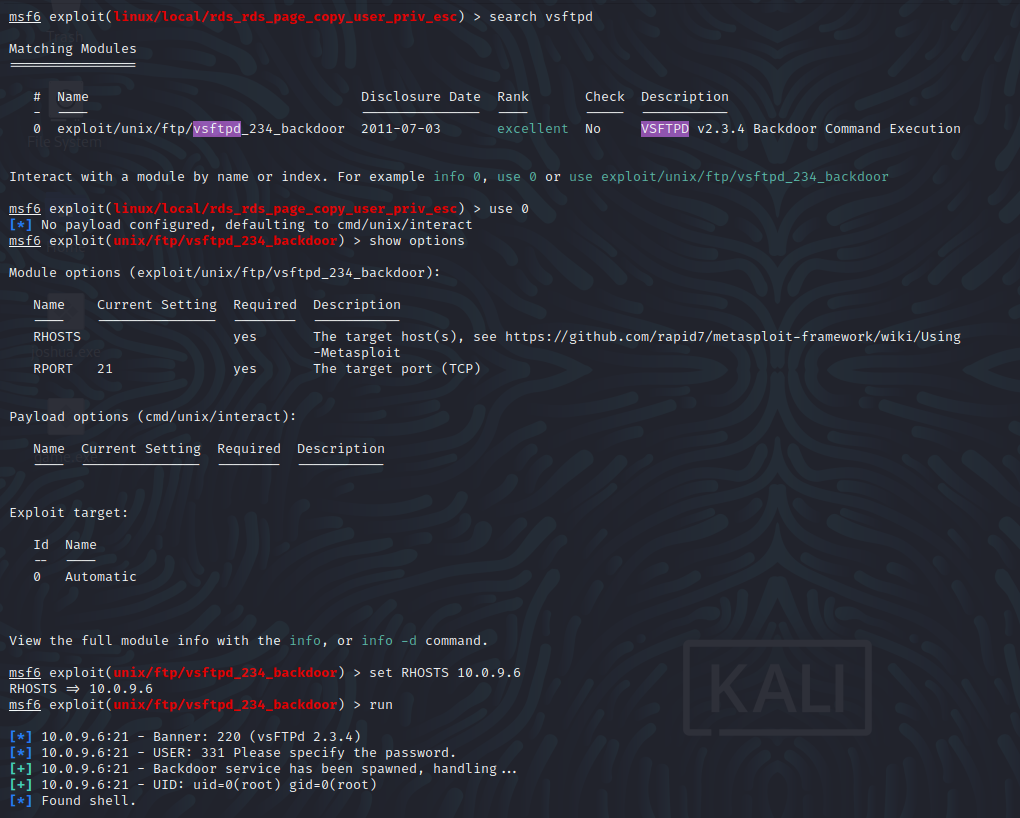
****

Figure 2: Searching Metasploit Framework for “vsftpd” exploits, setting parameters, and running exploit.

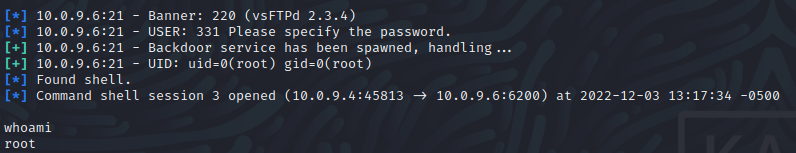
****

Figure 3: FTP Shell established through Metasploit Framework, “whoami” reveals root privileges.

# Open SSH - Port 22 (Kamith)

Secure Shell (SSH) is used to securely access the network remotely, initiate file transfers and general system level administrative work without needing physical access to the hardware. Our vulnerability scan showed that ECorp had left Port 22 open, commonly used for OpenSSH. Using msfconsole, there were two options available to test any vulnerabilities on the OpenSSH port.

Using auxiliary/scanner/ssh/ssh\_login\_pubkey, if ECorp had a compromised private\_key, we could have used that to gain access to their system via ssh\_login\_pubkey tool. With a private\_key, we could have been able to directly ssh into the network, seemingly no different from an authorized user.

Without a private\_key on hand, we resorted to using the auxiliary/scanner/ssh/ssh\_login tool (Figure 4). This tool used a brute force method to test common combinations of usernames and passwords to gain access. From discovery, we found an IP address for a device in their network, and we were able to brute force a session. We first created a file containing a list of common usernames (Figure 5), then created a file containing a list of common passwords (Figure 6). The tool brute forced all possible combinations until it found a working combination (Figure 7). WIth a working combination, we are able to start a session and able to access files within the compromised device (Figure 8).

## Recommended Solutions for OpenSSH Vulnerabilities

Most recommendations are to close Port 22 as it’s a common source of attacks, at the very least, we recommend using a different (higher numerical valued) port to handle remote access. Assuming the port is changed, we also recommend using an Universal SSH Key Manager, to manage any SSH keys created, any leaked keys would compromise the network.

As for the exploit we found, we would first set restrictions on password attempted, this can be changed in configuration. We would also change the base username and password. Overall, we recommend blocking username/password access to remote systems as it is not secure and vulnerable as demonstrated. This can be configured in the configuration file and will stop future attempts.

