Computer Fraud and Security
ISSN (online): 1873-7056

Securing Remote Access: Addressing Email and Remote Desktop Protocol Vulnerabilities in Corporate Environments through Multifaceted Solutions

Eric Blancaflor[1], Ronald Bernardo[1], Reanne Angela Buccat[1], Hayya Michaela Cajuday[1], Xyron Wheckxz Nucum[1], Nathalie Rein Ocampo[1]
[1]School of Information and Technology, Mapúa University, Philippines

Abstract:

Introduction: Remote-desktop software has become more popular since COVID-19 caused people to work from home. Remote desktop software helps administer remote machines, but it creates additional system vulnerabilities which may be exploited for unauthorized access to systems.

Objectives: This paper explores the complex issues of protecting business settings against email phishing attacks and vulnerabilities in the Remote Desktop Protocol (RDP). It carefully looks at how vulnerable RDP-based apps are to different kinds of attacks, like rootkits and URL phishing, and it suggests strong defenses like implementing Secure Shell (SSH) and Network Level Authentication (NLA).

Methods: The study investigates the nuances of email phishing concurrently, simulating attack scenarios and evaluating the efficacy of mitigation strategies such as Avast and Netcraft using the GoPhish program. Through an examination of these vulnerabilities and mitigation techniques, the study seeks to offer practical suggestions for enhancing network resilience and security for remote access.

Results: This study investigates corporate environment vulnerabilities in great detail, with special attention to email phishing attacks and flaws in the Remote Desktop Protocol (RDP). In order to improve network resilience and security, the study emphasizes how crucial it is to fix these weaknesses through in-depth analysis and attack scenario simulation. Through an analysis of the vulnerability of email systems and RDP-based apps to a range of attacks, such as malware, rootkits, and URL phishing, the study offers important insights into the complex nature of cyber threats.

Conclusions: The paper highlights the necessity of ongoing education and awareness campaigns to enable individuals and businesses to recognize and successfully block phishing efforts. By employing technologies such as GoPhish for simulation testing and empirical observations, practical suggestions are put forth to enhance the security of remote access and counteract email-based threats.

Keywords: Remote Desktop Protocol, Seth, Kali Linux

INTRODUCTION

Microsoft created the secure network communications protocol known as remote desktop protocol, or RDP. It allows users to remotely access their physical work desktop PCs and allows network managers to remotely troubleshoot issues that specific users face. In order to transfer data back and forth between the linked machines—the remote desktop and the computer that is presently in use—the RDP protocol establishes a dedicated network channel. For this, network port 3389 is always used. TCP/IP, the transport protocol used for most forms of Internet traffic, is utilized over this channel to send all essential data, including keystrokes, mouse movements, and desktop displays [1]. Remote-desktop software has become more popular since COVID-19 caused people to work from home. Remote desktop software helps administer remote machines, but it creates additional system vulnerabilities which may be exploited for unauthorized access to systems [2].

Email URL phishing is the most common security issue. In the world of cybersecurity, despite having many defenses against and methods of mitigation, phishing attacks remain one of the most prevalent attacks that are conducted on a corporate basis [3]. These attacks make full use of email vulnerabilities, luring unknowing and unsuspecting victims to click their malicious links and opening malicious files attachments [4]. The repercussions of

a successful phishing attack could be severe as it could result in data breaches, financial loss, and possible identity theft. The case study will conduct and simulate a phishing scenario through an E-mail web service.

Relevance of the Study

The study's relevance is underscored by its timely examination of the growing reliance on remote desktop applications, accelerated by the COVID-19 pandemic's impact on remote work practices. As businesses and individuals increasingly adopt tools like TeamViewer utilizing Remote Desktop Protocol (RDP), vulnerabilities in these systems become more pronounced.

Simultaneously, the study addresses the modernized techniques of phishing via deceptive email links, posing significant threats to organizational and user security. By identifying and addressing these vulnerabilities, the study aims to protect sensitive data, mitigate cyberattacks, and ensure network resilience in an environment increasingly susceptible to remote access and email-based threats.

OBJECTIVE OF THE STUDY

The purpose of this study is to address vulnerabilities in Remote Desktop Protocol (RDP)-based apps and identify how email phishing operates using GoPhish software. The paper will assess RDP's vulnerability to man-in-the-middle attacks and suggest countermeasures including using Secure Shell (SSH) and NLA. Additionally, the study will simulate an attack for phishing by generating a link in email. The study provides actionable advice to strengthen network resilience, remote access security using simulated situations and empirical observations and further apply a layered protection for incoming phishing scams.

To achieve the study's purpose, its objectives are to:

- To analyze the susceptibility of RDP-based applications and emailing systems to rootkits, malware, man-in-the-middle attacks, spamming, and URL phishing.
- To implement a simulation testing for RDP and Email phishing using Gophish.
- To provide solutions like using SSH and making use of NLA settings, software such as Avast and Netcraft was also utilized against email url phishing.
- To make doable recommendations for enhancing remote access security, network resilience, security software utilization and raise awareness for these kinds of attacks.

