

Giriş

BGM 553 - Sızma Testleri ve Güvenlik Denetlemeleri-I Bilgi Güvenliği Mühendisliği Yüksek Lisans Programı

Dr. Ferhat Özgür Çatak
ozgur.catak@tubitak.gov.tr

İstanbul Şehir Üniversitesi
2017 - Güz

İçindekiler

1

Giriş

- Ders Hakkında
- Internet
- Bashlite
- Terminoloji

2

Tehditler ve Saldırı Vektörleri

- Saldırılar
- Saldırı Vektörleri
- Bilgi Savaşı

3

Ethical Hacking

- Ethical Hacking
- Tanımlar

4

Temel Kavramlar

- Penetrasyon Testi (Pentest)
- Standartlar
- Zafiyet Taraması
- Sızma Testi Yaklaşımıları

Saldırı Türleri

5

PenTest Planlaması

- Planlama
- Amaç
- Kapsam
- Gereksinimler
- Sınırlamalar

6

Metodoloji

- Giriş
- Keşif
- Tarama
- Erişim Kazanma
- Sistemde Kalıcı Olma

7

Diğer Konular

- Kullanılan Araçlar
- Kali Linux
- Raporlama

İçindekiler

1

Giriş

- Ders Hakkında
- Internet
- Bashlite
- Terminoloji

2

Tehditler ve Saldırı Vektörleri

- Saldırılar
- Saldırı Vektörleri
- Bilgi Savaşı

3

Ethical Hacking

- Ethical Hacking
- Tanımlar

4

Temel Kavramlar

- Penetrasyon Testi (Pentest)
- Standartlar
- Zafiyet Taraması
- Sızma Testi Yaklaşımları

- Saldırı Türleri

5

PenTest Planlaması

- Planlama
- Amaç
- Kapsam
- Gereksinimler
- Sınırlamalar

6

Metodoloji

- Giriş
- Keşif
- Tarama
- Erişim Kazanma
- Sistemde Kalıcı Olma

7

Diğer Konular

- Kullanılan Araçlar
- Kali Linux
- Raporlama

Ders Hakkında

► Dr. Ferhat Özgür Çatak

- ▶ TÜBİTAK - BİLGEML Siber Güvenlik Enstitüsü
- ▶ ozgur.catak@tubitak.gov.tr

► Ders web sitesi: <http://bgm553.bilgiguvenligi.gov.tr>

- ▶ Bütün duyurular buradan yapılmaktadır. Takip edin

► Notlandırma

- ▶ Derse Katılım: %10
- ▶ Dönem Projesi : %20
- ▶ Ödev 1-2-3: %20
- ▶ Vize : %20
- ▶ Final : %30

► Dönem 14 Hafta

- ▶ 1 Hafta vize
- ▶ Dönem Sonu sınavları : 1-11 Şubat

► Sınavlar çoktan seçmeli sorular şeklinde

► Bilgisayar Lab ???

► Virtualbox, Kali Linux

Kurumsal ve Kişisel Uygulamalar



Equifax Veri Kaçağı

Equifax

- ▶ 2017 yılının en önemli veri sızıntısı
- ▶ 143 milyon kişinin bilgisi çalındı
 - ▶ ABD nüfusunun %44
- ▶ Finans ve kredi raporları
- ▶ 209.000 kişinin kredi kartı bilgisi
- ▶ Web sitesinin zafiyeti
- ▶ Mayıs 2017 başlangıç



21st Century Oncology Veri Kaçağı

21st Century Oncology

- ▶ 17 eyalet faaliyet, 145 sağlık merkezi
- ▶ 2016 yılında 2.2 milyon hassas veriye erişim

^a<http://cbs12.com/news/local/21st-century-oncology-notifies-22-million-of-hacking-data-breach>

^b<https://www.natlawreview.com/article/oh-no-not-again-chalk-yet-another-health-data-breach>

eBay Veri Kaçağı

eBay

- ▶ 145 milyon kullanıcı kaydı ele geçirildi.
- ▶ Ele geçirilen kayıtlar
 - ▶ Password
 - ▶ Email
 - ▶ Doğum tarihi
 - ▶ Posta adresleri

Mirai I



Mirai¹

- ▶ Internet's largest ever DDoS attacks of 1 TBPS in which 145,000 hacked webcams were used.