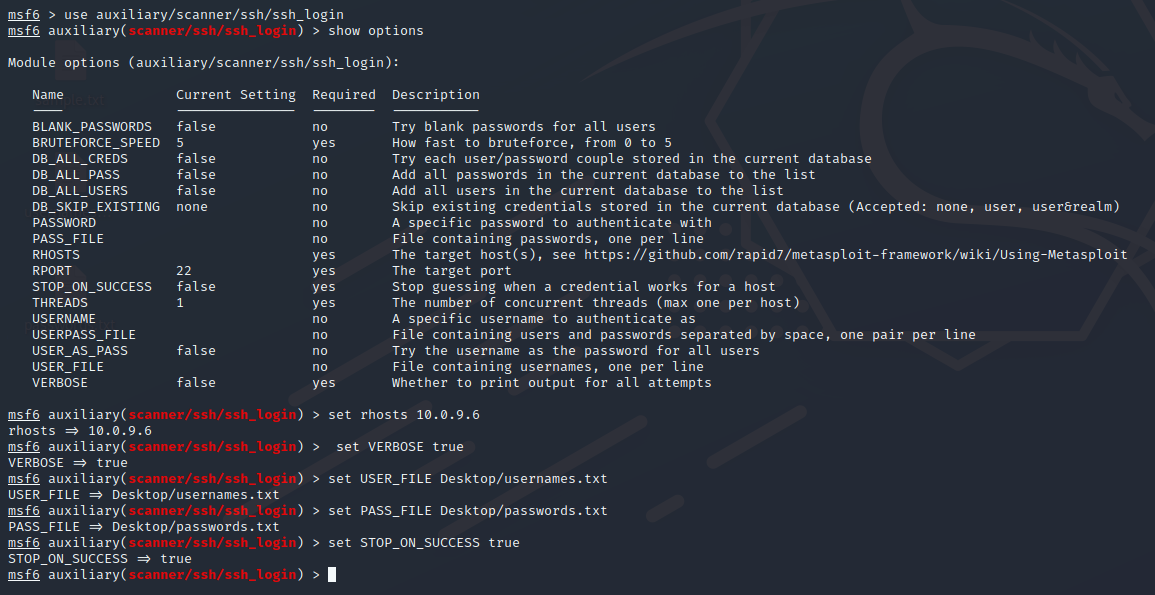


Figure 4: Auxiliary module setup

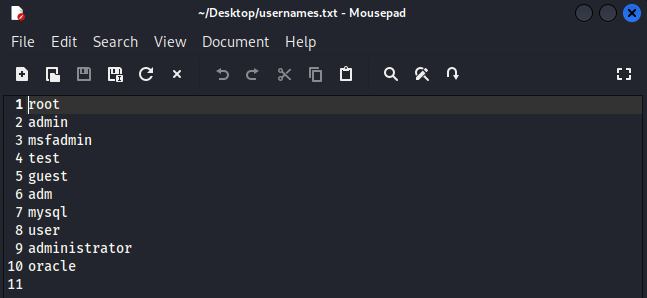


Figure 5: Example usernames to test

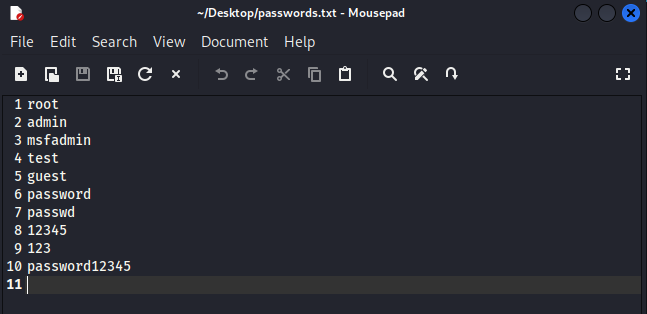


Figure 6: Example passwords to test

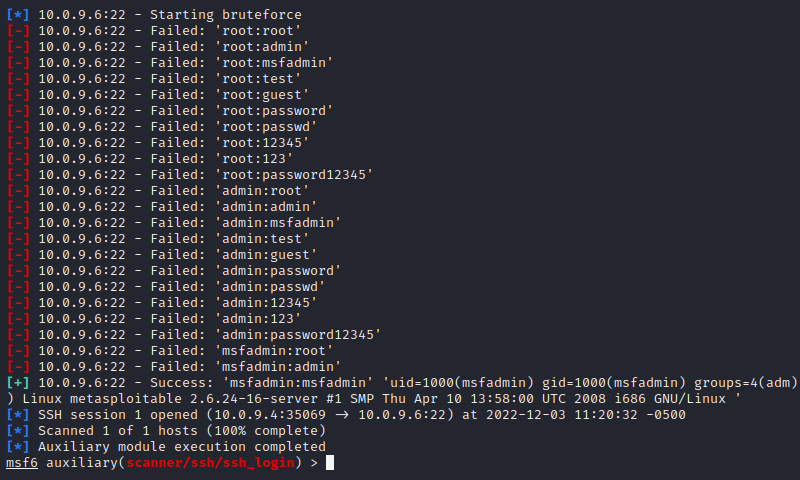


Figure 7: Brute Force Password Check - Success on user/msfadmin pass/msfadmin

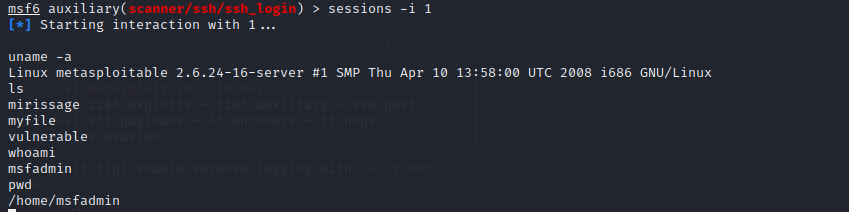


Figure 8: Create session and have access to files in hacked machine

# Telnet - Port 23 (Justin)

Telnet is a port on your network that is responsible for remote networking services. Telnet is quite outdated at this point here, and we are wondering as to why it remains open. This port and service is credential based, so it is vulnerable to a variety of attacking avenues. A man-in-the middle attack could leave you at risk, as a 3rd party could easily intercept Telnet login credentials, and access this service. Common brute forcing methods can also be effective in gaining network access through this service, so it is important that we address this quickly.

## Recommended Solutions for Telnet Vulnerabilities

The easiest way to remedy this situation is to simply close this port. Telnet has been mostly made obsolete by modern SSH services. Assuming your company has this service running on another port, your remote services should be more than satisfactory this way.

# 

# HTTP/PHP - Port 80 (Kevin)

Knowing the language on the server can lead an attacker to the CVE that your system is vulnerable to. During reconnaissance, we discovered that the server was running with PHP via an open port 80. For context, port 80 is used to access web pages via the HTTP protocol. A ping sweep and port scan revealed an employee’s IP address 10.0.9.6 and port 80 was open (Figures 9 and 10). We took advantage and connected to the victim’s machine via the browser (Figure 11). After navigating to the php index page from the host’s landing page, we discovered that the host was running PHP 5.2.4 on the server (Figure 12).

Using metasploit we found this version of PHP was vulnerable to an argument injection vulnerability (Figure 13). PHP versions 5.3.12 to 5.4.2 are vulnerable to this attack (Rapid 7, 2022). The vulnerability was weaponized through metasploit to get access to the host machine through reverse tcp (Figure 14). From there we were able to see everything on the host machine on our Kali machine (Figure 15).

## Recommended Solutions for HTTP/PHP Vulnerabilities

Closing unnecessary ports is the first step to make your system secure. Open ports are the entry point to your system. Your security staff should revisit default settings to close any unnecessary before shipping machines to your employees. Furthermore, to make your connection more secure you should use HTTPS on port 443 instead. HTTPS uses encryption and verification to make your web traffic secure. We also recommend updating your PHP version since later versions of PHP are patched against argument injection attacks. Lastly, we highly recommend installing a firewall in your company’s network to prevent port scanning. While performing our test we were able to ping your open ports without any issue. A firewall has the ability to drop suspicious packets. Firewalls can detect SYN, XMAS and other types of port scans.