Scope and Limitations

Two penetration testing will be performed. The first test will focus on Window's RDP-based application, Remote Desktop Connection, and the second part will focus on email phishing vulnerabilities. The penetration testing for RDP will only use Window's Remote Desktop Connection application in Oracle VM VirtualBox for a simulated and controlled environment, as well as Kali Linux's Seth tool. For the solution, Window's Network Level Authentication settings will be applied, and therefore no other applications will be used.

An email phishing utilized on a software will be implemented. The study's purview includes a fictitious assault scenario customized for the business. The attack's approach, its aftermath, and the effectiveness of security technologies in temporarily and permanently lessening its effects will all be examined by researchers. Furthermore, Gophish will be used and further mitigation techniques will be implemented using security programs such as Avast, and Netcraft extension.

LITERATURE REVIEW

Remote Desktop Software in Industries

Remote Desktop Protocol is not just used in the IT industry. Due to the convenience of the application and protocol, it is also used in Industrial Control Systems (ICS) that has a large geographic area [6, 10]. RDP is also used in healthcare systems and other critical sectors [13]. One of the advantages that workers get from using the RDP is the faster and easier accomplishment of routine checking and its complete access and control to the machine. However, as cited by Ramirez [10], as much as the convenience of RDP offers workers complete access, so will attackers that can hack into the protocol with various techniques such as session hijacking, brute force attacks, and man in the middle attacks. One such incident is the attack in Florida in February of 2021 where the water treatment facility was attacked, and harmful chemicals were mixed into the water supply system. Two attacks in different years, 2016 and 2022, happened in Ukraine, involving their power grid and another in the US in May 2021 [10]. As such, defense mechanisms such as honeypots were implemented.

Although Remote Desktop Protocol is a Microsoft proprietary protocol, a trusted brand and software developer, it still has weaknesses that may be exploited. As Nyakomitta et al. [8] discussed, RDP has authentication issues such as user identification, authorization, and session management. There have also been attacks such as that of BlueKeep and DejaBlue which Windows has already patched up in 2019 [8] and CrySiS/Dharma ransomware which used RDP as a propagation system as a persistent threat [10]. The exploitation of the weakness of RDP can also affect services that use the same port as RDP such as, but not limited to mstsc.exe, RTSApp.exe, ws_TunnelService.exe, and Terminals.exe [9].

GoPhish as an Attack

A study entitled “Lets Go Phishing: A Phishing Awareness Campaign Using Smishing, Email Phishing and Social Media Phishing Tools” [7], is conducted to test how phishing attacks works in gophish and how many individuals are victimized or are likely to fall for this campaign. The study established fake credentials and fake user info that will target the respondent’s social media accounts, email and SMS, according to the study. After generating the page for a fake website using GoPhish, the attacker sends the link for phishing. It mainly identifies several factors for mitigations after the said attack because the conducted paper wants to provide how vulnerable users are in each platform they use. The study also focuses on providing awareness and protection for safe interaction with these sites.

The objective of the study “Cybersecurity Awareness: Investigating Students’ Susceptibility to Phishing Attacks for Sustainable Safe Email Usage in Academic Environment (A Case Study of a Nigerian Leading University)” [12], focuses on investigating the vulnerability of the students for this attack called phishing. The study also shows the possibility of the students to be a victim of this kind of malicious emails. In the testing phase, according to the paper, there are two phishing emails being tested to better comprehend and analyze how the students will respond to the said email. The server was up and is set to fully provide access for interaction once the students are directed to the web page.

The study by Luse and Burkman titled "Gophish: Implementing a Real-World Phishing Exercise to Teach Social Engineering" [13] details a class project in which students conducted a phishing exercise against actual targets. Students gained knowledge of the legal, technological, behavioral, analytical, and reporting facets of social engineering through collaboration with an outside corporate partner. The outcome gave the students a worthwhile educational experience in addition to providing useful data for a real-world organization. The research offers a prototype for a one-semester project that allows students to engage in hands-on social engineering learning. Students create a purpose statement, design the system, set up the environment, and carry out a phishing exercise on real employees in collaboration with a partnering firm. After that, students present the data based on their findings.

METHOD

As there are two security issues that the paper will address, there will also be two separate methodologies for them. Both will provide the steps for attack and defense. To simulate a man-in-the-middle (MITM) attack for RDP, the Kali Linux OS will be used in a virtual environment, along with Seth, a tool for launching MITM attacks on RDP connections. In the second portion of the RDP setup where proposed solutions are applied, a Network Level Authentication (NLA) will be put in place. After which, the effectiveness of the advanced setting for TeamViewer will then be tested against the MITM attack.

The study will use GoPhish to generate a link and use it to send in email. The researchers will then simulate ways on how to mitigate and block or mark as spam potential phishing links so that it would not reach employees in a corporate scenario. This study would serve as a warning and as an informative piece for companies and individuals on how phishing tactics are conducted by attackers. This could also provide insight on how they can continue using and browsing the web as safely and as securely as possible.