Mirai II

Username/Password	Manufacturer	Link to supporting evidence
admin/123456	ACTi IP Camera	https://ipvm.com/reports/ip-cameras-default-passwords-directory
root/anke	ANKO Products DVR	http://www.cctvforum.com/viewtopic.php?f=3&t=44250
root/pass	Axis IP Camera, et. al	http://www.cleanacs.com/router-default/Axis/543-901
root/vizxv	Dahua Camera	http://www.cam-it.org/index.php?topic=5192.0
root/888888	Dahua DVR	http://www.cam-it.org/index.php?topic=5035.0
root/666666	Dahua DVR	http://www.cam-it.org/index.php?topic=5035.0
root/7ujfko0vzxv	Dahua IP Camera	http://www.cam-it.org/index.php?topic=5396.0
root/7ujfko0admin	Dahua IP Camera	http://www.cam-it.org/index.php?topic=5396.0
666666/666666	Dahua IP Camera	http://www.cleanacs.com/router-default/Dahua/DH-IPC-HDW4300C
root/dreambox	Dreambox TV receiver	https://www.satellites.co.uk/forums/thread/reset-root-password-plugin_101146/
root/zlx	EV ZLX Two-way Speaker?	?
root/juantech	Guangzhou Juan Optical	https://news.ycombinator.com/item?id=11114012
root/hx3511	H.264 - Chinese DVR	http://www.cctvforum.com/viewtopic.php?f=56&t=34930&start=15
root/hx3518	HiSilicon IP Camera	https://acasis.wordpress.com/2014/08/10/i-got-a-new-hx3518-ip-camera-modules/
root/fkv123	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd5a4f733f04735619bc7812fd
root/fkv1234	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd5a4f733f04735619bc7812fd
root/jvtzd	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd5a4f733f04735619bc7812fd
root/admin	IPX-ODK Network Camera	http://www.ipxinc.com/products/cameras-and-video-servers/network-cameras/
root/system	iQinVision Cameras, et. al	https://ipvm.com/reports/ip-cameras-default-passwords-directory
admin/meinsm	Mobotix Network Camera	http://www.forum.use-ip.co.uk/threads/mobotix-default-password.78/
root/54321	Packet8 VOIP Phone, et. al	http://webcache.googleusercontent.com/search?q=cache:WtjghzQZURUJ.community.freepbx.org%2fpacket8-atas-phones%2f11
root/000000000	Panasonic Printer	https://www.experts-exchange.com/questions/26194395/Default-User-Password-for-Panasonic-CP-C405-Web-Interface.html
root/realtek	RealTek Routers	
admin/1111111	Samsung IP Camera	https://ipvm.com/reports/ip-cameras-default-passwords-directory
root/xmhdpic	Shenzhen Anran Security Camera	https://www.amazon.com/MegaPixel-Wireless-Network-Surveillance-Camera/product-reviews/B00E86EN0I
admin/smccadmin	SMC Routers	http://www.cleanacs.com/router-default/SMC/ROUTER
root/kwb	Toshiba Network Camera	http://faq.surveillexdrsupport.com/index.php?action=article&cat=4&id=8&artlang=en
ubnt/ubnt	Ubiquiti AirOS Router	http://etherrouter.com/router/ubnt/ubnt/airos-airgrid-m5#login.htm
supervisor/supervisor	VideoIQ	https://ipvm.com/reports/ip-cameras-default-passwords-directory
root/<none>	Vivotek IP Camera	https://ipvm.com/reports/ip-cameras-default-passwords-directory
admin/1111	Xerox printers, et. al	https://ityourservice.blogspot.com/2012/08/logging-in-as-system-administrator-on-your-xerox-printer/
root/Zte521	ZTE Router	http://www.ironbugs.com/2016/02/hack-and-patch-your-zte-f660-routers.html

Şekil: Default passwords²

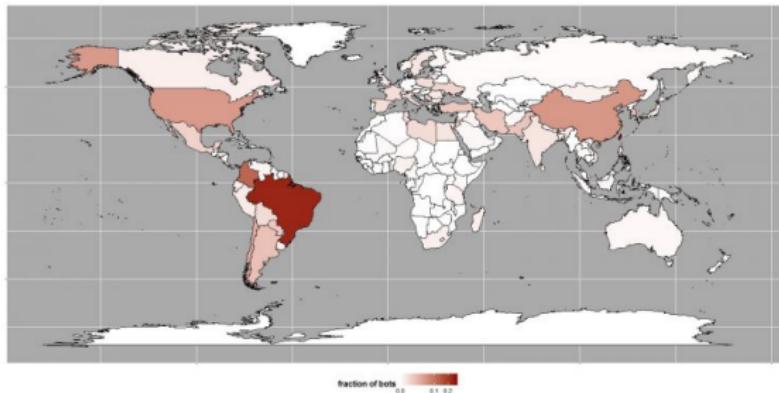
¹<https://www.hackread.com/mirai-botnet-linked-to-dyn-dns-ddos-attacks/>

²<https://intervisablog.wordpress.com/2016/10/26/here-are-the-devices-usernames-and->

Bashlite

Bashlite

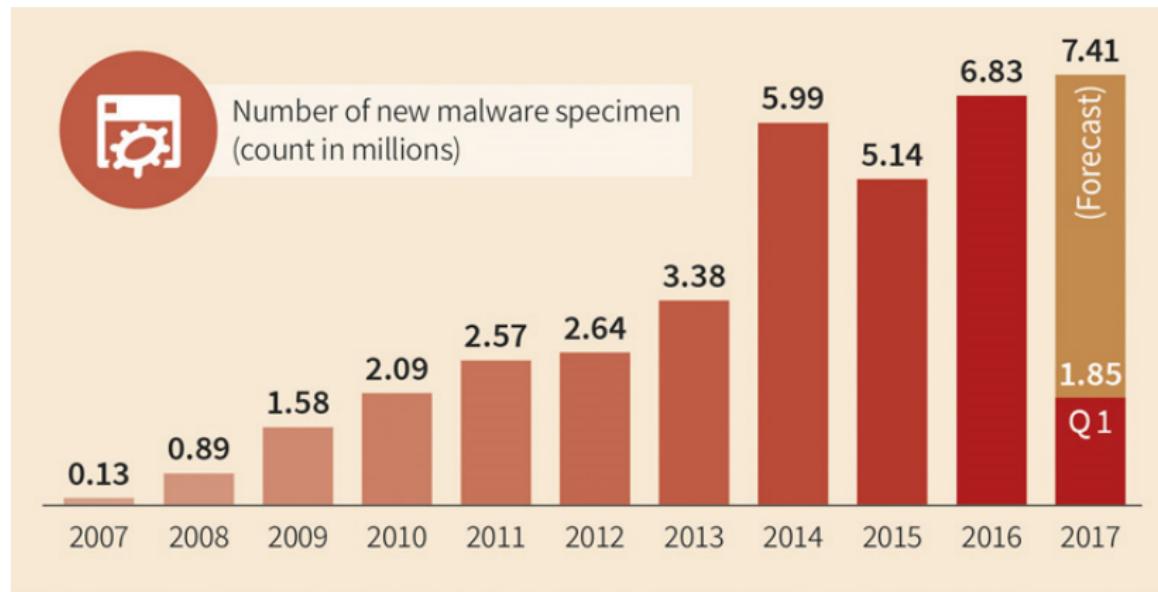
- ▶ **BASHLITE** (also known as **Gafgyt**, **Lizkebab**, **Qbot**, **Torlus** and **LizardStresser**) is malware which infects Linux systems in order to launch distributed denial-of-service attacks (DDoS).
- ▶ It has been used to launch attacks of up to 400 Gbps.



