Acta Scientific COMPUTER SCIENCES

Volume 4 Issue 12 December 2022

Research Article

Hacking the Bank and Countermeasures

Trust T Mapoka*, Joyce Tlhoolebe and Keneilwe Zuva

Department of Computer Science, University of Botswana, Botswana

***Corresponding Author:** Trust T Mapoka, Department of Computer Science, University of Botswana, Botswana.

Received: April 05, 2022

Published: November 22, 2022

Abstract

Financial institutions are tremendous targets of opportunity for electronic thievery. Intermingled threats, improvements to man-in-the-middle or browser exploits, and advances in malware diversity has resulted in to easy hacks in to the banks by even less-skilled cybercriminals. The hacks usually target something that is of utmost value such as customer credentials and money in the Bank. Historically, banks have purchased various systems to manage threat risks, however their existing perimeter defense controls don't necessarily integrate well. Banks typically have had various fraud prevention controls with various tools for each type of exploit. Further, as these exploits continue to blossom, regulators have struggled to figure out best practice recommendations. Payment Card Initiatives and other banking regulations are a great start, but they haven't kept up with the online threat landscape. This paper addresses many ways of hacking the bank and recommend best practices to securing online banking transactions.

Keywords: Financial Crime; Secure Banking; Fraud; Cybersecurity

Introduction

The emergence of the Internet over decades has indorsed people to adopt an all connected attitude in expediting their daily tasks [1]. Above all, the usage of internet has attracted the banking sector at large by introducing internet or online banking. The emergence of internet banking has enabled financial institutions to offer their customers relatively convenient and flexible banking, also referred to e- banking. Basically, e-banking refers to bank customers utilizing the internet to perform financial services such as online transactions [2]. Online transactions include but not limited to fund transfers, account management and bill payments. Furthermore, e-banking enables ubiquitous online access to the bank accounts without travelling to the bank branch [3]. Internet banking has also benefited both banks and customers because banks have diminished their operational costs by decreasing physical facilities involving human resources, paperwork, and supporting staff. Many countries have integrated the use of the internet into their traditional banking system.

Despite the benefits that the banks are offering through e-banking with faster access to various financial activities [4,5], there are security concerns that accompany the e-banking systems [6]. Threat actors widely known as hackers have emerged diversity of intangible techniques for hacking the bank. Though numerous rewards of utilizing e-banking, security issues discourage customers from accepting online usage. This has brought fear to many customers having discovered that online banking usage expose their financial information assets (private credentials, money) at risk [7,8]. Meanwhile, most banks are widely accepting online usage through the internet, a cumulative number of hackers commit their time to conduct fraudulent activities by using online banking system. It has also emerged in recent research studies that banks can be hacked in so many ways that will be described fully in this paper [9,10]. This paper is arranged as follows; Section III describes various ways of hacking the bank, Section IV describes results and discussion, Section V is the conclusion and lastly section VI gives the current recommendations that banks can adopt to enhance security and the future strategic best practices for securing the bank.

Materials and Methods

Hacking the bank

There are various methods that can be exploited by the threat actor to hack the bank. The attackers first interest is to verify the existence of exploitable vulnerabilities in a system's security. Some information that may be of interest to the attackers are but not limited to.

Organization information

Employee details, partner details, web links, web technologies, patents, trademarks, etc. the attackers may perform passive foot printing using some advance google hacking techniques and Web Data extractor to extract the bank's data or use the Who-is lookup using domain tools. Figure 1 below show a web data extractor that can be used to extract the target organization's data such as meta tags, emails, phones etc.

Figure 1: Network Trace routing.

Network information

Domains, sub-domains, network blocks, network topologies, trusted routers, firewalls, IP addresses of the reachable systems, the Whois record, DNS records, and other related information. Some operations such as OS discovery, port, host and service discovery can be done by the attackers to get the network information. Figure 1 below shows an example of obtaining network information using trace routing.

