

Giriş

BGM 531 - Sızma Testleri ve Güvenlik Denetlemeleri

Bilgi Güvenliği Mühendisliği
Yüksek Lisans Programı

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

İstanbul Şehir Üniversitesi
2018/2019 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 Yaklaşımları

• Saldırı Türleri

5 PenTest Planlaması

- Planlama
- Pen Test Tipleri
- 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
- Pen Test Tipleri
- Amaç
- Kapsam
- Gereksinimler
- Sınırlamalar

6 Metodoloji

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

7 Diğer Konular

- Kullanılan Araçlar
- Kali Linux
- Raporlama

Ders Hakkında I

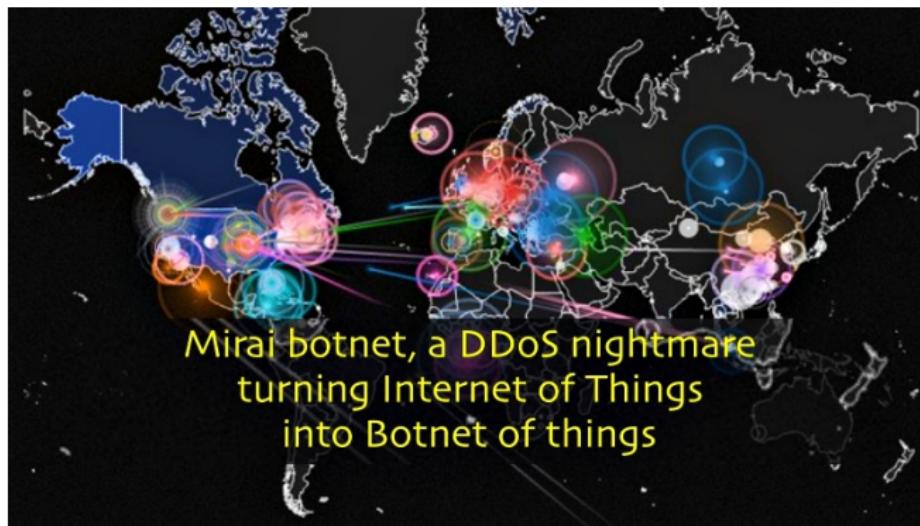
- ▶ Dr. Ferhat Özgür Çatak
 - ▶ TÜBİTAK - BİLGEM Siber Güvenlik Enstitüsü
 - ▶ ozqur.catak@tubitak.gov.tr

- ▶ **Ders web sitesi:**
<http://www.ozgurcatak.org/courses/bgm531>
 - ▶ Bütün duyurular buradan yapılmaktadır. Takip edin

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

- ▶ Sınavlar çoktan seçmeli sorular şeklinde
 - ▶ Bilgisayar Lab ???
 - ▶ Virtualbox, Kali Linux

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://ipwm.com/reports/lo-cameras-default-passwords-directory
root/lanke	ANKO Products DVR	http://www.cvcforum.com/viewtopic.php?f=3&t=44250
root/p@ss	Axis IP Camera, et. al	http://www.diancas.com/router-default/Axis0543-001
root/lvzv	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/7uMko0vIzv	Dahua IP Camera	http://www.cam-it.org/index.php?topic=9398.0
root/7uMko0admin	Dahua IP Camera	http://www.cam-it.org/index.php?topic=9396.0
666666/666666	Dahua IP Camera	http://www.diancas.com/router-default/DahuaDH-IPC-HDVA4300C
root/dreambox	Dreambox TV Receiver	https://www.satellites.co.uk/forums/threads/reset-root-password-plugin.10114/
root/lzx	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.cvcforum.com/viewtopic.php?f=56&t=34930&start=15
root/h3518	HiSilicon IP Camera	https://facassie.wordpress.com/2014/08/01/get-a-new-h3518-ip-camera-modules/
root/kv123	HiSilicon IP Camera	https://gist.github.com/gabonator/74cd9ab47733ff047356198c781527d
root/hv124	HiSilicon IP Camera	https://gist.github.com/gabonator/74cd9ab47733ff047356198c781527d
root/ybzd	HiSilicon IP Camera	https://gist.github.com/gabonator/74cd9ab47733ff047356198c781527d
root/admin	IPX-ODK Network Camera	http://www.ipinc.com/products/cameras-as-video-servers/network-cameras/
root/system	iQinVision Cameras, et. al	https://ipwm.com/reports/lo-cameras-default-passwords-directory
admin/mmeinsm	Mobots Network Camera	http://www.forum.usip.co.uk/threads/mobots-default-password.79/
root/54321	Packet8 VoIP Phone, et. al	http://webcache.googleusercontent.com/search?q=cache:V1phzGZURUJj.community.freepbx.org/packet8-atlas-phones/44
root/0000000000	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://ipwm.com/reports/lo-cameras-default-passwords-directory
root/xmhdpic	Shenzhen Anran Security Camera	https://www.amazon.com/MegaPixel-Wireless-Network-Surveillance-Camera/product-reviews/B00E86FNDI
admin/srmadmin	SMC Routers	http://www.diancas.com/router-default/SMCRUTER
root/kwb	Toshiba Network Camera	http://faq.surveilledsupport.com/index.php?action=article&id=8&lang=en
ubntubnt	Ubiquiti AirOS Router	http://ubntusergroup.com/forums/ubiquiti/airos-argnd-m9nlog.htm
supervisor/supervisor	VideoIQ	https://ipwm.com/reports/lo-cameras-default-passwords-directory
root/none>	Vivotek IP Camera	https://ipwm.com/reports/lo-cameras-default-passwords-directory
admin/11111	Xerox printers, et. al	http://itbyyourself.wordpress.com/2012/08/26/moggling-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