Şekil: Bashlite ³

³<https://www.hackread.com/bashlite-malware-linux-iot-ddos-botnet/>

Malware Trends - 2017



Şekil: Malware trends

- ▶ 2016 yılında her 4.6 saniyede yeni bir malware örneği raporlandı
- ▶ 2017 yılında 4.2 saniye

¹<https://www.gdatasoftware.com/blog/2017/04/29666-malware-trends-2017>

Terminoloji

Gerekli Terminoloji

► Hack Value:

- ▶ Bilgisayar korsanları arasında, yapmaya değer olacak amaç.

► 0. gün saldırısı (Zero-Day Attack)

- ▶ Yazılım geliştiricilerin yama yayınlanmadan önce, uygulama zayıflıklarını sızdırmasıyla (exploit) yapılan saldırı

► Zayıflık (Vulnerability)

- ▶ Bir sistemin ele geçirilmesine sebep olan zayıflık, tasarım veya gerçekleştirmen hatası

► Sızdırma (Exploit)

- ▶ Zayıf noktalar yoluyla BT sistem güvenliğinin ihlal edilmesi.

► Payload

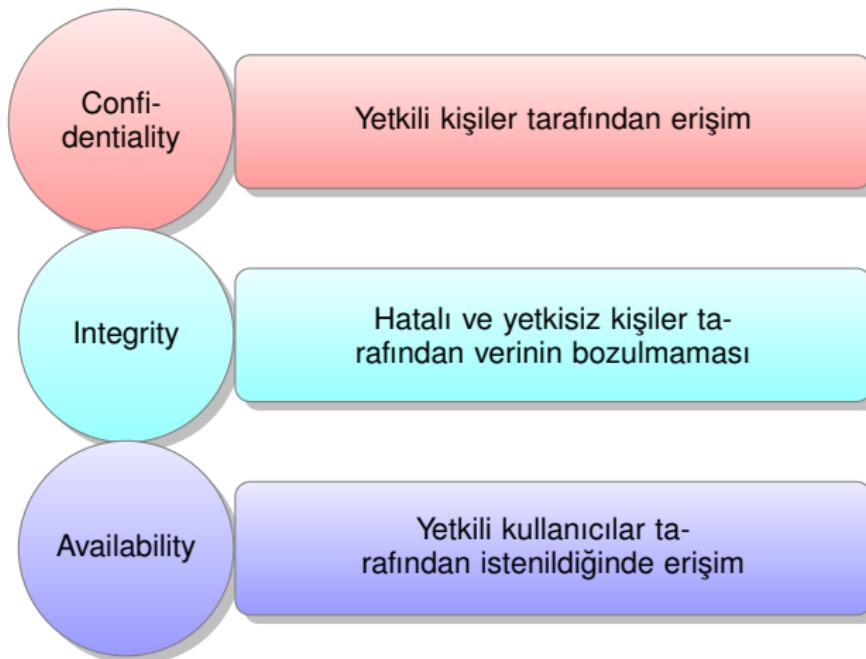
- ▶ İstenmeyen kötü amaçlı eylemi gerçekleştiren, yıkma, arka kapı oluşturma ve bilgisayar ele geçirme gibi bir istismar kodunun parçasıdır.

► Bot

- ▶ Bir "bot", önceden tanımlanmış görevleri yürütmek veya otomatikleştirmek için uzaktan kontrol edilebilen bir yazılım uygulamasıdır.

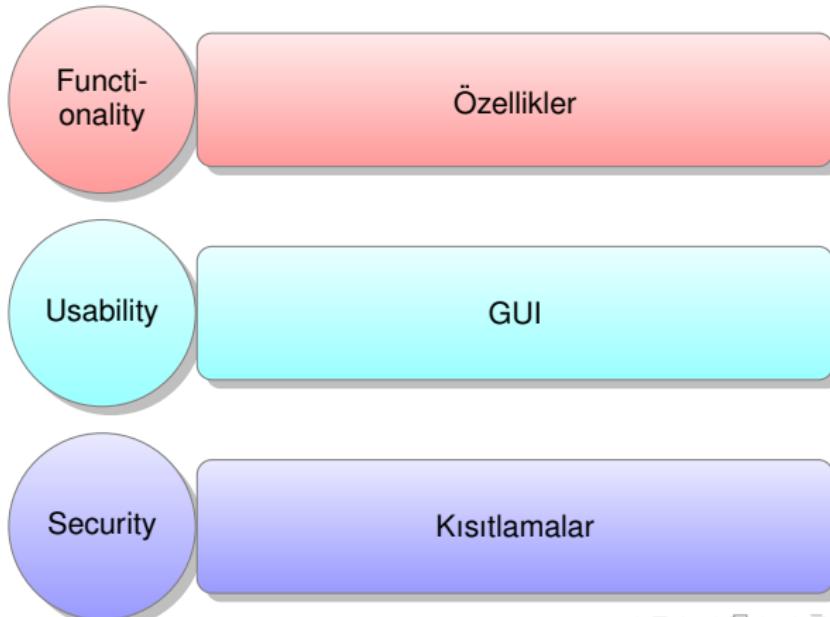
Bilgi Güvenliği Bileşenleri

Bilgi güvenliği, bilgi ve altyapı konusundaki **hırsızlık, dolandırıcılık** ve **bozulma** olasılığının düşük veya tolere edilebilir olduğu bir durumdur.