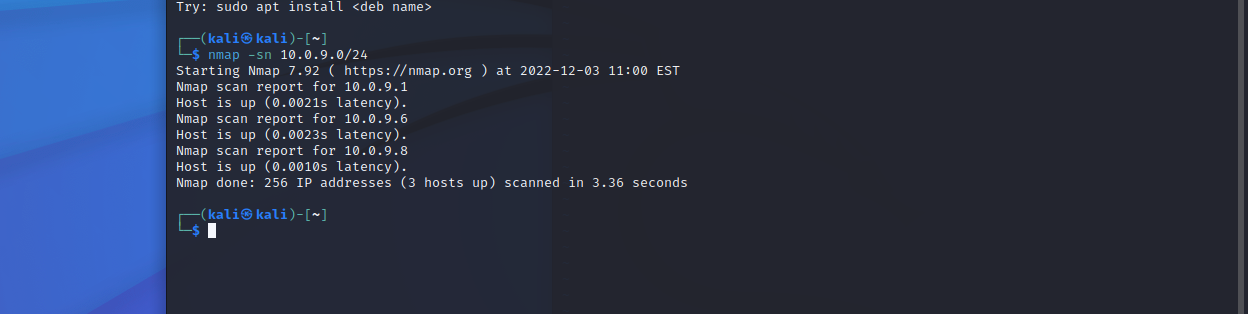


Figure 9: Ping sweep revealing the host’s ip address on the line 7

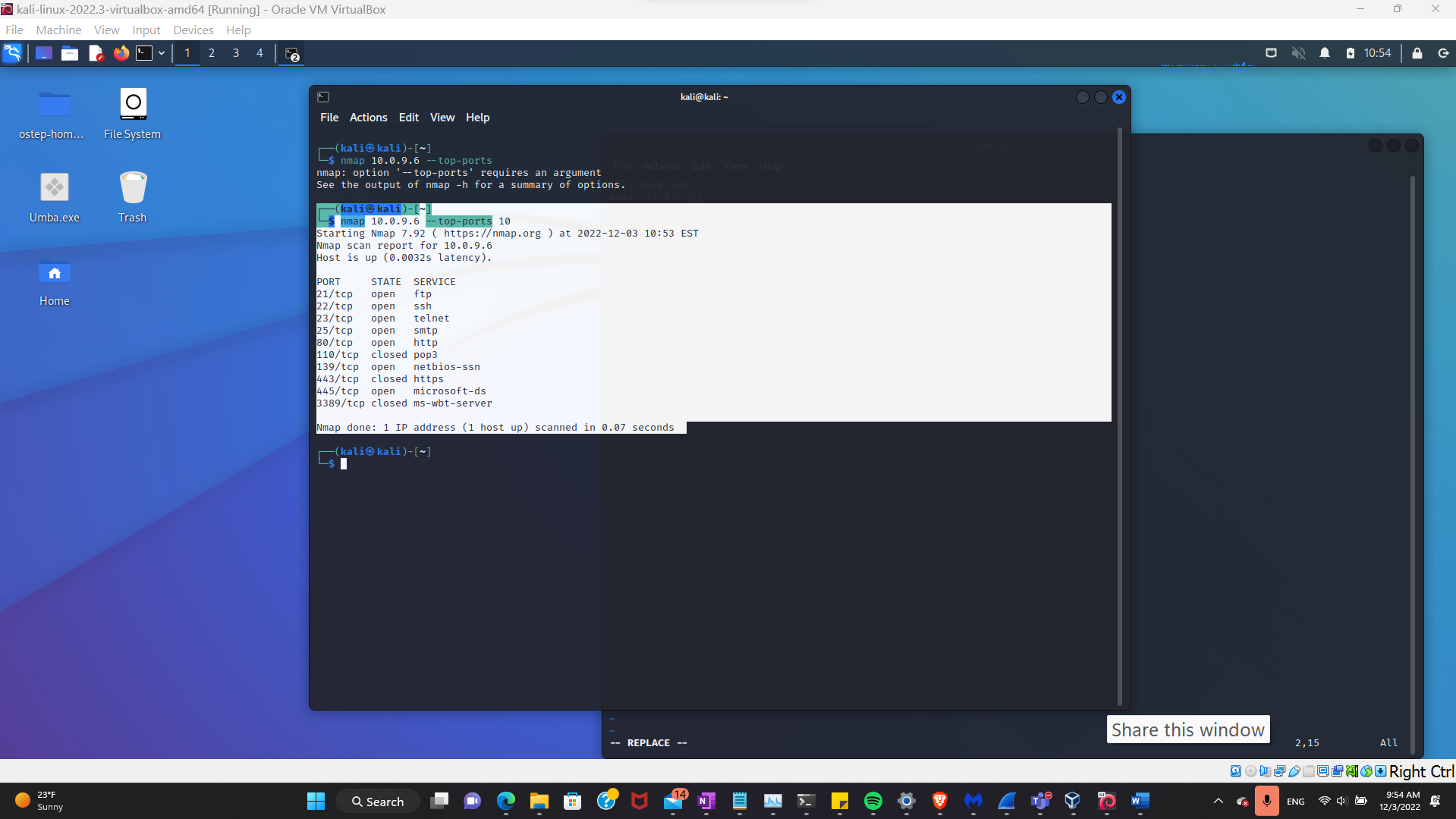


Figure 10: line 15 shows port 80 open

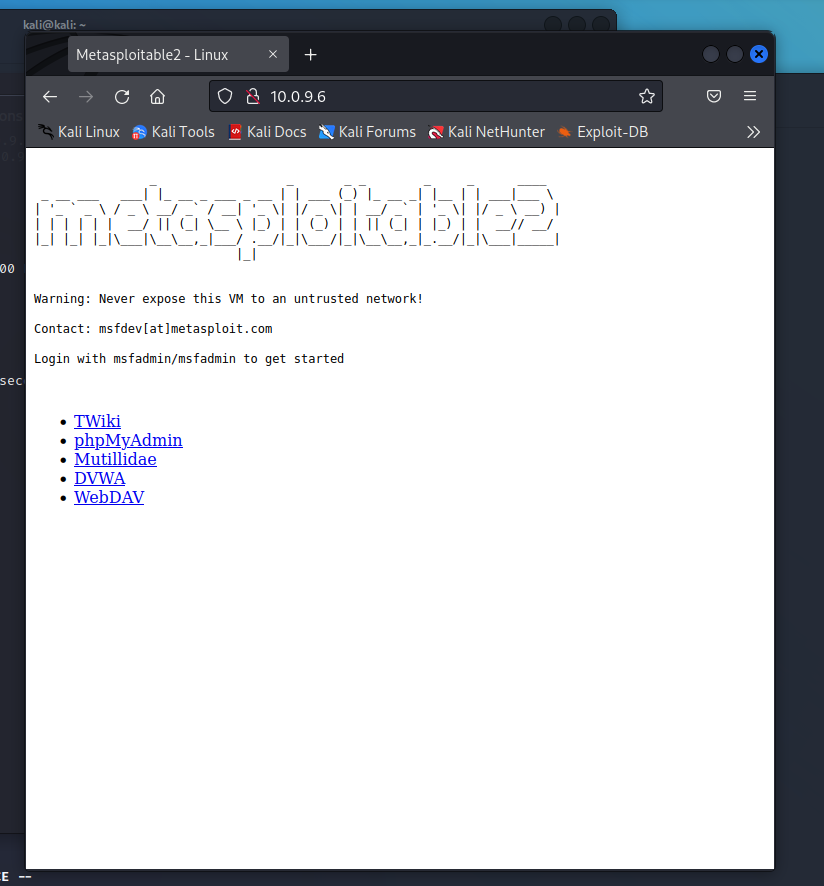
****

Figure 11: We connected to the host via the browser on port 80 by typing 10.0.9.6:80