Case site of this study is in the ISP industry that uses various technologies to maintain their networks and sites. They use Remote Desktop Connection (RDC) and Teamviewer during their troubleshooting and some maintenance activities. These were used even more during the Pandemic and until now due to their assimilation of the work from home setup. With that, the higher positions are usually out of the office, while others are deployed onsite. Due to the need for guidance during some of the tasks, RDC is used to ease the completion and teaching of routines and troubleshooting.

The overall existence of email service on the web has become very prominent. Email is the most common messaging platform; Company A has several generating emails each day. Using this platform, it enables them to send and receive attachments, files and attached links for verification, accessibility, and work-related reasons. During this phase phishing links attached to the files of the company potentially can harm the production.

RDP Setup

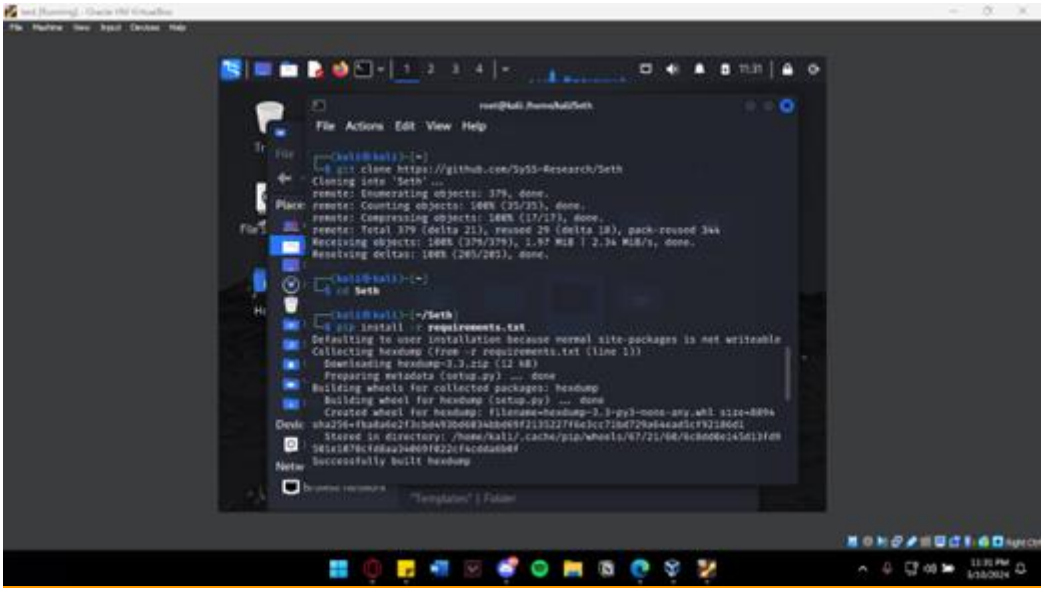

Figure 1. INSTALLATION OF SETH (Security Event and Threat Hunting)

The SETH (Security Event and Threat Hunting) setup procedure is shown in Figure 1. This process is necessary for identifying prospective threats and examining suspicious activity that could point to an upcoming attack. The first command line points to the SETH installation. Changing directories subsequently

guarantees that commands are carried out in the proper place. Lastly, installing the necessary packages guarantees SETH will function properly.

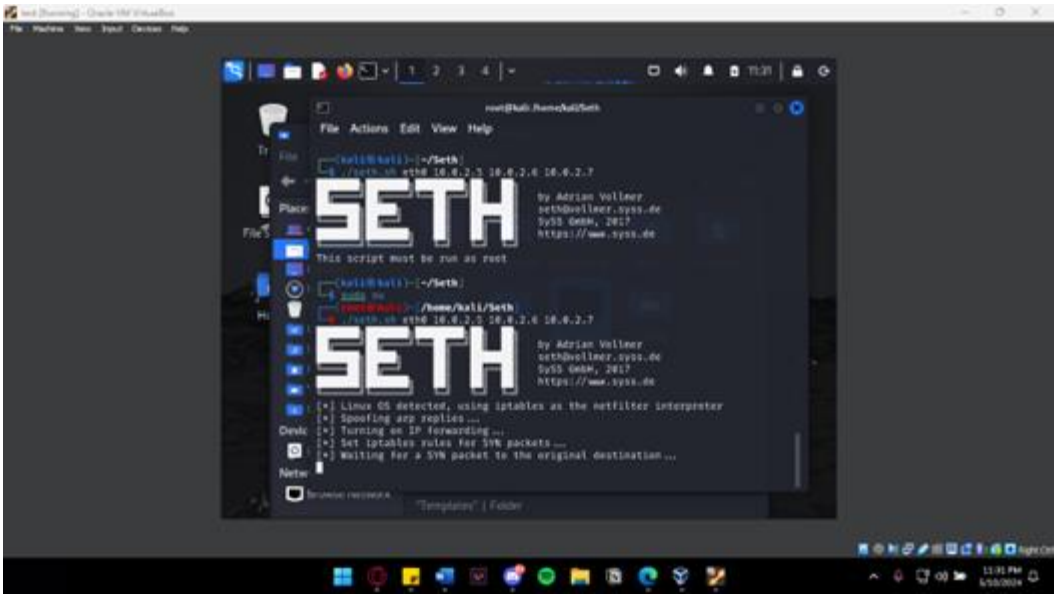

Figure 2. Attack Command for Seth

In Figure 2, the first line denotes the IP addresses of the relevant clients involved. Specifically, 10.0.2.5 represents the IP address of the Kali Linux system, while 10.0.2.6 and 10.0.2.7 correspond to the IP addresses of Client 1 and Client 2, respectively. To access system resources and execute commands with elevated privileges, the script needs to run as the root user. Following this, the second line uses "sudo su" to elevate privileges, resulting in a change from "kali@kali" to "root@kali" as the command prompt, indicating the transition to the root user.