Security, Functionality, Usability

- ▶ Bir sistemdeki güvenlik seviyesi üç bileşenin gücüyle tanımlanabilir:
- ▶ Herhangibirine yanlışıldığı zaman diğerlerinden uzaklaşmış olur.
- ▶ **Usable Security**



İçindekiler

1 Giriş

- Ders Hakkında
- Internet
- Bashlite
- Terminoloji

2 Tehditler ve Saldırı Vektörleri

- Saldırılar
- Saldırı Vektörleri
- Bilgi Savaşı

3 Ethical Hacking

- Ethical Hacking
- Tanımlar

4 Temel Kavramlar

- Penetrasyon Testi (Pentest)
- Standartlar
- Zafiyet Taraması
- Sızma Testi Yaklaşımları

● Saldırı Türleri

5 PenTest Planlaması

- Planlama
- Amaç
- Kapsam
- Gereksinimler
- Sınırlamalar

6 Metodoloji

- Giriş
- Keşif
- Tarama
- Erişim Kazanma
- Sistemde Kalıcı Olma

7 Diğer Konular

- Kullanılan Araçlar
- Kali Linux
- Raporlama

Saldırıların Motivasyonu, Hedefleri, Amaçları

Saldırı = Motivasyon (Amaç) + Yöntem + Zafiyet

- ▶ **Motivasyon:** hedef sistemin değerli bir şeyi depoladığı veya işlediği, bunun sonucu olarak sisteme saldırı için bir tehdit bulunduğu fikrinden kaynaklanmaktadır.
- ▶ **Yöntem:** Saldırganlar, bilgisayar sistemindeki güvenlik açıklarından veya güvenlik politikasından yararlanmaya yönelik çeşitli araçlar ve saldırı teknikleri denerler ve motivasyonlarını sağlamak için denetimler yaparlar.

Güvenlik Saldırılarının Motivasyonları

- ▶ İş sürekliliğin engellenmesi
- ▶ Bilgi hırsızlığı
- ▶ Veri manipülasyonu
- ▶ Kritik altyapıları bozarak korku ve kaos oluşturmak
- ▶ Dini ve politik inançların yayılması
- ▶ Hedefin saygınlığının yok edilmesi

Saldırı Vektörleri

Ağ Tehditleri

- ▶ Bilgi toplama
- ▶ Sniffing
- ▶ Spoofing
- ▶ Man-in-the-Middle
- ▶ DNS ve ARP zehirlenmesi
- ▶ Parola saldırıları
- ▶ DOS

İstemci Tehditleri

- ▶ Malware
- ▶ Footprinting
- ▶ Parola saldırıları
- ▶ DOS
- ▶ Yetkisiz erişim
- ▶ Hak yükseltme
- ▶ Backdoor

Uygulama Tehditleri

- ▶ Veri doğrulama
- ▶ Hatalı güvenlik ayarları
- ▶ Bilgi ifşası
- ▶ Buffer overflow
- ▶ SQL injection
- ▶ Hatalı exception handling

Sistem Saldırı Türleri

► **İşletim Sistemi Saldırıları:**

- ▶ Bir sisteme erişim için işletim sisteminin tasarımında, kurulumunda veya konfigurasyonunda yer alan zayıflıkların araştırılması
- ▶ Buffer overflow, OS bugs, unpatched operating system

► **Hatalı Konfigurasyon Saldırıları:**

- ▶ Veritabanı, ağ, uygulama sunucuları, web sunucularının hatalı konfigurasyon zayıflıkları, sisteme illegal erişim sağlayabilir.

► **Uygulama Saldırıları:**

- ▶ Yetkisiz erişim veya veri çalma amacıyla kuruluş içinde kullanılan uygulamaların sahip olduğu zayıflıkların sömürülmesi
- ▶ Buffer overflow, cross-site scripting, SQL injection, man-in-the-middle, denial-of-service

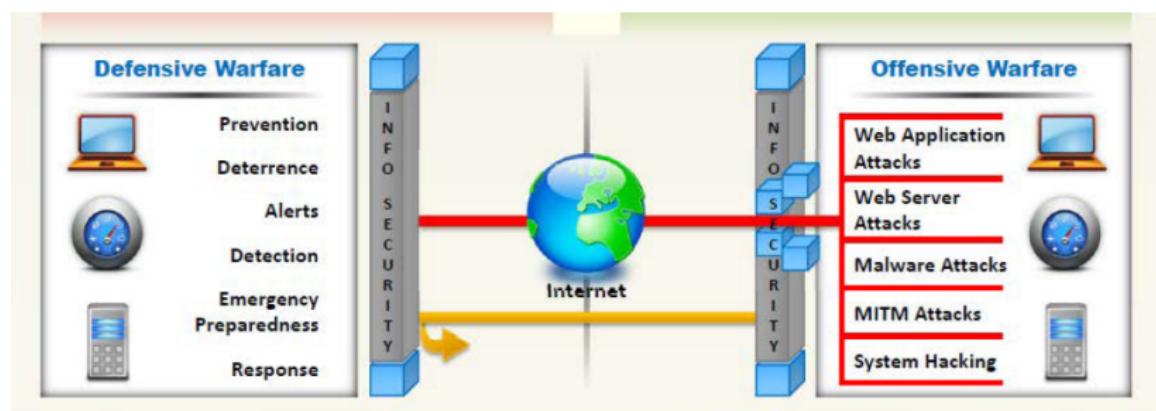
► **Shrink-Wrap Code Attacks:**

- ▶ Varsayılan yapılandırma ve ayarlar
 - ▶ MsSQL - Brute Force Password Attacks
 - ▶ Mirai - DDoS Attack

Bilgi Savaşı

Bilgi Savaşı

Rakibe karşı üstün avantajlar sağlamak için bilgi ve iletişim teknolojilerinin (ICT) kullanılmasını ifade etmektedir.