System information

Operating systems, web server OSes, user accounts and passwords. The attackers can perform enumeration on a system or network to extract usernames, machine names, network resources, shares. They can perform NetBIOS enumeration using Windows Command- Line utilities and perform NetBIOS enumeration using NetBIOS Enumerator. Figure 2 below shows an example of obtaining the system information using the NetBIOS Enumeration using the command line.

Figure 2: NetBIOS Enumeration using Windows Command-Line.

Common methods for exploiting banks

Cyber security professionals should always stay ahead of the hackers in order to keep enterprises safe. This starts by understanding the network or systems vulnerabilities, and then putting in place the security measures needed to maintain a secure, resilient cybersecurity environment. Below are common methods that hackers usually use to exploit banks [11]:

- Downloading malicious software in to the enterprise network.
- Social engineering tips to get in to the infrastructure (servers, systems).
- Use of affected peripheral devices such as external USBs.
- Use of Weak cipher suites (SSL/TLS) from web applications.
- Malicious account takeover (Command and Control) which has now increased by greater than 150%.
- Use of weak perimeter controls to defend (Antivirus).
- Connect to any network is undesirably.
- Total access and control to untrusted private bank sites. Above ALL, the common weak point that the threat actors/ hackers take advantage of is the internal staff or people who have interacted or have prior knowledge about the banking system. Above ALL, the common weak point that the threat actors/hackers take advantage of is the internal staff or people who have interacted or have prior knowledge about the banking system.

Most common hacking types

The most common hacking types in financial institutions include:

- Online and Mobile fraud,
- Phishing scams (misleading emails, pop ups or messages) and malware.
- Distributed Denial of Service (DDoS),
- Money Mule scams (triggers the use your own account to perform illegal money transactions),
- Social networking risks and identity theft.

Similar hacking attempts recently

A series of recent bank heists or attempted heist follows malware enabled SWIFT transfers where bank officials received through phishing attempt a malware disguised as the PDF reader. This is what happens: Attackers conduct months' worth of reconnaissance (study the banks internal processes and controls) before attempting to submit fraudulent SWIFT messages and route bank funds to attacker controlled offshore accounts. In simple context, the hackers use the knowledge and access gained during reconnaissance to begin submitting fraudulent money orders to webs of offshore companies hence enabling them to siphon off millions of dollars. The hackers usually use banks publicly available information and tools to penetrate then commit the theft. The perpetrators gain access to the credentials of those authorized to create and approve messages. The perpetrators then have the capability to send fake messages via Bank computers/systems that interface with the SWIFT system, which enables financial institutions to exchange information on transaction details. Recently, dozens of Banks mostly in Russia and Ukraine surfaced with unprecedented massive hit of fraudulent enabled SWIFT transfers which led to Hundreds of millions of Dollars being stolen and some salvaged.

Banco De Chile loses $10Million in SWIFT related attack

The bank in May 24 2018 surfaced a malware attack then lost about $10 million due to fraudulent SWIFT wire transfers. The compromise occurred while the bank was dealing hundreds of workstations and servers that suddenly ceased working. The malware targeted the bank work stations, affecting cashiers and hampering branch services and phone banking. Some funds were successfully transferred to Hong Kong [12].

Hackers siphon $100 million from Bangladesh central bank's reserve account in New York

The incident follows a malware SWIFT related transfer heist at the BCB reserve Bank in New York. This took place in February 2016, when instructions to fraudulently withdraw US$ 1 billion from the account of Bangladesh Bank, the central bank of Bangladesh, at the Federal Reserve Bank of New York were issued via the SWIFT network. Five transactions issued by security hackers, worth $101 million and withdrawn from a Bangladesh Bank account at the Federal Reserve Bank of New York, succeeded, with $20 million traced to Sri Lanka (since recovered) and $81 million to the Philippines (about $18 million recovered). The Federal Reserve Bank of New York blocked the remaining thirty transactions, amounting to $850 million, at the request of Bangladesh Bank. It

was identified later that Dridex malware was used for the attack. Basically, the attackers were able to move laterally within the banks' networks with direction from the attackers' command-and-control servers, compromise administrators' credentials and use those credentials to execute their attacks [13].