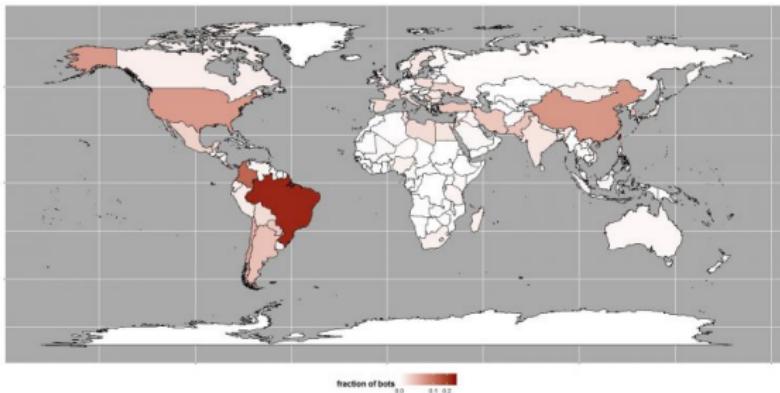
¹<https://www.hackread.com/mirai-botnet-linked-to-dyn-dns-ddos-attacks/>

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

Bashlite

Bashlite

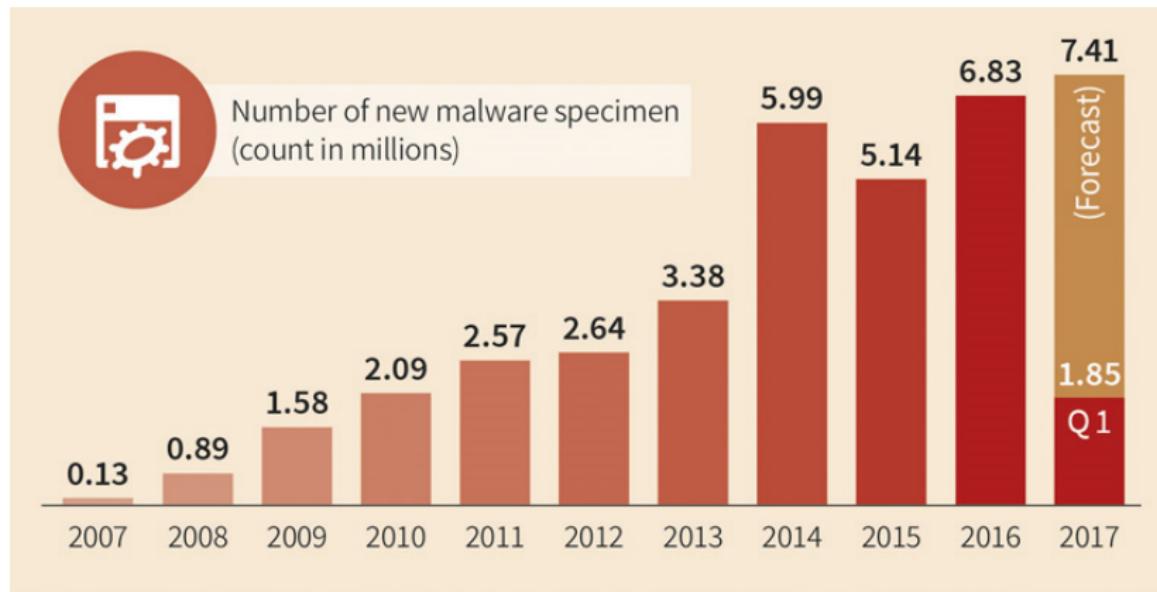
- ▶ **BASHLITE** (also known as **Gafgyt**, **Lizkebab**, **Qbot**, **Torlus** and **LizardStresser**) is malware which infects Linux systems in order to launch distributed denial-of-service attacks (DDoS).
- ▶ It has been used to launch attacks of up to 400 Gbps.