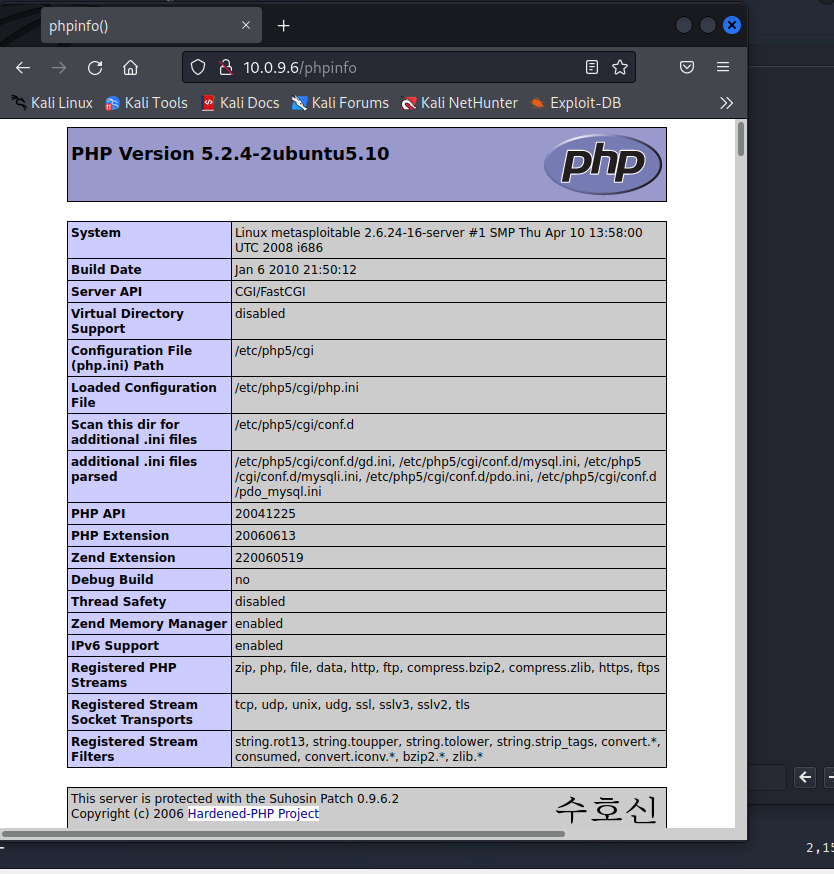
****

Figure 12: we navigated to the php info page adding /phpinfo to the landing page url

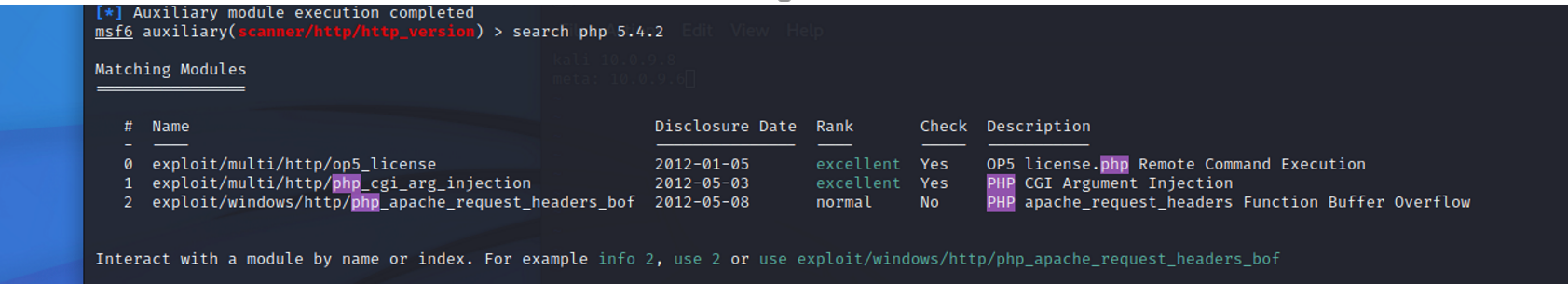
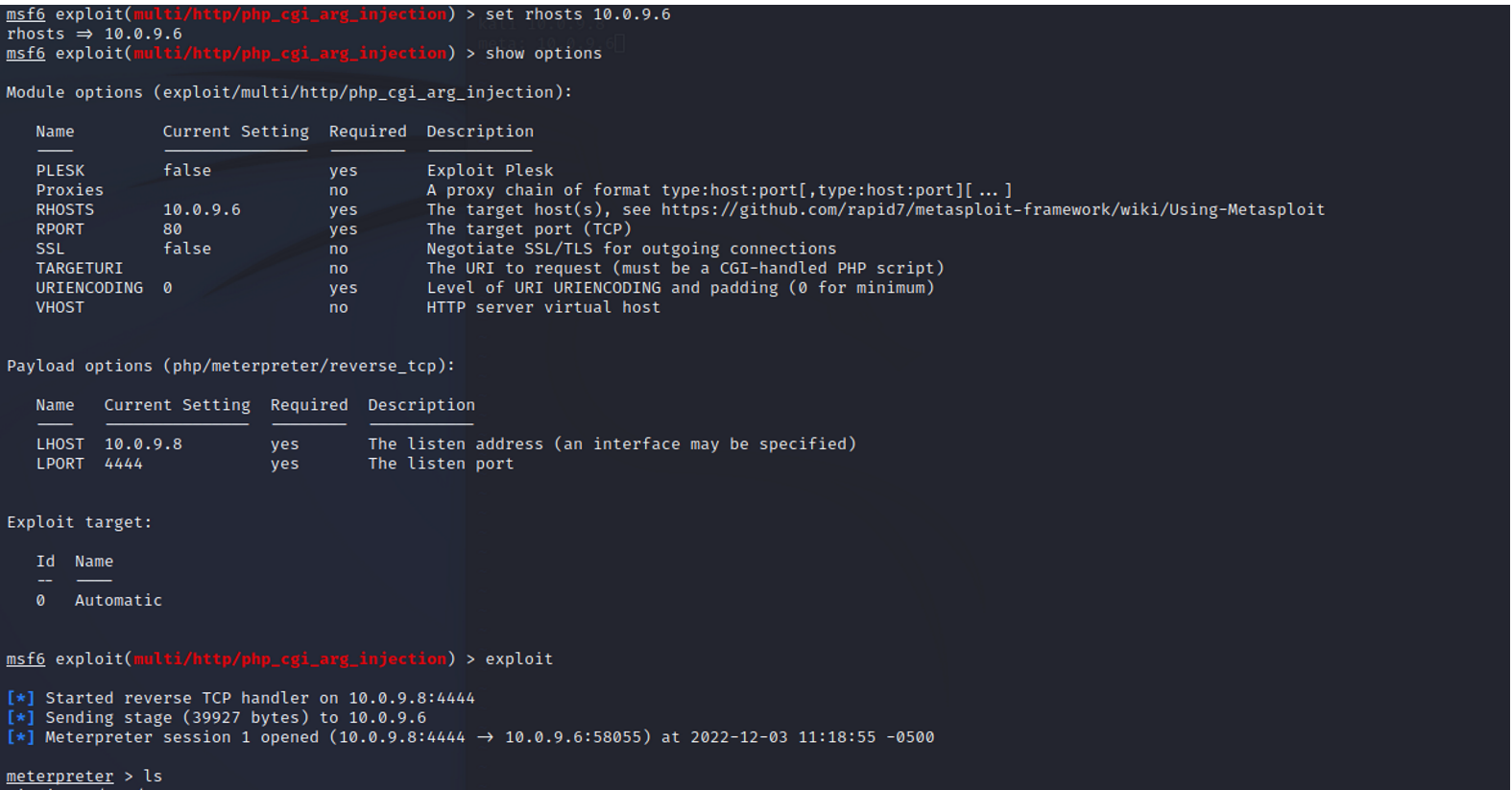
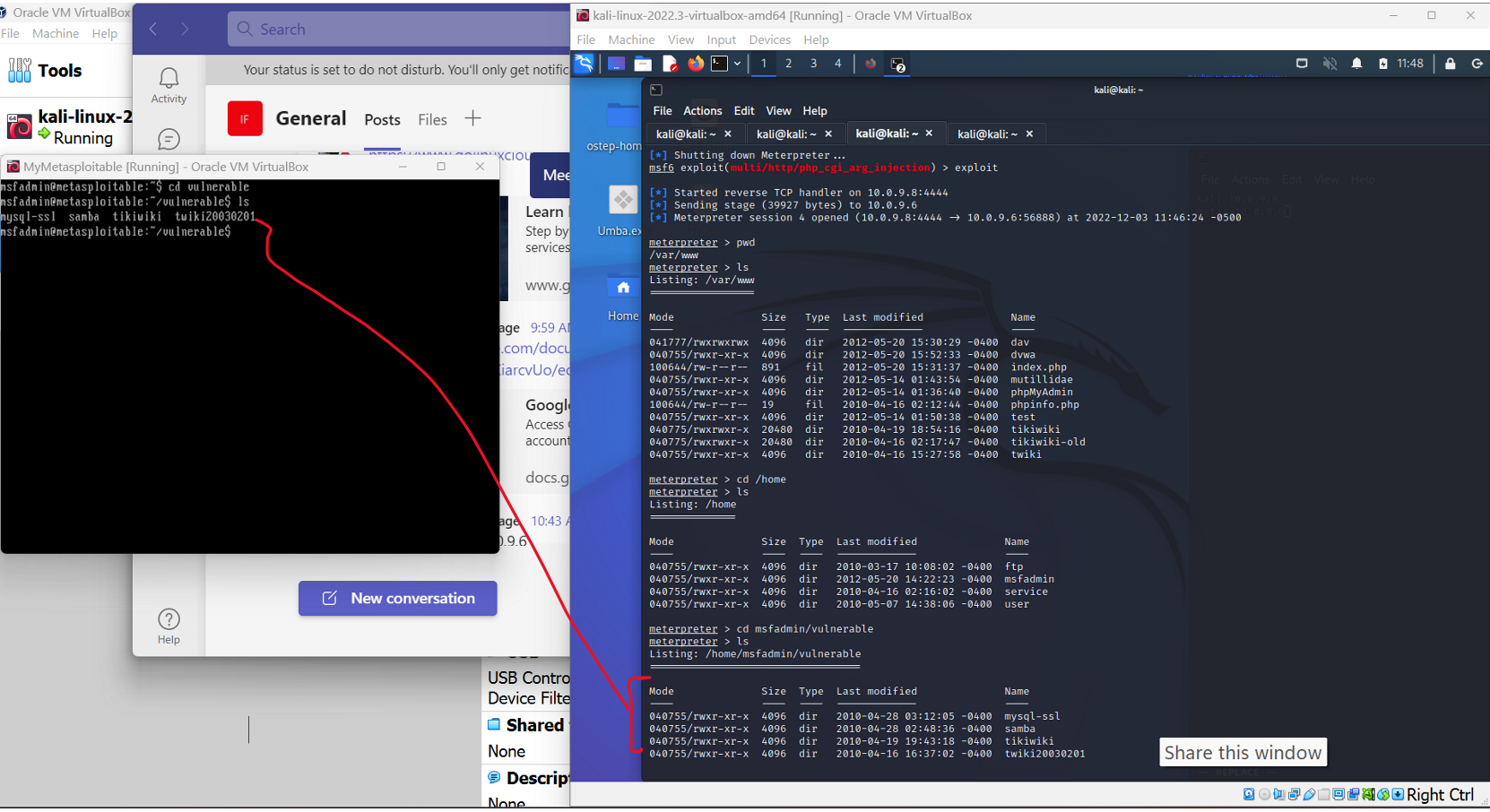
****