İçindekiler

1 Giriş

- Ders Hakkında
- Internet
- Bashlite
- Terminoloji

2 Tehditler ve Saldırı Vektörleri

- Saldırılar
- Saldırı Vektörleri
- Bilgi Savaşı

3 Ethical Hacking

- Ethical Hacking
- Tanımlar

4 Temel Kavramlar

- Penetrasyon Testi (Pentest)
- Standartlar
- Zafiyet Taraması
- Sızma Testi Yaklaşımları

● Saldırı Türleri

5 PenTest Planlaması

- Planlama
- Amaç
- Kapsam
- Gereksinimler
- Sınırlamalar

6 Metodoloji

- Giriş
- Keşif
- Tarama
- Erişim Kazanma
- Sistemde Kalıcı Olma

7 Diğer Konular

- Kullanılan Araçlar
- Kali Linux
- Raporlama

Hacking

- ▶ **Hacking:** Sık duyulan ifade
 - ▶ Web sitelerine istenmeyen girdiler eklenmesi
 - ▶ Verilerin çalınması
- ▶ **Ethical Hacking**
 - ▶ Konsept olarak aynı
 - ▶ Temel fark: Amaç
- ▶ **Hacking (Tanım):** Çeşitli güvenlik açıklıklarını araştırabilme yeteneği.

Ethical Hacking

- ▶ **Tanım:** Teknolojiyi daha iyi hale getirmek amacıyla kaynakların test edilmesidir.
 - ▶ **Ethical hacking = Sızma testi**

Tanımlar

- ▶ Hacking: odak noktası zafiyet (vulnerability) ve sömürü (exploit)
 - ▶ **Zafiyet:** Yazılım üzerinde veya yazılım konfigurasyonunda bulunan zayıf halka.
 - ▶ Yazılım: SQL injection (parameterized sql kullanılmaması).
 - ▶ Konfigurasyon: Veritabanının parola politikasında hatalı deneme sayısının yüksek olması.
 - ▶ **Sömürü:** Zayıf halkayı kullanarak zarar verme işlemi için kullanılan araç.
 - ▶ Kod parçası veya teknoloji olabilir.
 - ▶ Eğer exploit bir kod ise, genellikle oldukça ufak kod parçalarıdır.

İçindekiler

1 Giriş

- Ders Hakkında
- Internet
- Bashlite
- Terminoloji

2 Tehditler ve Saldırı Vektörleri

- Saldırılar
- Saldırı Vektörleri
- Bilgi Savaşı

3 Ethical Hacking

- Ethical Hacking
- Tanımlar

4 Temel Kavramlar

- Penetrasyon Testi (Pentest)
- Standartlar
- Zafiyet Taraması
- Sızma Testi Yaklaşımıları

● Saldırı Türleri

5 PenTest Planlaması

- Planlama
- Amaç
- Kapsam
- Gereksinimler
- Sınırlamalar

6 Metodoloji

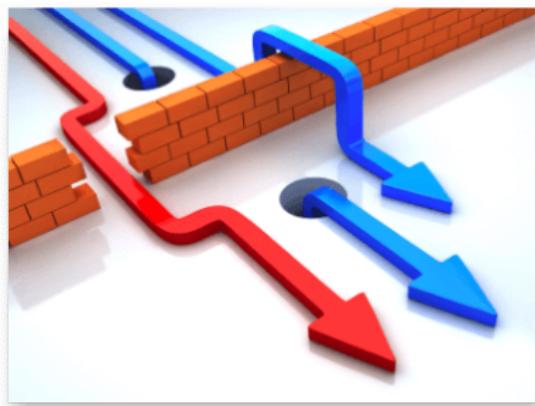
- Giriş
- Keşif
- Tarama
- Erişim Kazanma
- Sistemde Kalıcı Olma

7 Diğer Konular

- Kullanılan Araçlar
- Kali Linux
- Raporlama

Penetrasyon Testi (Pentest) I

Tanım



- ▶ **Sızma Testi:** Bilgisayar sistemlerinin daha güvenli hale getirilmesi için bilgisayarlarda bulunan açıklık ve zayıflıklar kullanılarak yapılan yasal ve yetkili erişimdir.
- ▶ Diğer isimlendirmeler
 - ▶ Penetrasyon testi
 - ▶ Hacking
 - ▶ Ethical hacking
 - ▶ Offensive security
- ▶ Kurumlara sistemlerini daha güvenli hale getirmelerini sağlamak

Penetrasyon Testi (Pentest) II

Tanım

► Yetkili olarak yapanlara

- ▶ *White hat*
- ▶ *Ethical hacker*
- ▶ *Penetration tester*



► Yetkisiz olanlara

- ▶ *Black hats*
- ▶ *Crackers*
- ▶ *Malicious attackers*

Benzerlik/Fark

- ▶ *Ethical hacker, malicious attacker*'ların kullandığı aynı aktiviteleri ve benzer araçları kullanmaktadır.
- ▶ *White hat, black hat* farkı: Yetki. Herhangi bir test/saldırı yapılmadan önce onay alınması.

Penetrasyon Testi (Pentest) III

Tanım

Saldırırganlarının Sınıflandırılması

BlackHat

Kötü niyetli veya yıkıcı faaliyetlere başvuran ve aynı zamanda **cracker** olarak da bilinen kişiler.