Şekil: Bashlite³

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.



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

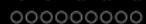
- Planlama
- Pen Test Tipleri
- Amaç
- Kapsam
- Gereksinimler
- Sınırlamalar

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

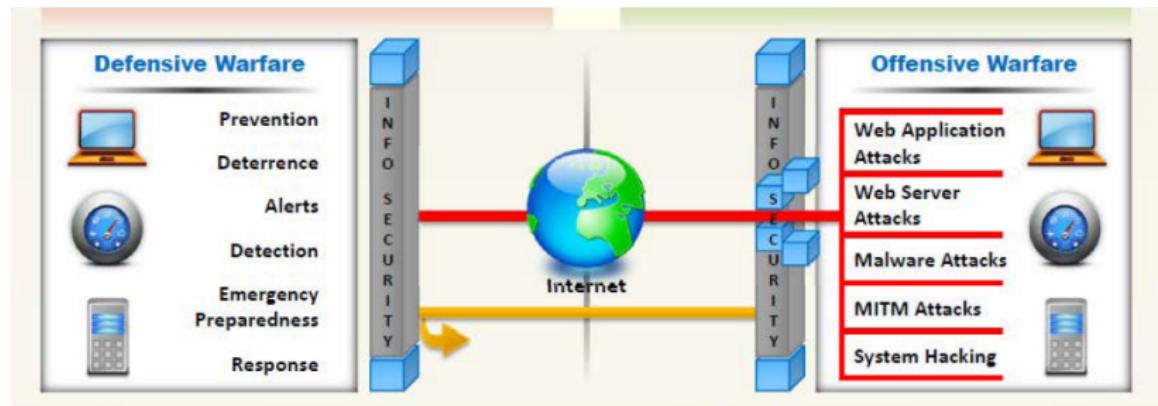
► **Shrink-Wrap Code Attacks:**

- ▶ 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
- Pen Test Tipleri
- Amaç
- Kapsam
- Gereksinimler
- Sınırlamalar

6 Metodoloji

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

7 Diğer Konular

- Kullanılan Araçlar
- Kali Linux
- Raporlama

Hacking I

Hacking

- ▶ **Hacking:** Sık duyulan ifade
 - ▶ Bir teknolojinin istenilen (veya tasarıımı) dışında davranışmasını sağlamak
- ▶ **Ethical Hacking**
 - ▶ Konsept olarak aynı
 - ▶ Temel fark: Amaç
- ▶ **Hacking (Tanım):** Çeşitli güvenlik açıklıklarını araştırabilme yeteneği.

Ethical Hacking

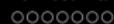
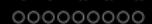
- ▶ **Tanım:** Teknolojiyi daha iyi hale getirmek amacıyla kaynakların test edilmesidir.
 - ▶ **Ethical hacking = Sızma testi**

Hacking II

Sızma Testi

Başarılı bir pentest için akılda tutulması gereken iki konu

- ▶ Sistem yöneticilerinden farklı düşünmek, yazılımı tasarlayanlardan farklı düşünmek
- ▶ Aynı zamanda, metodoloji takip etmek, dikkatli olmak
- ▶ Başarı için bu ikisi arasında bir denge sağlamak gerekmektedir.