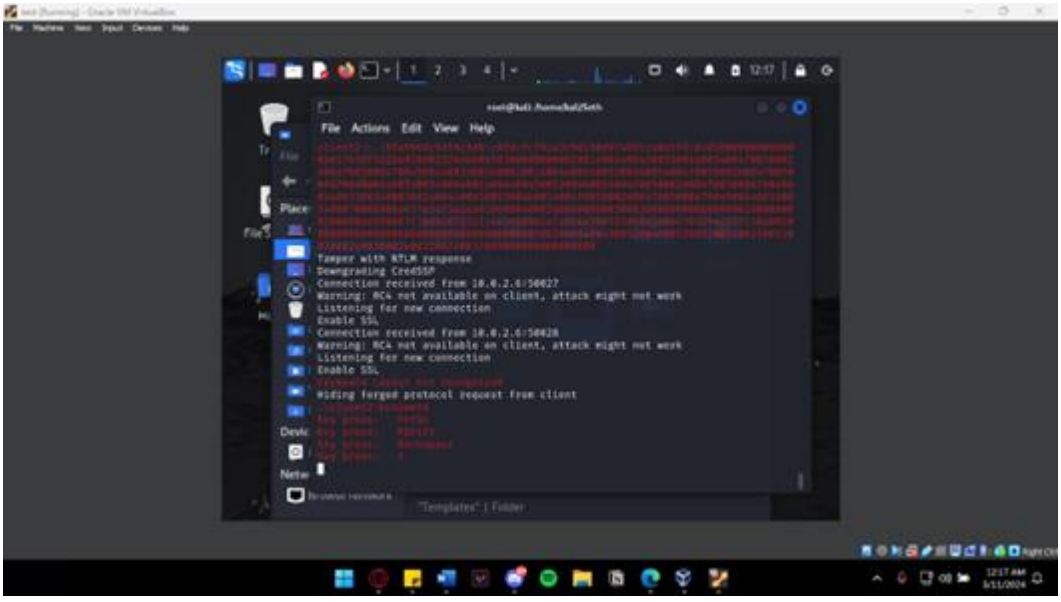

Figure 3. Successful Attack and Key logging

A successful attack is illustrated in Figure 3. The hash characters are represented by the long red strings above. The password belonging to Client 2 has been discovered or accessed beneath these hashes. This suggests that the attacker has effectively circumvented security protocols and obtained unauthorized access to Client 2's password. The

existence of the hashes implies that the attacker might have extracted the hashed password from its plaintext version using methods like hash extraction or password cracking. This breach emphasizes how serious the security flaw is and how crucial it is to have strong security measures in place to keep private data safe from prying eyes.