Figure 13: Option 1 is the argument injection vulnerability we used to gain access to the host’s machine  
****  
Figure 14: Metasploit creates a reverse tcp session to get access to the host machine  
  
****  
Figure 15: The Kali machine on the right can see the files on the victim machine on the left.

PostgreSQL - Port 5432(Joshua)

I searched Metasploit Framework for postgresql which brought back multiple results. I selected one that clearly was labeled Linux and ranked “excellent,” as I knew that the target system’s operating system was linux from my initial port scan, and assumed an exploit ranked “excellent” would be most effective (Figure 16). The exploit I used was “exploit/linux/postgres/postgres\_payload.” I then configured RHOSTS with the target system’s IP address and LHOST with my IP address and ran the program (Figures 17 and 18). This gave me an open meterpreter session, through which I was able to access the files on the target system; giving me full access to download and alter any files, as well as escalate privilege.

## Recommended Solutions for PostgreSQL Vulnerabilities

The penetration revealed that postgresql allowed connection without a password, and once connected, I was able to freely interact with the file system and could have escalated privileges through meterpreter. Because PostgreSQL is a database, it “assumes that anyone connected to the server is authorized to access the database,” so it’s important to make sure that the database is set up to use a “non-trust” authentication method; this can be easily configured in the ”pg\_hba.conf” file (Tunggal, 2022). Another method would be to establish an access list of approved users, and then establish roles that would provide additional control over access within the organization; roles could be established to limit users to basic view access or allow them to edit the database, roles could also limit a user’s access to a certain area of the database; because each user would have a unique password, it would still be advisable to enforce a strong password requirement to enhance security (*How to Secure PostgreSQL*, n.d.).

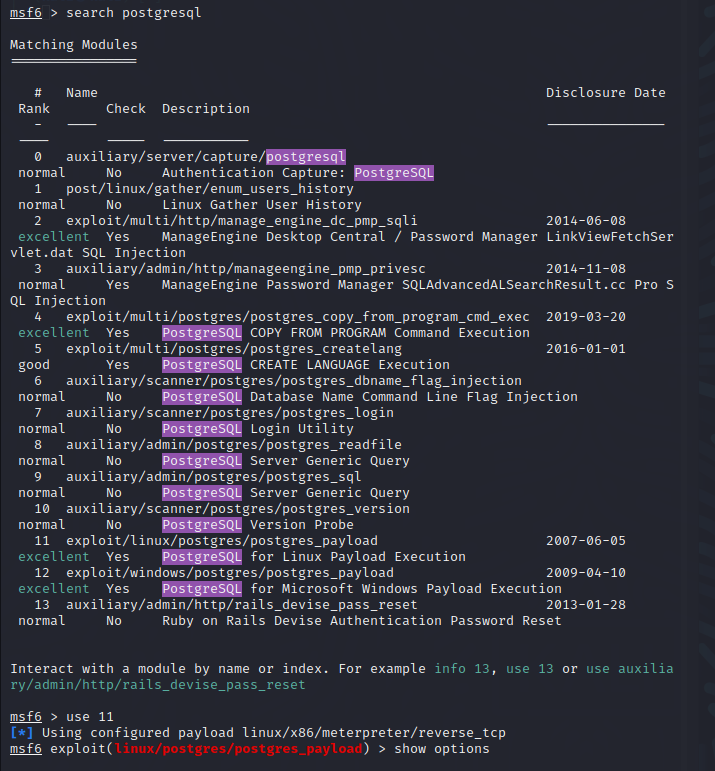
****

Figure 16: Searching Metasploit Framerowk for postgresql exploits, selecting option 11.