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.
- ▶ *Threat:* Hedef sisteme zarar vermek isteyen *actor* veya *agent*

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
- Pen Test Tipleri
- Amaç
- Kapsam
- Gereksinimler
- Sınırlamalar

6 Metodoloji

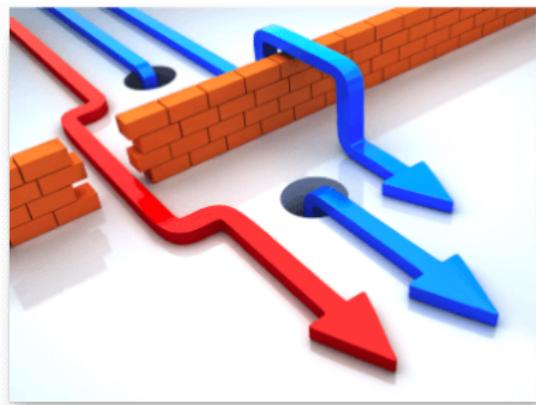
- Giriş
- Keşif
- Tarama
- Erişim Kazanma
- Sistemde Kalıcı Olma

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.

SANS - Ethical Hacking Tanımı

Ethical Hacking

- ▶ **Hacking (traditional)**: Teknolojiyi, yapmak için tasarılanmamış bir şey yapmak için manipüle etmek.
- ▶ **Hacking (sinister)**: Bilgisayarlara ve ağ sistemlerine izinsiz girme.
- ▶ **Hacker**ın önünde **ethical** kelimesinin eklenmesi, kötü çağrışımı geçersiz kılmaktadır.
- ▶ **Ethical Hacking**: Hedef sahibinin izniyle güvenlik kusurlarını bulmak ve hedefin güvenliğini arttırmak için bilgisayar saldırısı tekniklerini kullanmak.
- ▶ Wikipedia'ya göre, **White Hat Hacker** sıklıkla **etik hack** ile eşanlamlı olarak kullanılmaktadır.

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.

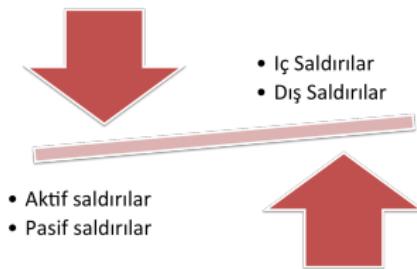
Sızma Testi Yaklaşımları

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 Yaklaşımları

● Saldırı Türleri

5 PenTest Planlaması

- Planlama
- Pen Test Tipleri
- 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

Pen Test Tipleri

Sızma Testleri

Cok sayıda etik hack ve sızma testi vardır:

- ▶ **Ağ hizmetleri testi:** En yaygın test türü.
 - ▶ ağ üzerinde hedef sistemler bulmayı
 - ▶ alta yatan işletim sistemlerinde ve mevcut ağ hizmetlerinde açıklıkları aramayı
 - ▶ bunları uzaktan kullanmasını içerir.
 - ▶ hedefin kendi tesislerinden yerel olarak başlatılır.
- ▶ **İstemci tarafı testi:** tarayıcılar, medya oynatıcılar, belge düzenleme programları vb. gibi istemci tarafı yazılımlarda güvenlik açıklarını bulmak ve bunlardan yararlanmak.
- ▶ **Web uygulama testi:** hedef ortamda bulunan web tabanlı uygulamalardaki güvenlik açıklarını.
- ▶ **Sosyal mühendislik testi:**
 - ▶ Telefon/e-posta aracılığıyla parola elde etmek
 - ▶ Bir linke tıklamasını sağlamak
- ▶ **Kablosuz güvenlik testi:** yetkisiz kablosuz erişim noktaları veya güvenlik zayıflıkları olan yetkili kablosuz erişim noktalarının araştırılması

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
- Pen Test Tipleri
- Amaç
- Kapsam
- Gereksinimler
- Sınırlamalar

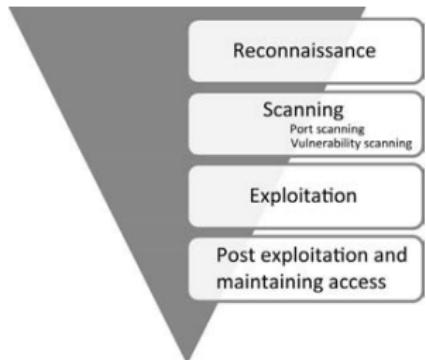
6 Metodoloji

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

7 Diğer Konular

- Kullanılan Araçlar
- Kali Linux
- Raporlama

Metodoloji I



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)?