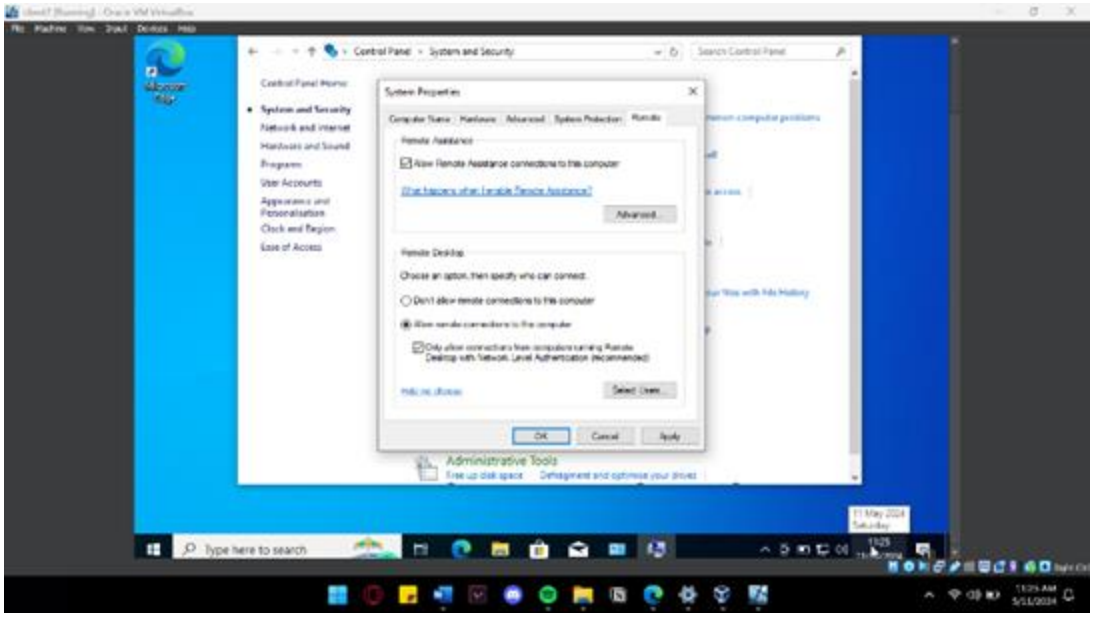

Figure 4. NLA Network Level Authentication Implementation

Figure 4 displays the system properties and security settings related to the Remote Desktop Protocol (RDP). These settings include the activation of Network Level Authentication (NLA), which enhances security by requiring authentication before a remote desktop connection is established. Enabling NLA serves as a defense mechanism against the attacks depicted in the preceding figures.

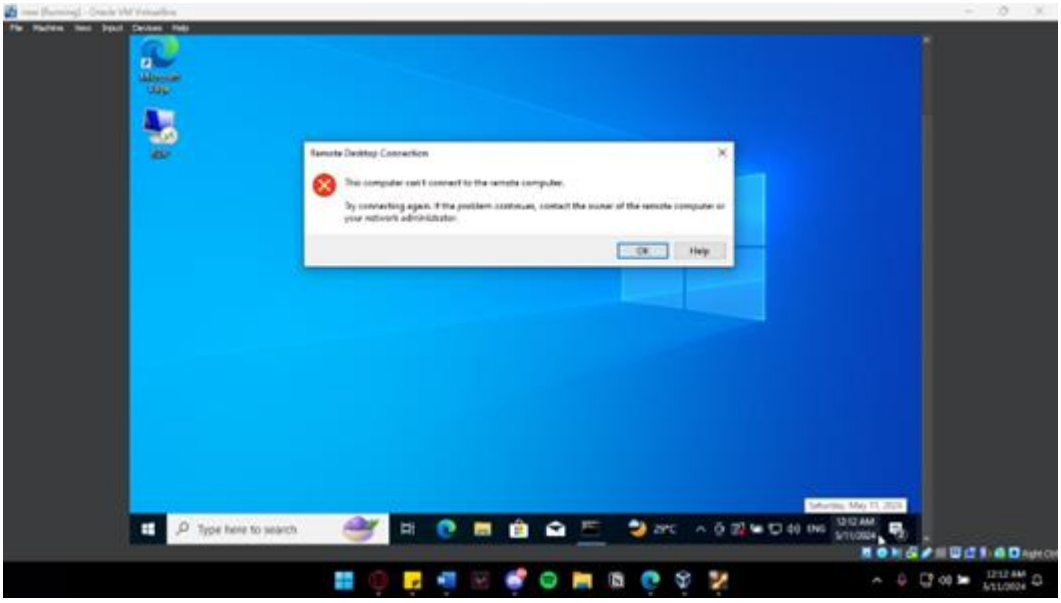

Figure 5. NLA Network Level Authentication Implementation

Prioritizing Network Level Authentication (NLA) is crucial for enhancing security against possible attacks on the remote desktop protocol (RDP). To do this, you must enable NLA protocols in your desktop settings. Open the RDP

settings and select the remote tab to get started. Make sure that every checkbox pertaining to NLA is checked off here. This process considerably lowers the possibility of unwanted access by authenticating users who are trying to connect to your desktop before allowing access. You strengthen your system's security and protect it from possible attacks by putting these preventative steps into practice. Another possible solution would be the transferring of the port that RDP is using to another port in order to make use of more secure protocols such as SSH or port 443 [12]. Group Policy settings in the Active Directory can also be used to enforce some rules and limitations for the access of remotely controlled devices.

Email Technical Setup

This study utilized GoPhish for the attacks to easily start phishing campaigns and send phishing emails to multiple people at once. GoPhish is an open-source framework that provides support for creation of phishing email templates, landing pages, sending profiles, and campaign settings. We used a virtual machine with Kali Linux OS as a vps to harness the GoPhish interface. To do set this up we installed GoPhish in a separate directory using the root system of Kali Linux.