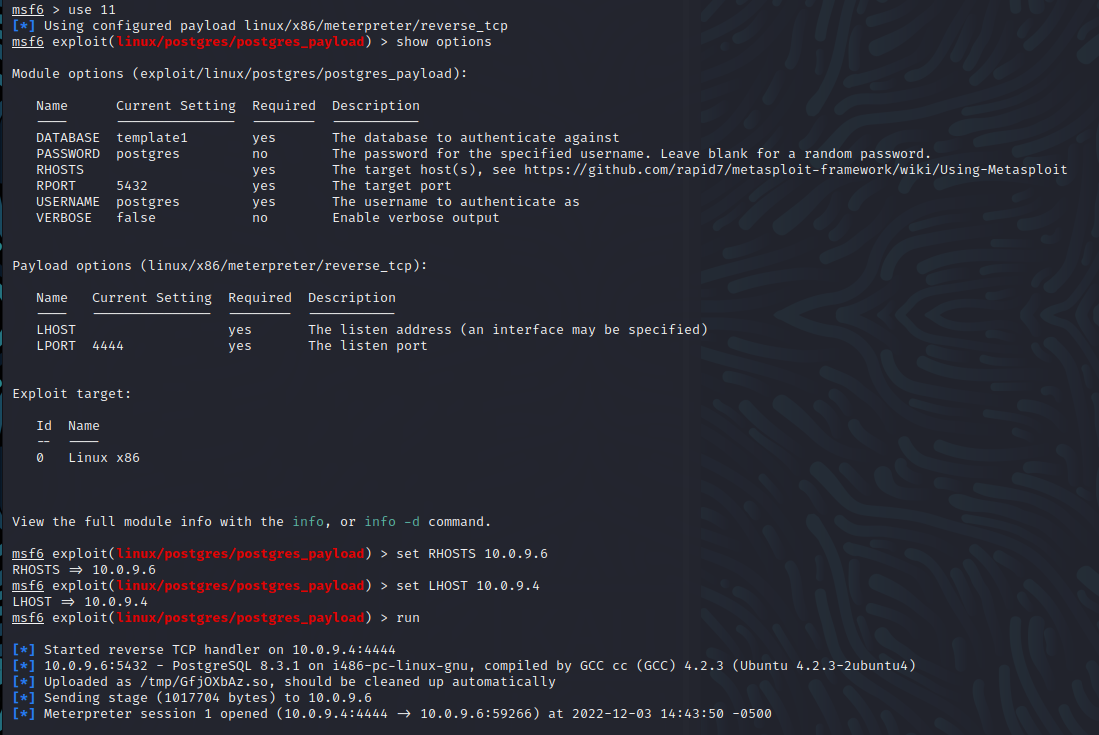
****

Figure 17: Setting parameters for postgresql exploit and running exploit, established Meterpreter session.

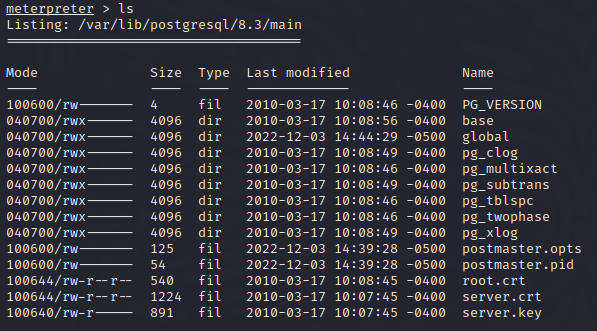
****

Figure 18: Running ls in Meterpreter to demonstrate access to the file system.

# VNC - Port 5900 (Joshua)

I searched Metasploit Framework for “vnc login” to find available exploits, one of the options was specifically for Windows, so I tried the other option: auxiliary/scanner/vnc/vnc\_login. Upon reviewing the options, it became clear that this module would run a brute force attack in effort at determining the password for vnc login on the target system (Figure 19). I configured RHOSTS to the target system’s IP address, and kept the password list provided by Metasploit. Upon running the program, Metasploit Framework was able to determine that the VNC password was “password” (Figure 20) I opened another terminal window and used the command “vncviewer” with the target system’s IP address, and entered the password when requested, which gave me root access to the system (Figure 21).

Recommended Solutions for VNC Vulnerabilities

The penetration test revealed that the VNC port was open, but required a password to access. The password on this system was set to “password,” which was extremely easy for a brute force attack to discover using Metasploit Fremework’s default password list. My first recommendation for addressing this would be to use a strong password for access to VNC; while VNC has other vulnerabilities, having the password gives the most direct access, and so this should be updated immediately using a strong password service or password manager. Beyond this, however, there are other steps that can be taken to improve VNC security: establishing allowed devices and blocking all others is an excellent way of improving VNC security, and there is security software that can be utilized in enterprise settings (Grustniy, 2019). Like with FTP, SSH tunnels can also be used to funnel connection traffic through a proxy and encrypt it (Geier, 2020).

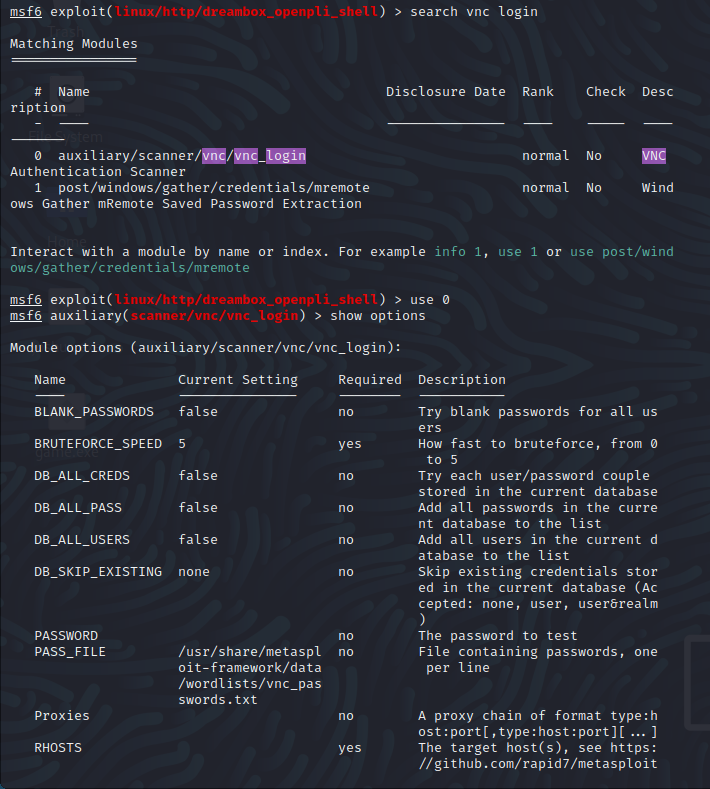
****

Figure 19: Searching Metasploit Framework for VNC exploits, reviewing parameters.