Ukraine: US $ 10 million stolen from unnamed bank via swift

It was revealed that revealed that cyber criminals exploited the SWIFT international banking system to steal US$ 10 million from a Ukrainian bank. The theft was conducted in a way similar to the one the Bangladesh central bank experienced earlier this year – when cyber criminals stole about US$ 81 million from the bank [14].

Tien Phong Bank in Vietnam in May

In May 2016, such similar fake transfer requests were also used in an attempt to steal more than US$ 1.1 million from the Tien Phong Bank in Vietnam [15].

India's Cosmos bank raided for $13m by hackers

Cosmos Bank in India says that hackers made off with $13.4m in stolen funds through Money mule and SWIFT related attacks. Multiple reports out of the country say that a group of attackers used cloned cards to withdraw cash from ATMs at a set time and perform a fraudulent SWIFT money transfer. Together, the efforts resulted in about $13.4m being stolen from the bank and its account holders. The attack was believed to have taken place in two phases. The first attacker was an international effort with money mules in 28 different countries, all extracting cash from their local ATMs. According to the Hindustan Times, 15,000 transactions were carried out over the seven- hour period. The second phase when a SWIFT transaction saw Cosmos move $1.93m to an account at a bank in Hong Kong [16].

SolarWinds attack

This follows an operation that was identified in December 2019 and was deemed the largest and the most sophisticated attack ever by Microsoft President Brad Smith. The attack was believed to have likely been orchestrated by Russia, and they breached the software made by SolarWinds Corp, giving hackers access to thousands of companies that used its products [17]. The scope and sophistication of the attack is unmatched, infiltrating an abundance of corporate and administrative bodies, while remaining undetected for so many months. Threat actors performed reconnaissance and gained access to the SolarWinds Orion Platform and gained information on SolarWinds and their clients and eventually stealing authorized credentials [18], Solarwinds attack is a supply chain attack. A supply chain attack is a kind of cyber-attack such that the organizations are not attacked directly, but the intermediate parties such as vendors and their software code are attacked instead [19]. Supply chain attackers target software developers and suppliers, seeking access to source code, software build mechanisms or software update processes.

True facts about swift

SWIFT is a Brussel based cooperative that interconnect about 11 000 banks worldwide, thus making it attractive and widespread target to the threat actor. However, attackers haven't yet exploited any specific vulnerabilities within the SWIFT system but rather sort to exploit the weak controls at the Enterprise networks for the Banks [20,21]. The threat actor then compromises key accounts for bank officials in order to create fraudulent transfers. Since the breath taking attacks, Banks around the world have seen attempts to undermine the SWIFT infrastructures but to its credit, SWIFT has tripled its security team by launching a 24/7 Security Operation Centre (SOC) that performs real time monitoring of emanating cyber threats and vulnerabilities. In addition, the SWIFT raise continuous awareness to users and improve security by sharing attack related information. Therefore, it is the responsibility of the Banks to up their game with proactive defensive controls to triple the impact of the existing security [22-24].

Password cracking techniques

Hacking often begins with password-cracking attempts [25,26]. A password is a key piece of information necessary to access a system. Consequently, most attackers use password-cracking techniques to gain unauthorized access. An attacker may either crack a password manually by guessing it or use automated tools and techniques such as a dictionary or a brute-force method. Most password-cracking techniques are successful because of weak or easy to guess passwords [27]. We will focus on the following two techniques;

Perform active online attack to crack the system's password using Responder

An Active online attack is one of the easiest ways to gain unauthorized administrator-level system access [28]. Here, the

attacker communicates with the target machine to gain password access. Techniques used to perform active online attacks include password guessing, dictionary and brute- forcing attacks, hash injection, LLMNR/NBT-NS poisoning, use of Trojans/spyware/ key loggers, internal monologue attacks, Markov-chain attacks, Kerberos password cracking, etc. [29]. Here we demonstrate how easily hackers can gather password computer networks. Responder works by First listening to multicast NR queries, NBT-NS – UDP/137) and, under the right circumstances it will spoof a response and direct the victim to the machine on which it is running. Once a victim will try and connect to our machine, Responder will exploit the connection to steal credentials and other data. For demonstration purposes, we will only provide responder with the interface we wish to run it on.