WhiteHat

Bilgisayar korsanlığı becerilerini savunma amaçlı kullanan kişiler, **güvenlik analistleri** olarak da bilinirler.

GrayHat

Hem saldırı hem savunma tarafında yer alan kişiler.

Script Kiddies

Gerçek korsanlar tarafından geliştirilen **komut dosyalarını, araçları ve yazılımı**, beceri sahibi olmayan kişiler

Cyber Terrorists

Bilgisayar sistemlerine saldırımı için **dini** veya **siyasi** inançlarla motive edilmiş geniş beceri düzeyine sahip kişiler

Devlet Destekli Hackerlar

Hükümetler tarafından çok gizli bilgilere nüfuz etmek ve diğer hükümetlerin bilgi sistemlerine zarar vermek amacıyla istihdam edilen kişiler.

Hacktivist

Özellikle web sitelerini engelleyen veya devre dışı bırakılan, korsanlıkla siyasi gündemi teşvik eden kişiler.

Standartlar



► NDA (Non Disclosure Agreement)

- *Gizlilik sözleşmesi:* Kuruluş hassas bilgilerinin korunması
- **PCI DSS (Payment Card Industry - Data Security Standard)**
 - <https://www.pcisecuritystandards.org/documents/PenetrationTestingStandard.pdf>
- **PTES (Penetration Testing Execution Standard)**
 - <http://www.pentest-standard.org/>

► NIST SP800-115

- Technical Guide to Information Security Testing and Assessment

► FedRAMP (Federal Risk and Authorization Management Program)

- FedRAMP Penetration Test Guidance 1.0.1

► OSSTMM v3

► OWASP (Open Web Application Security Project) Testing Guide

Zafiyet Taraması (Vulnerability Assessment) ve Sızma Testi



- ▶ **Zafiyet Taraması :** Güvenlik açıklıklarının belirlenmesi. Zafiyetlerin belirlenmesi, sayısallaştırma, önceliklendirme.
 - ▶ Ortaya çıkan sonuçlar sadece uyarı: Örnek: **https** kullanılması gereken bir yerde **http** kullanılması zafiyet taramasında bulgudur. Fakat sistemde bir gereklilik olabilir.
 - ▶ **Adımlar:**
 - ▶ Sistem yer alan varlıklarını ve kaynakları tanımla.
 - ▶ Kaynaklara önemlerine göre sayısal değer ata.
 - ▶ Her bir kaynak için güvenlik zafiyetlerini ve potansiyel tehditleri belirle.
 - ▶ En değerli kaynaklar için en önemli zafiyetleri kaldır.
- ▶ **Sızma Testi :**
 - ▶ Sızma gerçekleştiriliip, istismar (exploitation) yapılır.
 - ▶ Kavram ispatı (Proof of concept PoC) gerçekleştirilir.

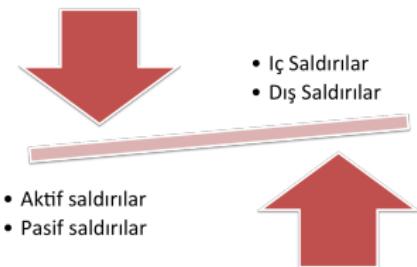
Sızma Testi Yaklaşımları

Pentest



- ▶ **Black-Box:** Test edilen sistem ve ağ altyapısı hakkında herhangi bir bilgi olmaksızın dışarıdan yapılan güvenlik değerlendirmesi ve test işlemidir.
 - ▶ **Avantajı:** Gerçek saldırgan metodlarını kullanarak sonuca ulaşılır.
 - ▶ **Dezavantajı:** Zaman ve test maliyeti
- ▶ **Gray-Box:** Ağ içersinde yer alan kişilerin erişimlerinin artırılması testidir. Amaç, çalışanların veya yüklenicilerin yetkilerini erişim yetkilerini artırabildiğinin test edilmesi.
- ▶ **White-Box:** Sistem yöneticisinin sahip olduğu bilgilere sahip olarak yapılan güvenlik değerlendirmesi ve testi.
 - ▶ **Avantajı:** Ön bilgi toplama aşamasını geçip direk saldırısı aşamasına geçilir. Maliyet ve zaman olarak düşük.

Saldırı Türleri



- ▶ Birinci yaklaşım
 - ▶ **Aktif saldırı (Active attacks)**: Sistem veya ağ üzerinde değişiklik yapmak için yapılan saldırılar. CIA (Confidentiality, Integrity, Availability) saldırıları.
 - ▶ **Pasif saldırı (Passive attacks)**: Gizlilik ihlalleri. Hassas verinin ifşa olması.
- ▶ İkinci yaklaşım
 - ▶ **İç saldırılar (Inside attacks)**: Organizasyonun güvenlik şemsiyesinin içinde yer alan kullanıcılar (çalışanlar)
 - ▶ **Dış saldırılar (Outside attacks)**: Internet veya uzaktan erişim gibi kurum dışı saldırılar.