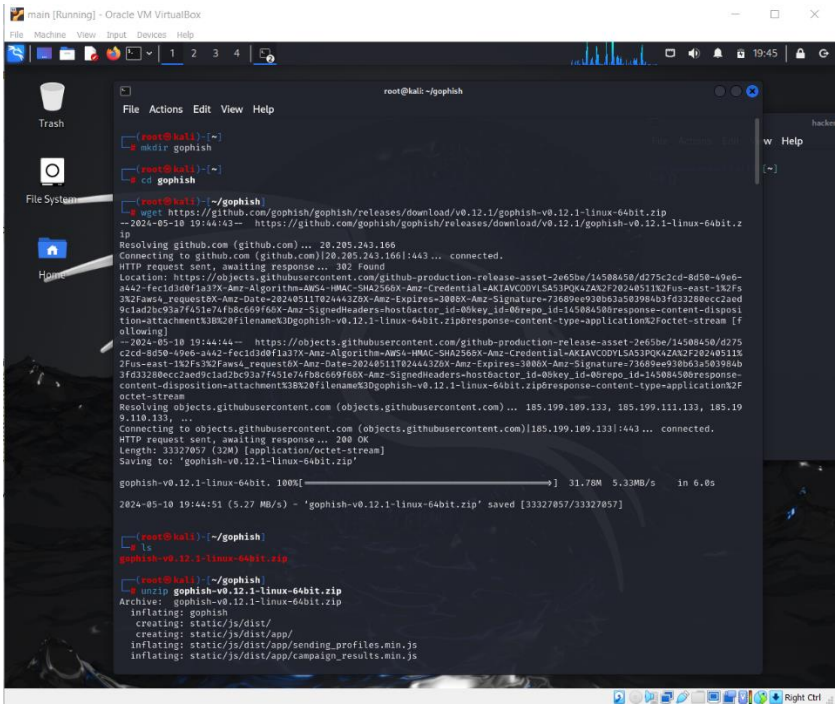

Figure 6. GoPhish Installation

After installation (see figure 6), we setup the GoPhish config file to be accessible through the Kali Linux ip instead of being accessible only to the localhost 127.0.0.1.

After setting up and making GoPhish executable. It is launched and the UI can be opened through the host desktop through the IP address of the Kali Linux server and the set-up port number in the config file [0.0.0.0:3333].

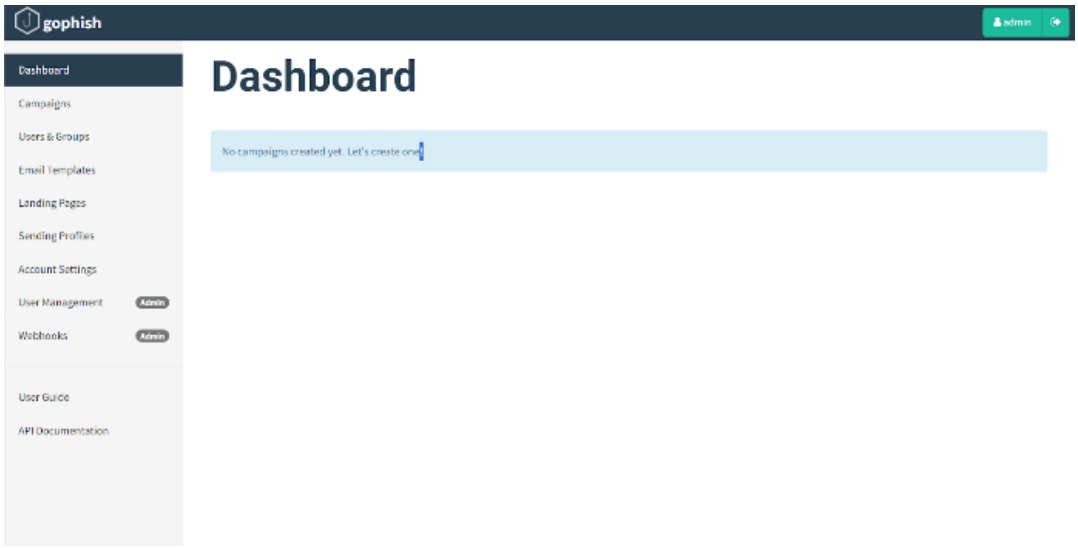

Figure 7. GoPhish Dashboard

We then set up campaigns by setting up email templates, landing pages, groups, and sending profiles to launch campaigns. We will be using a dummy email: Kevin Ball <hellohellobaby08@outlook.com>. The email will be sent through the SMTP server of outlook from this dummy email account. The Email template will then be distributed to group profiles from the setup sending profile waiting to be clicked on and redirect the user to the setup landing page. GoPhish dashboard is shown in figure 7.

After configuring these necessary templates, we will use them to launch a campaign on a modified and configured group of users. The sender template will email everyone in the configured group the Email template that we configured, and it will contain the landing page upon click. It will redirect the victim to the phishing page.

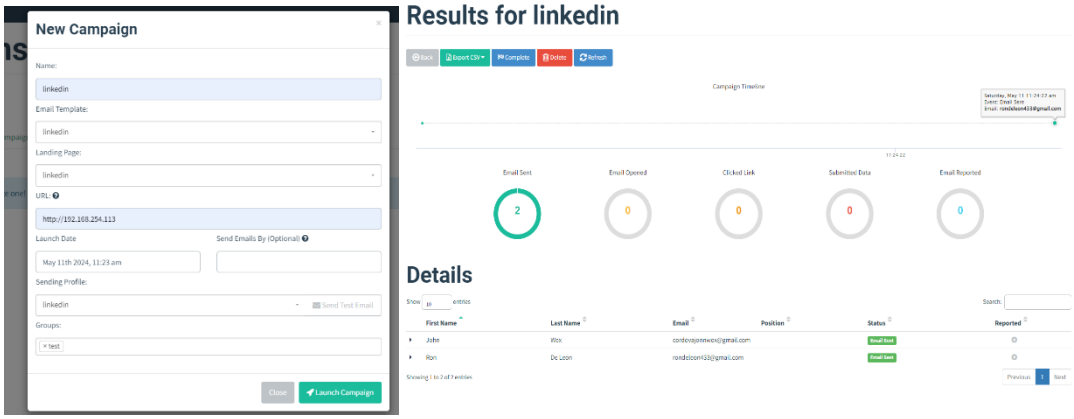

Figure 8. GoPhish Campaign Dashboard

After launching the campaign, shown in figure 8, targets indicated in the group's page will receive an email that looks like the landing page that we configured. The victim will then be prompted to login when they click the link. After they put in their credentials and press the sign in button, the inputs will be sent back to the GoPhish UI. The user will then be redirected to the original linked in login website.