Audit system passwords using L0phtCrack

Password auditing is one of the crucial stages in checking the security of a system. Password- auditing mechanisms often exploit otherwise legal means to gain unauthorized system access, such as recovering a user's forgotten password feature. The classification of password attacks depends on the attacker's actions L0phtCrack is a tool designed to audit passwords and recover applications. It recovers lost Microsoft Windows passwords with the help of a dictionary, hybrid, rainbow table, and brute-force attacks. It can also be used to check the strength of a password.

Results and Discussion

Perform active online attack to crack the system's password using responder

Responder is an LLMNR, NBT-NS, and MDNS poisoner. It responds to specific NBT-NS (NetBIOS Name Service) queries based on their name suffix. By default, the tool only responds to a File Server Service request, which is for SMB. LLMNR (Link Local Multicast Name Resolution) and NBT-NS (NetBIOS Name Service) are two main elements of Windows OSes that are used to perform name resolution for hosts present on the same link. These services are enabled by default in Windows OSes and can be used to extract the password hashes from a user. Since the awareness of this attack is low, there is a good chance of acquiring user credentials in an internal network penetration test. By listening for LLMNR/NBT-NS broadcast requests, an attacker can spoof the server and send a response claiming to be the legitimate server. After the victim system accepts the connection, it is possible to gain the victim's user-credentials by using a tool such as Responder.py. from the observation of this task, it is easy credentials both in plain text and password hashes. To mitigate this attack, it is advisable to disable LLMNR and NBT-NS so that the chances of this attack happening to your local network domain are zero to minimal [30]. Figure 3 below shows how the responder tool was used to extract information such as the target system 's OS version client version, NTLM client IP address, and NTLM username and password hash.

Figure 3: Responder starts listening to the network interface for events.

By default, Responder stores the logs in Home/Responder/logs. John the Ripper starts cracking the password hashes and displays the password in plain text, sudo john/home/ubuntu/Responder/logs/[Log File Name.txt].

Audit system passwords using L0phtCrack

You can use the L0phtCrack tool for auditing the system passwords of machines in the target network and later enhance network security by implementing a strong password policy for any systems with weak passwords. L0phtCrack starts cracking the passwords of the remote machine. After the status bar completes, L0phtCrack displays the cracked passwords of the users that are available on the remote machine It will take some time to crack all the passwords of a remote system. There are different password audit types that can be performed on the remote system, the quick password audit, common password audit, strong password audit and through the password audit. Figure 4 below shows different password audit types.