İçindekiler

1 Giriş

- Ders Hakkında
- Internet
- Bashlite
- Terminoloji

2 Tehditler ve Saldırı Vektörleri

- Saldırılar
- Saldırı Vektörleri
- Bilgi Savaşı

3 Ethical Hacking

- Ethical Hacking
- Tanımlar

4 Temel Kavramlar

- Penetrasyon Testi (Pentest)
- Standartlar
- Zafiyet Taraması
- Sızma Testi Yaklaşımıları

● Saldırı Türleri

5 PenTest Planlaması

- Planlama
- Amaç
- Kapsam
- Gereksinimler
- Sınırlamalar

6 Metodoloji

- Giriş
- Keşif
- Tarama
- Erişim Kazanma
- Sistemde Kalıcı Olma

7 Diğer Konular

- Kullanılan Araçlar
- Kali Linux
- Raporlama

PenTest Planlaması



Aşamalar

- ▶ Amaç
- ▶ Kapsam
- ▶ Gereksinimler
- ▶ Sınırlamalar

Amaç



► **Hedef Belirleme :**

- ▶ Kuruluşa yer alan bütün paydaşlar hedeflerin belirlenmesinde yer almalıdır.
 - ▶ Veri kümelerinin kritiklik seviyesinin belirlenmesi
 - ▶ Korunması en önemli kaynaklara odaklanması sağlanması

► **Uyum Gereksinimleri(Compliance Requirements)**

Kapsam



- ▶ Etki Alanı
- ▶ Sunucular
- ▶ Veritabanı
- ▶ Uygulamalar
- ▶ Sosyal Mühendislik
- ▶ DDoS
- ▶ Fiziksel Güvenlik

Gereksinimler



► Gerekli Araçlar

- ▶ Linux tabanlı bilgisayar
- ▶ nmap
- ▶ theharvester

► Yedekleme Yapılması Gerekenler

► Acil Önlem Planı

Sınırlamalar



- ▶ **Kapsam**
- ▶ **Zaman**
- ▶ **Erişim** (veritabanı, intranet)
- ▶ **Yöntem**
 - ▶ **Örnek:** Brute force yapılması

İçindekiler

1 Giriş

- Ders Hakkında
- Internet
- Bashlite
- Terminoloji

2 Tehditler ve Saldırı Vektörleri

- Saldırılar
- Saldırı Vektörleri
- Bilgi Savaşı

3 Ethical Hacking

- Ethical Hacking
- Tanımlar

4 Temel Kavramlar

- Penetrasyon Testi (Pentest)
- Standartlar
- Zafiyet Taraması
- Sızma Testi Yaklaşımları

● Saldırı Türleri

5 PenTest Planlaması

- Planlama
- Amaç
- Kapsam
- Gereksinimler
- Sınırlamalar

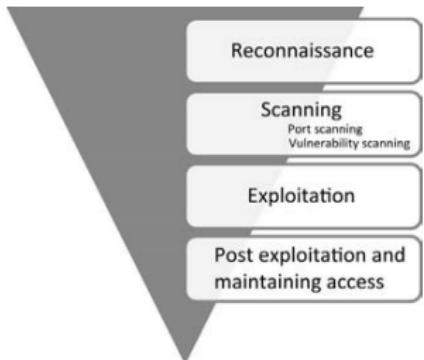
6 Metodoloji

- Giriş
- Keşif
- Tarama
- Erişim Kazanma
- Sistemde Kalıcı Olma

7 Diğer Konular

- Kullanılan Araçlar
- Kali Linux
- Raporlama

Metodoloji



Şekil: Pентest metodoloji

- ▶ Literatürde farklı (3-7) aşama mevcut (Reconnaissance, Scanning, Gaining Access, Maintaining Access, Covering Tracks)
- ▶ Sıralama önemli
- ▶ Son aşama: "hiding", "removing evidence"
- ▶ Ters üçgen: ilk aşamanın çıktısı oldukça geniş. Aşağıya doğru spesifik hale gelmektedir. Ağ taramasından elde edilen sonuçlar.
- ▶ IP adresi nedir? Hedef işletim sistemi? hangi servisler ve yazılımlar (versiyon bilgileri)?

Faz 1: Keşif (Reconnaissance) I

- ▶ En önemli aşama. Ne kadar süre harcanırsa ilerleyen aşamalar o kadar başarılı.
- ▶ Saldırganlar, atak başlatmadan önce hedef hakkında bilgi toplamaya çalışırlar.
- ▶ Hedef hakkında geniş ölçekli bilgi sahibi olunması durumunda, saldırı için giriş kolaylığı olan noktanın bulunması
- ▶ Hedef aralığı: kuruluşun **müşterileri, çalışanları, operasyonu, ağ ve sistemleri**

Faz 1: Keşif (Reconnaissance) II

Recon. Türleri

Pasif Recon.

- ▶ Direk olarak hedefle etkileşim yoktur. Hedefin yapılan işle ilgili bilgisi, kayıtları yoktur.
- ▶ Örnek: haberlerde çıkan kayıtların araştırılması

Aktif Recon.

- ▶ Hedefle ile direkt etkileşim.
- ▶ Ağ incelenerek sunucular, IP adresleri ve servislerin keşfi.
- ▶ Farkedilme ihtimali yüksek.
- ▶ Bir çok yazılım aracı, aktif keşif yaparak bilgi toplamaktadır.

Faz 1: Keşif (Reconnaissance) III

Örnek Araçlar

- ▶ *theharverster*⁴ : e-mail toplama
- ▶ *Google Direktifleri (Google-Fu)*:site:domain term(s) to search, allintitle:index of, filetype:pdf
- ▶ *httrack*⁵ : web site kopyalama aracı
- ▶ *FOCA (Fingerprinting Organizations with Collected Archives)*⁶ : belgelerin meta verileri ve gizli bilgilerini bulmak için çoğunlukla kullanılan bir araçtır.