Altyapı I

Pentest için altyapı

- ▶ Yazılım araçları
- ▶ Donanım
- ▶ Ağ altyapısı

Altyapı II

Yazılım araçları

- ▶ KALI işletim sistemi <https://www.kali.org/>
- ▶ Windows işletim sistemi ???
- ▶ Mac OS X ???
- ▶ Sanallaştırma
 - ▶ Vmware
 - ▶ VirtualBox
 - ▶ Parallels
- ▶ Diğer yazılımlar: nmap, metasploit, hydra, scapy
- ▶ Free Tools and Exploits
 - ▶ Exploit-DB: <http://www.exploit-db.com>
 - ▶ Security Focus BID search: <https://www.securityfocus.com/bid/>
 - ▶ SEBUG Vulnerability DB: <http://sebug.net>
 - ▶ Packetstorm Security: <http://packetstormsecurity.org>

Altyapı III

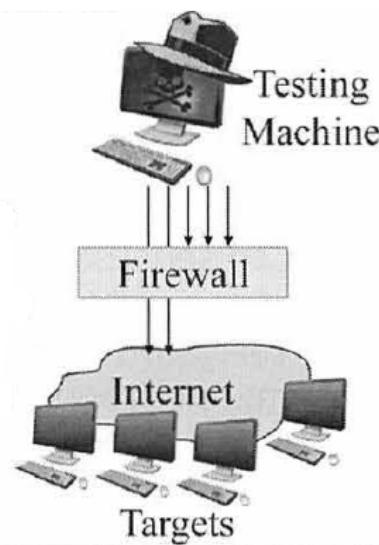
Donanım

- ▶ **Test makineleri:** Diğer makinelerin güvenliğini değerlendirmek için pentester tarafından kullanılan sistemler. *attack machines*
 - ▶ dedicated to the testing
- ▶ **Hedef makineler:** Güvenlik durumu değerlendirilen sistemler. *victim machines*

Altyapı IV

Ağ Altyapısı

- ▶ Test makineleriniz Internet'ten güvenlik duvarına alınmışsa, saldırınız engellenebilir.
- ▶ Güvenlik duvari ağ adresi çevirisi (Network Address Translation - NAT), test kullanıcılarının sorun yaratmasına neden olur;
 - ▶ Paketlerin kaynak IP adresini ağdan çıkış yolunda değiştirirler ve herhangi bir yanıt paketini orijinal IP adresine geri gönderirler.
- ▶ HTTP proxy'leri baen üzerinden geçen web trafığının kodlanması (encoding) değiştirir ve bu da "*calibrated exploitation code*" bozulmasına neden olabilir.





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: Kesif (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  
temiztekr@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**: saldırı 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 gerçekleştirilmesi.
- ▶ **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
- Pen Test Tipleri
- 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

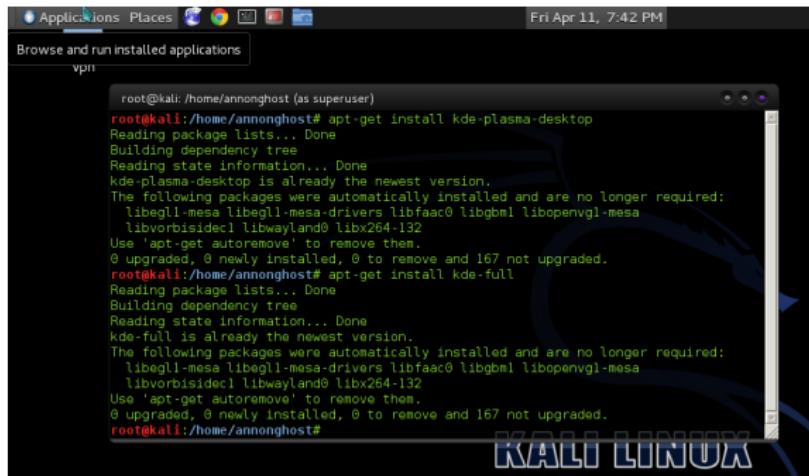
► Brute Force

- ▶ 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