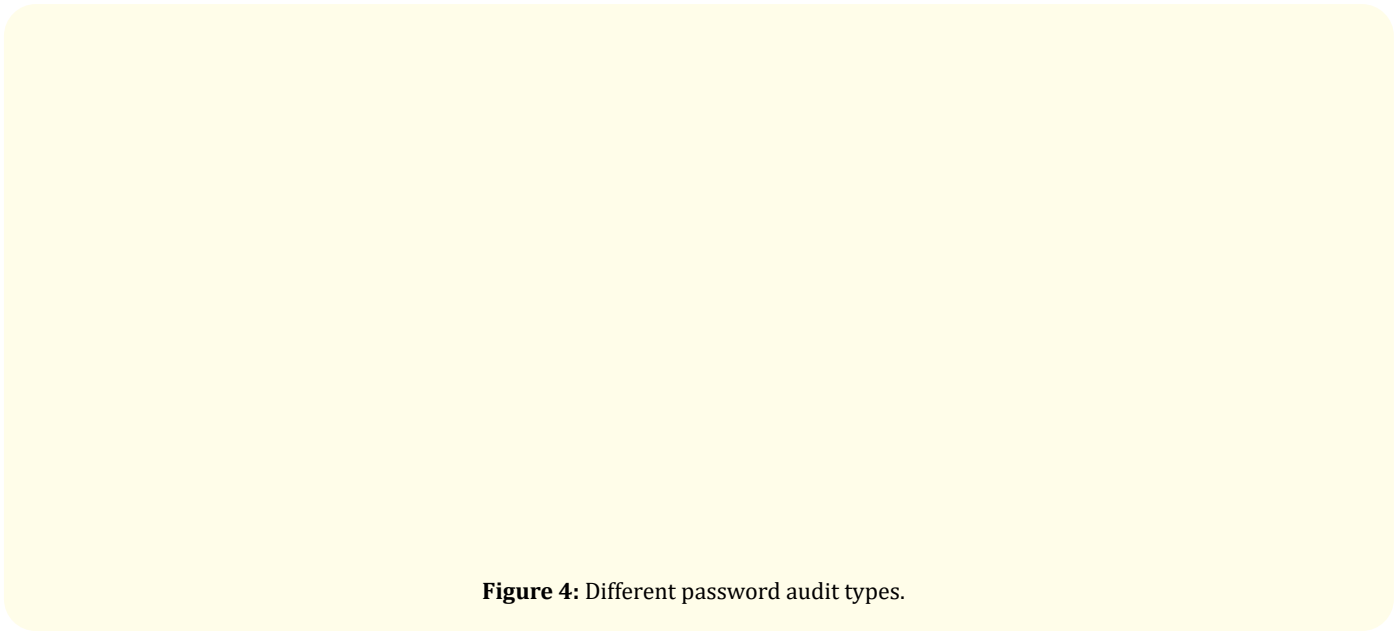

Figure 4: Different password audit types.

When reporting, most of the time you'll want to know what the audited passwords are, but in some situations you may wish to verify the safety of the password without disclosing what it is. Figure 5 below shows different reporting options for audited passwords.

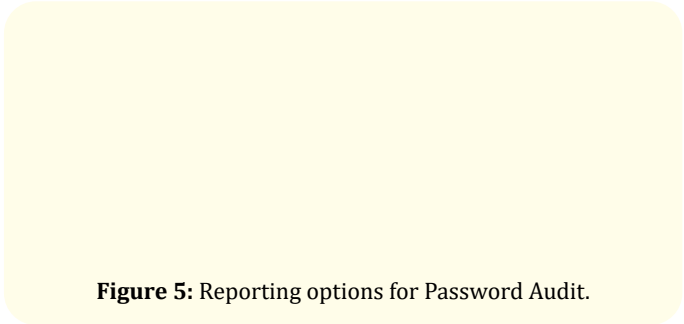

Figure 5: Reporting options for Password Audit.

User account passwords that are cracked in a short amount of time are weak, meaning that you need to take certain measures to strengthen them. You can use the L0phtCrack tool for auditing the system passwords of machines in the target network and later enhance network security by implementing a strong password policy for any systems with weak passwords. Figure 6 below shows cracked user accounts. From the six accounts from the target machine, five out of six accounts passwords were cracked within a short period of time.

Figure 5: Reporting options for Password Audit.

Conclusion

To help protect your Bank from security breaches, you should adopt best practice internal controls [31] and guidelines like the following.

Enhance Identity verification during logon

Bank MUST at all times adopt multi factor authentication such that during system logon attempt, the system interacts with the actual entity attempting to login. E.g. utilize combination of factors such as Credentials plus OTP sent through text to the mobile phone. Geolocation, pattern based or face recognition factors can be incorporated if desired.

Creating and protecting credentials password

Adopt best practice when creating passwords such as use of combination of alphanumeric characters (./?!#@%*&), One upper case letter, 2 numbers. Bank users SHOULD never share login credentials with anyone and SHOULD never write it down. Use a secure password manager if you need help keeping track of many passwords.

Implement dual custody during transactions

Adopt dual authorization and/or transaction-based authentication procedures during financial transfers. Identify verification should adopt real time interaction with the actual entity performing the transaction (Multi factor authentication must apply during transfers).