Faz 1: Keşif (Reconnaissance) IV

Faz 1: Keşif (Reconnaissance) V

```
[+] Emails found:  
-----  
ulakbim.dpdestek@tubitak.gov.tr  
eris@uekae.tubitak.gov.tr  
jsmith@tubitak.gov.tr  
smith@tubitak.gov.tr  
john.smith@tubitak.gov.tr  
kemal.tan@tubitak.gov.tr  
cafer.kirbas@tubitak.gov.tr  
baki.karaboce@tubitak.gov.tr  
karatas@tubitak.gov.tr  
dilek.sahin@tubitak.gov.tr  
yte.bilgem@tubitak.gov.tr  
temiztektr@tubitak.gov.tr  
bayram.yilmaz@tubitak.gov.tr  
1511@tubitak.gov.tr
```

⁴<https://github.com/laramies/theHarvester>

⁵<https://www.httrack.com>

⁶<https://www.elevenpaths.com/labstools/foca/index.html>

Faz 2: Tarama

- ▶ **Pre-Attack** : Saldırgan, keşif sırasında toplanan bilgilere dayanarak belirli bilgiler için ağı tarar.
- ▶ **Port taraması**: port scanners, network mappers, ping tools, vulnerability scanners
- ▶ **Bilgi çıkarımı**: saldırısı aşamasında kullanılmak üzere açık sunucular, portlar, port durumları, OS detayları gibi bilgilerin elde edilmesi.



Faz 3: Erişim Kazanma

- ▶ Sistem üzerinde kontrolün elde edilmesi.
- ▶ Sistem üzerinde yer alan zafiyetin gerçekleştirilemesi.
- ▶ **Sızma**'nın gerçekleştirildiği aşama
- ▶ Buffer overflow, Denial of Servis (DoS), session hijacking, password cracking
- ▶ İşletim sistemi seviyesi, uygulama seviyesi veya ağ seviyesinde erişim kazanılmıştır.

Faz 4: Sistemde Kalıcı Olma

- ▶ Tartışılması gereken bir konu
- ▶ Sistem üzerinde elde edilen sahipligin kalıcı hale gelmesi
- ▶ Sahip olunan sistem üzerinde yer alan yazılımların indirilmesi, manipüle edilmesi veya konfigürasyonun değiştirilmesi

İçindekiler

1 Giriş

- Ders Hakkında
- Internet
- Bashlite
- Terminoloji

2 Tehditler ve Saldırı Vektörleri

- Saldırılar
- Saldırı Vektörleri
- Bilgi Savaşı

3 Ethical Hacking

- Ethical Hacking
- Tanımlar

4 Temel Kavramlar

- Penetrasyon Testi (Pentest)
- Standartlar
- Zafiyet Taraması
- Sızma Testi Yaklaşımları

● Saldırı Türleri

5 PenTest Planlaması

- Planlama
- Amaç
- Kapsam
- Gereksinimler
- Sınırlamalar

6 Metodoloji

- Giriş
- Keşif
- Tarama
- Erişim Kazanma
- Sistemde Kalıcı Olma

7 Diğer Konular

- Kullanılan Araçlar
- Kali Linux
- Raporlama

Pentest Sırasında Kullanılan Araçlar

► Kesif

- ▶ Nmap
- ▶ Hping
- ▶ Scapy

► Sniffer

- ▶ Cain & Abel
- ▶ Tcpdump
- ▶ Wireshark

► Zafiyet Tarama

- ▶ Nessus
- ▶ Metasploit
- ▶ Immunity Canvas

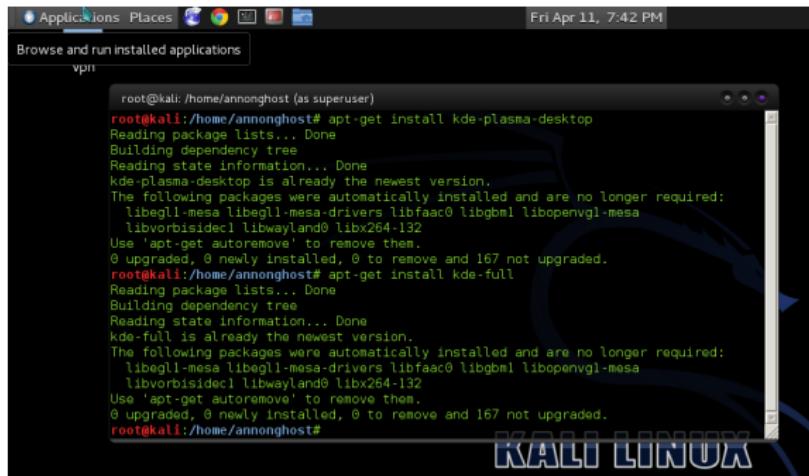
► Brute Force

- ▶ Hydra
- ▶ John the Ripper
- ▶ Cain, Ophrack

► Web

- ▶ Burp
- ▶ Acunetix
- ▶ Net sparker

Kali Linux



Şekil: Kali linux

- Debian tabanlı, sızma testi için tasarlanmış Linux dağıtımı

- Offensive Security şirketi tarafından fonlanmaktadır.

- nmap
- Wireshark
- John the Ripper

Raporlama

- ▶ Sızma testlerinin en önemli aşaması: **Raporlama**
- ▶ Sızma testi yapılan kurum için yapılan işin değerlendirmesi: Raporun kalitesi.
- ▶ **Yönetici özeti** (executive summary), her bir raporda olmalıdır.
 - ▶ 1-2 sayfalık, basit ifadelerle, bulgularınızın teknik olmayan ifadelerle özetlenmesi
- ▶ **Kapsam**
 - ▶ Sızma testinin yapıldığı IP adresleri
- ▶ **Bulgular**
 - ▶ Yetersiz kimlik doğrulama: Sayfa ...', kullanıcı herhangi bir kullanıcı adı/şifre login olabilmektedir.
 - ▶ Girdi filtremelemesi yetersiz: Formlarda javascript filtreleme yok
- ▶ **Tavsiyeler**
 - ▶ SQL injection saldırılarına karşı stored procedure kullanımı.
 - ▶ VT üzerinde erişim kontrolü
 - ▶ Gereksiz IIS modüllerinin kapatılması