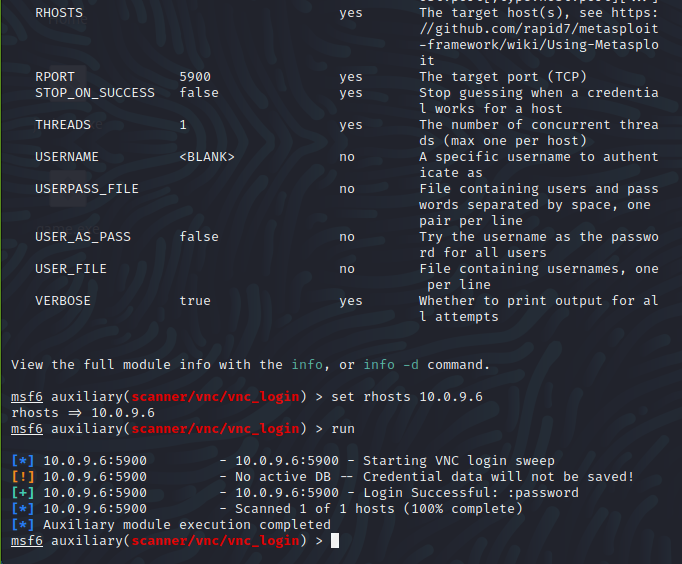
****

Figure 20: Setting parameters for VNC exploit and running exploit, discovered VNC password was “password”.

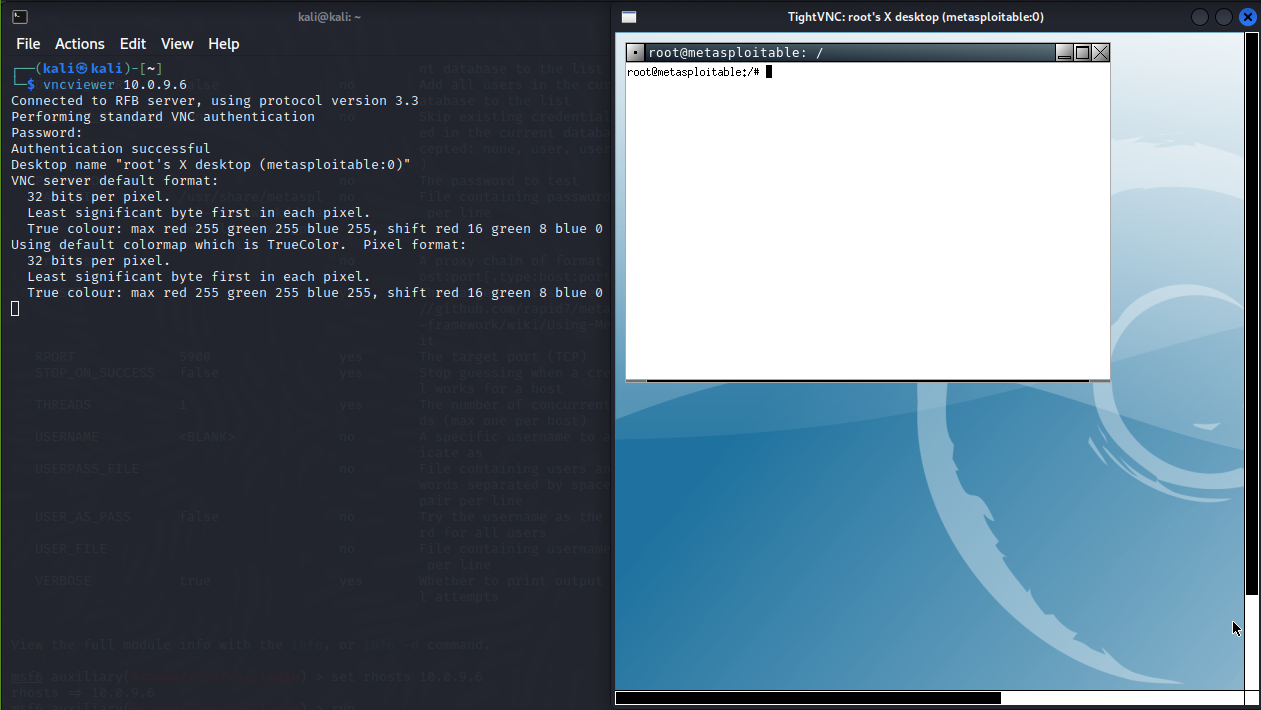
****

Figure 21: Using a separate Kali Terminal to connect to target system through VNC using the password discovered.

# Web Application - Discovered Vulnerabilities and Solutions (Kevin)

We found unsanitized input fields while testing the employee login portal. We created an SQL exception on purpose (Figure 22). Since an error occurred we concluded that the field accepted SQL inputs. Then, we tried the payload ‘admin #’ to bypass the login. Admin is a common account name used by developers in their development environment and the # is a comment tag used to ignore the rest of the query. Thus, we gained admin access to the employee portal (Figures 23 and 24). This is a threat to confidentiality and accessibility as anybody can access your employee’s personal information. Furthermore, a skillful SQL injection can also lead to privilege escalation as shown with this example.

## Recommended Solutions for Web Application SQL Vulnerabilities

It is recommended to avoid verbose and unnecessary error messages. Like we have seen in the example above, error messages can reveal information about the system. We recommend using a generic error message like “Username or password is incorrect”. Proper input sanitization is the solution to SQL injections. Sanitizing the input fields will prevent the user from weaponizing the SQL script. This can be done with prepared statements (OWASP - SQL injection prevention cheat sheet, 2022 ). Prepare statements treat the query and the input string as separate entities. Any input from the user is strictly used as a parameter and cannot change the query.

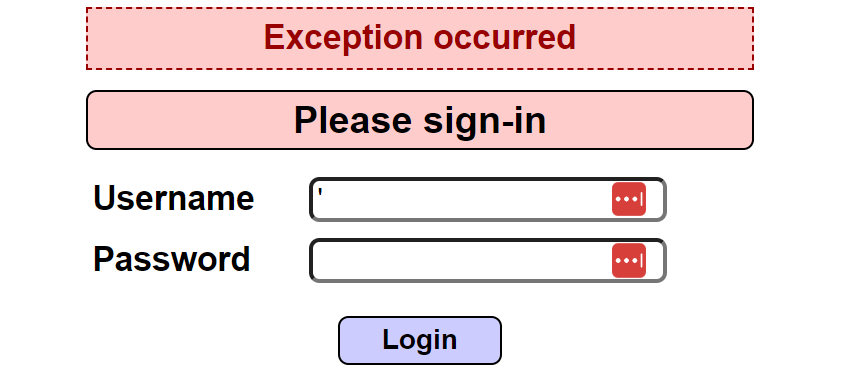
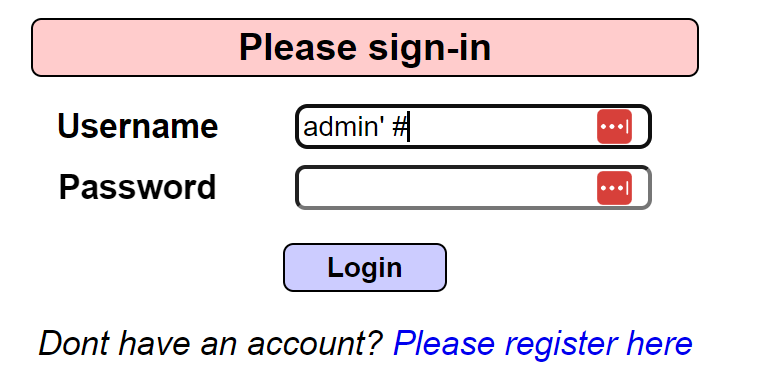


Figure 22: the comma creates an SQL exception denoted by the “Exception Occured” text.