Routine risk and vulnerability assessment

Since no risk and vulnerability assessment has been carried out before, it is important for the Bank to know its security posture from the risk perspective. Threat actors take advantage of exploitable vulnerabilities that exist within enterprise (corporate) network points (endpoints, systems, servers) to penetrate deep in to something that is value (i.e. systems that does money transfers, user credentials for online, user privilege escalation procedures). Therefore, recommend the bank to perform routine vulnerability assessment for entire system in combination with Penetration test in the perspective of the hacker. The results will determine the vulnerabilities that can exploited and tested against the existing perimeter controls then report on remediation control measures (necessary patching) that should be in place to maintain protection.

From the risk assessment perspective, routine risk assessment screening must be performed in this context so that any employee contractor, or third party user termination or change of employment or responsibilities cannot result in to deliberate breach. Usually the ex-employees/contractors/third party users understand the banking system and have the credentials at termination. Therefore, termination procedures between the Human resource and IT resource must be in place to ensure immediate disabled access of the terminated within the AD or any other related security access to the enterprise and disable access to the facility to avoid future disgruntled breaches. Risk assessment must be performed Prior to employment, during employment and after employment (termination) to maintain up to date records.

Future strategic security initiatives

Due to persistent cyber heists affecting Banks recently, we suggest the following:

- Proactive approach to Cyber security [32-34]: Establish Unified Security Operations and Analytics platform known as the Cyber Security Operation Centre (CSOC/CERT/CSIRT/CIRT) similar to the SWIFT SOC. The CSOC [35-37] shall integrate with the existing perimeter controls acting as perimeter wall that provides overall visibility and proactive real time monitoring over evolving (insider and outsider) threats and vulnerability exploits targeting the Bank enterprise network systems. Early detection and prevention is better than cure. The centralized platform consists of incident response management team that promote information sharing on current surfaced threats targeting the Bank. If you cannot afford the establishment then outsource through reputable Managed Security Service Provider (MSSP) so that you are monitored 24-7-365 days.
- Enhance strong information sharing capability of emanating security incidents with SWIFT.
- Eliminate single sign on factor and expand to multifactor support to authenticate SWIFT messages
- Enhance security and audit risk baselines for participating banks,
- Increase integrity support for anomaly detection and stop-payment controls,
- Engage third-party consultants to assist with security assessments and implementation
- Adopt analytics technology that performs Darkweb monitoring [38] for threats that occur in the dark space such as Blockchain (Bitcoins).
- Carry out risk assessment by updating the employee credentials database such that terminated officials have disabled access to the VPN, ADs and disabled physical access to sensitive facility areas.
- Carry out vulnerability assessment to proactively identify, prioritize, and remediate vulnerabilities before being breached.

Bibliography

1. Mohammed A Al-Sharafi., *et al*. "The Effect Of Security And Privacy Perceptions On Customers' Trust To Accept Internet Banking Services: An Extension Of TAM". *Journal of Engineering and Applied Sciences* 11.3 (2016): 545-552.
2. Vidhya Jolly. "The Influence of Internet Banking on the Efficiency and Cost Savings for Banks' Customers". *International Journal of Social Sciences and Management* 3.3 (2016): 163.
3. R Safeena., *et al*. "Customer Perspectives on E-business Value: Case Study on Internet Banking". *Journal of Internet Banking and Commerce* 15 (2010): 1-13.
4. S Sharma. "A detail comparative study on e- banking VS traditional banking". *International Journal of Applied Research* 2.7 (2016): 302-307.
5. R K Konoth., *et al*. "How Anywhere Computing Just Killed Your Phone-Based Two-Factor Authentication". in Financial Cryptography and Data Security, Berlin, Heidelberg, (2017): 405-421.
6. G Vaciago and D S Ramalho. "Online searches and online surveillance: the use of trojans and other types of malware as means of obtaining evidence in criminal proceedings". (2016).
7. D Wong., *et al*. "To trust or not to trust: the consumer's dilemma with e- banking". *Journal of Internet Bus* 6 (2009): 1-27.
8. E R Leukfeldt., *et al*. "Cybercriminal Networks, Social Ties and Online Forums: Social Ties Versus Digital Ties Within Phishing and Malware Networks". *The British Journal of Criminology* 57.3 (2017): 704-722.
9. CL Chiu., *et al*. "Privacy, security, infrastructure and cost issues in internet banking in the Philippines: initial trust formation". *International Journal of Financial Services Management* 8.3 (2016): 240-271.
10. N A G Arachchilage., *et al*. "Phishing threat avoidance behaviour: An empirical investigation". *Computers in Human Behavior* 60 (2016): 185-197.
11. "Banks Under Attack: Tactics and Techniques Used to Target Financial Organizations - Security News". (2022).
12. "Banco de Chile Loses $10 Million in SWIFT-Related Attack" (2022).
13. "Bangladesh bank says hackers stole $100M from its New York Fed account" (2022).
14. "Ukraine: US$ 10 Million Stolen From Unnamed Bank via Swift" (2022).
15. "Vietnam's Tien Phong Bank Targeted in Bangladesh-Like Cyberattack WSJ" (2022).