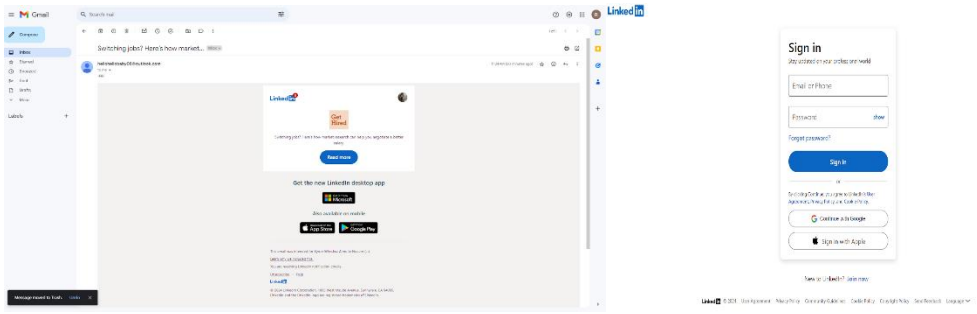

Figure 9. Receiving Attack

This will all be prompted in the Dashboard of the GoPhish tool-see figure 9. The attacker can also see information such as the tokens used for the handshake, the device the user used for the login, the OS and browser version they use along with their credentials. During the execution of the GoPhish software, the perpetrator successfully obtained the credentials of the user who clicked and logged into the web page. The instance of login stored the values in GoPhish database and presented the result from the perpetrator. Details were also presented below the GoPhish interface. Phishers can always be tricky, and users can be tricked if their protection level in their system is low. In this phase, anti-software such as with premium benefits are mostly secured and can be a defender for such an attack. There are also ways to identify if a certain URL link from email is legible or not such as using extension browser for phishing detection mail or secure your connection in your browser.

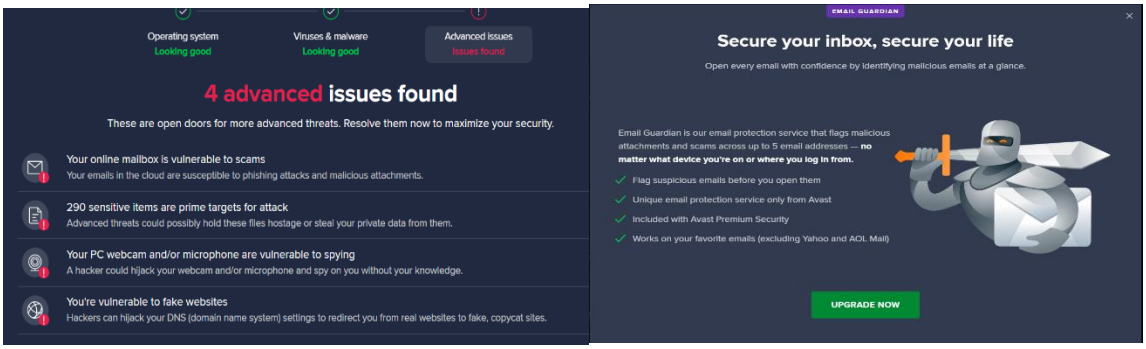

Figure 10. Avast Report

The study conducted a run scan in Avast and it generated four advanced issues in the system including the susceptibility of mail to phishing attacks- see figure 10. Besides, Avast Premium can also secure the overall protection against the threat of phishing. This protection flags malicious attachment scams and links and has a unique protection service. This feature will also safeguard the user from different kinds of attacks on the internet. Additionally, install anti-phishing extensions services on web browser Chrome like Netcraft to enable another protection layer on your account against phishers. And users should always check their secure connection on this tab to determine whether their connection to these web pages are secured and fully protected.

CONCLUSION

To sum up, this study investigates corporate environment vulnerabilities in great detail, with special attention to email phishing attacks and flaws in the Remote Desktop Protocol (RDP). In order to improve network resilience and security, the study emphasizes how crucial it is to fix these weaknesses through in-depth analysis and attack scenario simulation. Through an analysis of the vulnerability of email systems and RDP-based apps to a range of attacks, such

as malware, rootkits, and URL phishing, the study offers important insights into the complex nature of cyber threats. Risk mitigation techniques that must be used include the use of strong defense mechanisms like Secure Shell (SSH), Network Level Authentication (NLA), and security software like Avast and Netcraft. In addition, the research highlights the necessity of ongoing education and awareness campaigns to enable individuals and businesses to recognize and successfully block phishing efforts. By employing technologies such as GoPhish for simulation testing and empirical observations, practical suggestions are put forth to enhance the security of remote access and counteract email-based threats. In order to protect sensitive data and guarantee a secure computing environment in the face of evolving cyber threats, the study ultimately emphasizes the significance of proactive measures and layered protection solutions.