  
Figure 23: used the ‘admin #’ payload to access the portal with full privilege.

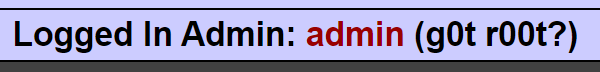


Figure 24: the portal was accessed with admin privileges.

## 

## Security Report Summary

Our test of the eCorp facility and systems revealed vulnerabilities in several potential areas:

Physical vulnerabilities include unsecured entrances, lack of monitoring and procedures for limiting guest access, and poorly secured servers. An attacker having physical access to your building or server gives them the easiest means of infiltrating your systems, so we advise revising your security policies, updating and upgrading locks, and adding cameras to ensure these vulnerabilities are better protected.

Personnel and policy vulnerabilities include lack of password policies, lack of end-point encryption for the use of personal devices, lack of firewall, and lack of security awareness trainings. Uninformed employees are often the weakest link that provides access to an entire system for a hacker, by simply clicking a link in an email or visiting a suspicious website, malware can be easily introduced to your systems; password policies should be enforced at the administrative level so that employees must create a strong password for their account, a firewall should be implemented to prevent risks associated with visiting suspicious sites, VPN services should be required for using personal devices, and mandatory security trainings and awareness campaigns should be regularly offered to all employees.

Our testing of your systems revealed numerous open ports on your system; attackers use open ports as a means of accessing systems, and as out testing revealed, many of these ports were vulnerabile to attack. A firewall would be a good first step to provide some coverage of open ports, but we strongly advise closing many of these ports, as there is no reason for them to be open. Unsecure services like FTP and HTTP should be discontinued and moved to their newer, secured versions, which offer additional encryption. Passwords for SSH and VNC should changed to strong passwords, and passwords should be tied to individual accounts, rather than the overall system. SSH Tunnels should also be used to provide encryption.

Finally, your web application is vulnerable to SQL injection attacks; by simply adding a string to the input, users are able to gain access to your employee portal’s administrative account, which can reveal sensitive information about your employees. Other SQL injection attacks could be used to identify accountnames and passwords, so this vulnerability should be addressed as soon as possible. We recommend input sanitization and using prepared statements to prevent form entries from being able to query the database.

Overall, our test revealed many concerning vulnerabilities, and we would advise that you work with contracted security specialists in order to find solutions that can help you quickly secure the most severe vulnerabilities.

**Works cited:**

*8 Tips for Developing a Security Awareness Program*. (2019, July 7). Commonwealth Financial Network.<https://www.commonwealth.com/insights/8-tips-for-developing-a-security-awareness-program>

*10 Essential Tips for Securing FTP and SFTP Servers*. (n.d.).<https://www.fortra.com/blog/10-essential-tips-securing-ftp-and-sftp-servers>

Chouffani, R., & Wigmore, I. (2021, May 20). *BYOD (bring your own device)*. TechTarget. Retrieved October 21, 2022, from<https://www.techtarget.com/whatis/definition/BYOD-bring-your-own-device>

Din, A. (2022, June 20). *What Is BYOD? Bring Your Own Device Security Policy*. Heimdal Security Blog. Retrieved October 21, 2022, from<https://heimdalsecurity.com/blog/byod-bring-your-own-device/>

*Estimating Password Cracking Times*. (n.d.). Better Buys.<https://www.betterbuys.com/estimating-password-cracking-times/>

Geier, E. (2020, November 10). *Securing a VNC Server on Linux with SSH*. ServerWatch.<https://www.serverwatch.com/guides/securing-a-vnc-server-on-linux-with-ssh/>

Gromek. (2002, February 12). *Securing FTP Authentication*. SANS.<https://www.sans.org/white-papers/374/>

Grustniy, L. (2019, November 28). *VNC remote access vulnerabilities*.<https://usa.kaspersky.com/blog/vnc-vulnerabilities/19962/>

​​*How to Recognize and Avoid Phishing Scams*. (2022, October 25). Consumer Advice.<https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams>

How to Secure PostgreSQL: Security Hardening Best Practices & Tips. (n.d.). EDB.<https://www.enterprisedb.com/blog/how-to-secure-postgresql-security-hardening-best-practices-checklist-tips-encryption-authentication-vulnerabilities>

*Kaspersky: Secure Password Check*. (n.d.).<https://password.kaspersky.com/>

Lawson, Kent. (2018, March 8). *Managing BYOD Security Threats For an On-The-Go Workforce*. LinkedIn. Retrieved October 21, 2022, from<https://www.linkedin.com/pulse/managing-byod-security-threats-on-the-go-workforce-kent/>

Maxwell, J. (2022, February 7). *5 reasons why businesses need Network Firewall Security*.<https://www.cm-alliance.com/cybersecurity-blog/5-reasons-why-businesses-need-network-firewall-security>

McKay, D. (2019, October 11). *The Best Ways to Secure Your SSH Server*. How-To Geek. <https://www.howtogeek.com/443156/the-best-ways-to-secure-your-ssh-server/>

Microsoft. (2022, November 22). *Password policy recommendations - Microsoft 365 admin*. Microsoft Learn.<https://learn.microsoft.com/en-us/microsoft-365/admin/misc/password-policy-recommendations?view=o365-worldwide>

Microsoft. (n.d.). *Set up an authenticator app as a two-step verification method - Microsoft Support*.<https://support.microsoft.com/en-us/account-billing/set-up-an-authenticator-app-as-a-two-step-verification-method-2db39828-15e1-4614-b825-6e2b524e7c95>

Minhas. (2021, April 18). *A Beginner’s Guide to Malicious Websites*. MakeUseOf.<https://www.makeuseof.com/beginners-guide-to-malicious-websites/>

Offensive Security. (2019, November 1). *Scanner SSH Auxiliary Modules - Metasploit Unleashed*. <https://www.offensive-security.com/metasploit-unleashed/scanner-ssh-auxiliary-modules/>

OWASP Mutillidae. (n.d.). Login - 128.198.49.198:8102. Retrieved December 13, 2022, from <http://128.198.49.198:8102/mutillidae/index.php?page=login.php>

OWASP. (n.d.). SQL injection prevention cheat sheet¶. SQL Injection Prevention - OWASP Cheat Sheet Series. Retrieved December 13, 2022, from <https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html>

PHP CGI Argument Injection. Rapid7. (n.d.). Retrieved December 13, 2022, <https://www.rapid7.com/db/modules/exploit/multi/http/php_cgi_arg_injection/>

Tatianna. (2018, November 5). *Spoofing: RFID and SMS*. Cybrary. <https://www.cybrary.it/blog/2018/11/spoofing-rfid-sms/>

Tunggal. (2022, May 9). *How to Secure Your PostgreSQL Database*. UpGuard.<https://www.upguard.com/blog/10-ways-to-bolster-postgresql-security>

*UKM Zero Trust SSH Encryption Key Management*. (n.d.). <https://www.ssh.com/products/universal-ssh-key-manager/>

*What is OpenSSH?* (n.d.). <https://www.ssh.com/academy/ssh/openssh>

*What is Security Awareness Training and Why is it Important?* (n.d.). Mimecast.<https://www.mimecast.com/content/what-is-security-awareness-training/>