16. "India's Cosmos bank raided for $13m by hackers • The Register" (2022).

17. "SolarWinds hack was 'largest and most sophisticated attack' ever: Microsoft president". *Reuters,* (2021).

18. L Sterle and S Bhunia. "On SolarWinds Orion Platform Security Breach". in 2021 IEEE SmartWorld, Ubiquitous Intelligence Computing, Advanced Trusted Computing, Scalable Computing Communications, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/IOP/SCI), (2021): 636-641.

19. X Wang. "On the Feasibility of Detecting Software Supply Chain Attacks". in MILCOM 2021 - 2021 IEEE Military Communications Conference (MILCOM), Nov. (2021): 458-463.

20. J Ko¨ ppel. "Annex 1: The History and Detailed Functioning of SWIFT". in The SWIFT Affair : Swiss Banking Secrecy and the Fight against Terrorist Financing, Gene`ve: Graduate Institute Publications, (2011).

21. "Homepage". SWIFT - The global provider of secure financial messaging services (2022).

22. R Andrade., *et al*. "Management of information security indicators under a cognitive security model". in 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC), Jan. (2018): 478-483.

23. Shakeel Durrani., *et al*. "Design and development of wireless RTU and cybersecurity framework for SCADA system". (2013).

24. JM Ahrend., *et al*. "On the collaborative practices of cyber threat intelligence analysts to develop and utilize tacit Threat and Defence Knowledge". in 2016 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (CyberSA), Jun. (2016): 1-10.

25. "Password Cracking – an overview | ScienceDirect Topics" (2022).

26. "The top 12 password-cracking techniques used by hackers". IT PRO (2022).

27. "Password Cracking Techniques - EC-Council iClass" (2022).

28. "What is Active Online Attacks and how to Defend". Zerosuniverse (2022).

29. S. of Jersey. "Government of Jersey". gov.je. (2022).

30. W Hurer-Mackay. "LLMNR and NBT-NS Poisoning Using Responder". 4ARMED Cloud Security Professional Services, Jun. 06, (2016).

31. S Mahajan., *et al*. "BRB dashboard: A web-based statistical dashboard". in 2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), Mar. (2017): 1-6.

32. "National/governmental CERTs - ENISA's recommendations on baseline capabilities — ENISA" (2022).

33. "What is NIST Compliance? | Digital Guardian" (2022).

34. "Creating and Managing an Incident Response Team for a Large Company". SANS Institute (2022).

35. "Hidden Markov based anomaly detection for water supply systems". IEEE Conference Publication | IEEE Xplore (2022).

36. PQ Nguyen and J Zhou. Information Security: 20th International Conference, ISC 2017, Ho Chi Minh City, Vietnam, November 22-24, 2017, Proceedings. Springer, (2017).

37. B Song., *et al*. "Visualization of security event logs across multiple networks and its application to a CSOC". *Cluster Computing* 22.1 (2019): 1861-1872.

38. E Nunes., *et al*. "At-risk system identification via analysis of discussions on the darkweb". in 2018 APWG Symposium on Electronic Crime Research (eCrime), May (2018): 1-12.