REFERENCES

[1] Cloudflare. 2025. What is the Remote Desktop Protocol (RDP)? [Online]. Available: https://www.cloudflare.com/learning/access-management/what-is-the-remote-desktop-protocol/

[2] D. Noble, “Behavioral Characterization of Attacks on the Remote Desktop Protocol (RDP),” 2022, 129 pages. [Online]. Available: https://apps.dtic.mil/sti/trecms/pdf/AD1201693.pdf

[3] E. Dzuba and J. Cash, CloudFlare's 2023 Phishing Threats Report, August 2023. [Online]. Available: https://blog.cloudflare.com/2023-phishing-report

[4] Phishing.org, “How Phishing Works,” April 18, 2024. [Online]. Available: [https://www.phishing.org/how-phishing-works]

[5] Z. Alkhalil et al., “Phishing Attacks: A Recent Comprehensive Study and a New Anatomy,” Frontiers in Computer Science, vol. 3, 2021. [Online]. Available: https://doi.org/10.3389/fcomp.2021.563060

[6] S. Zaman, “Internet of Things (IoT) Data Protection and Security Concerns - Review,” 2023. [Online]. Available: https://www.researchgate.net/profile/Saad-Zaman-5/publication/373439194_Internet_of_Things_IoT_data_protection_and_security_concerns_-Review/links/64ec595e434d3f628c52394a/Internet-of-Things-IoT-data-protection-and-security-concerns-Review.pdf

[7] A. Luse and J. Burkman, “Gophish: Implementing a Real-World Phishing Exercise to Teach Social Engineering,” Journal of Cybersecurity Education, Research and Practice, vol. 2020, no. 2, 2021. [Online]. Available: https://doi.org/10.62915/2472-2707.1072

[8] P. S. Nyakomitta and S. O. Abeka, "Security Investigation on Remote Access," 2020. [Online]. Available: https://www.researchgate.net/profile/Peter-S-Nyakomitta/publication/350885415_Security_Investigation_on_Remote_Access_Methods_of_Virtual_Private_Network/links/609d7a67299bf1a25f0c2c80/Security-Investigation-on-Remote-Access-Methods-of-Virtual-Private-Network.pdf

[9] C. Smiliotopoulos, K. Barmpatsalou, and G. Kambourakis, 2022. [Online]. Revisiting the Detection of Lateral Movement through SysmonAvailable: https://www.mdpi.com/2076-3417/12/15/7746

[10] R. P. Ramirez et al., 2022. [Online]. Classifying RDP Remote Attacks on User Interfaces to Industrial Control Systems. 2022 International Conference on Computational Science and Computational Intelligence (CSCI) Available: https://american-cse.org/csci2022-ieee/pdfs/CSCI2022-2lPzsUSRQukMlxf8K2x89I/202800a871/202800a871.pdf

[11] A. C. Wood and T. Eze, "The Evolution of Ransomware Variants," 2020. [Online]. Available: https://www.researchgate.net/profile/Thaddeus-Eze/publication/342510766_The_Evolution_of_Ransomware_Variants/links/5f770a16299bf1b53e075e1c/The-Evolution-of-Ransomware-Variants.pdf

[12] C. Cohen, "What is Port 3389?" 2023. [Online]. Available: https://www.cbtnuggets.com/common-ports/what-is-port-3389

[13] J. Manson, 2022. [Online]. Available: https://www.tandfonline.com/doi/epdf/10.1080/23742917.2022.2049560?needAccess=true

[14] E. B. Blancaflor et al., 2021. [Online]. Let's Go Phishing: A Phishing Awareness Campaign Using Smishing, Email Phishing, and Social Media Phishing Tools. Proceedings of the 11th Annual International Conference on Industrial Engineering and Operations Management Singapore, March 7-11, 2021. Available: https://ieomsociety.org/singapore2021/papers/1105.pdf

[15] K. Okokpujie et al., "Cybersecurity Awareness: Investigating Students' Susceptibility to Phishing Attacks for Sustainable Safe Email Usage in Academic Environment: A Case Study of a Nigerian Leading University," 2023. [Online]. Available: https://www.researchgate.net/profile/KennedyOkokpujie/publication/368543209_Cybersecurity_Awareness_Investigating_Students%27_Susceptibility_to_Phishing_Attacks_for_Sustainable_Safe_Email_Usage_in_Academic_Environment_A_Case_Study_of_a_Nigerian_Leading_University/links/63eddb8231cb6a6d1d0741f6/Cybersecurity-Awareness-Investigating-Students-Susceptibility-to-Phishing-Attacks-for-Sustainable-Safe-Email-Usage-in-Academic-Environment-A-Case-Study-of-a-Nigerian-Leading-University.pdf