Penetrasyon Testinin

Önemi

İÇERİK

Penetrasyon Testi (Pentest) Nedir, Ne Değildir ?

Kurumlar için Neden Önemlidir ?

Neden Kurumlar Pentester Arıyorlar ?

İyi Bir Pentester Nasıl Olunur ?

Sonuç

BEN KİMİM?

Ahlaklı Korsan	Mesai saatlerinde...
Blog Yazarı	http://www.mertsarica.com
Güvenlik TV	http://www.guvenliktv.org
Python Programcısı	http://www.mertsarica.com/programlar
Zararlı Yazılım Analisti	Boş zamanlarımda...
Sertifika Kolleksiyoncusu	CISSP , SSCP , OSCP , OPST , CREA

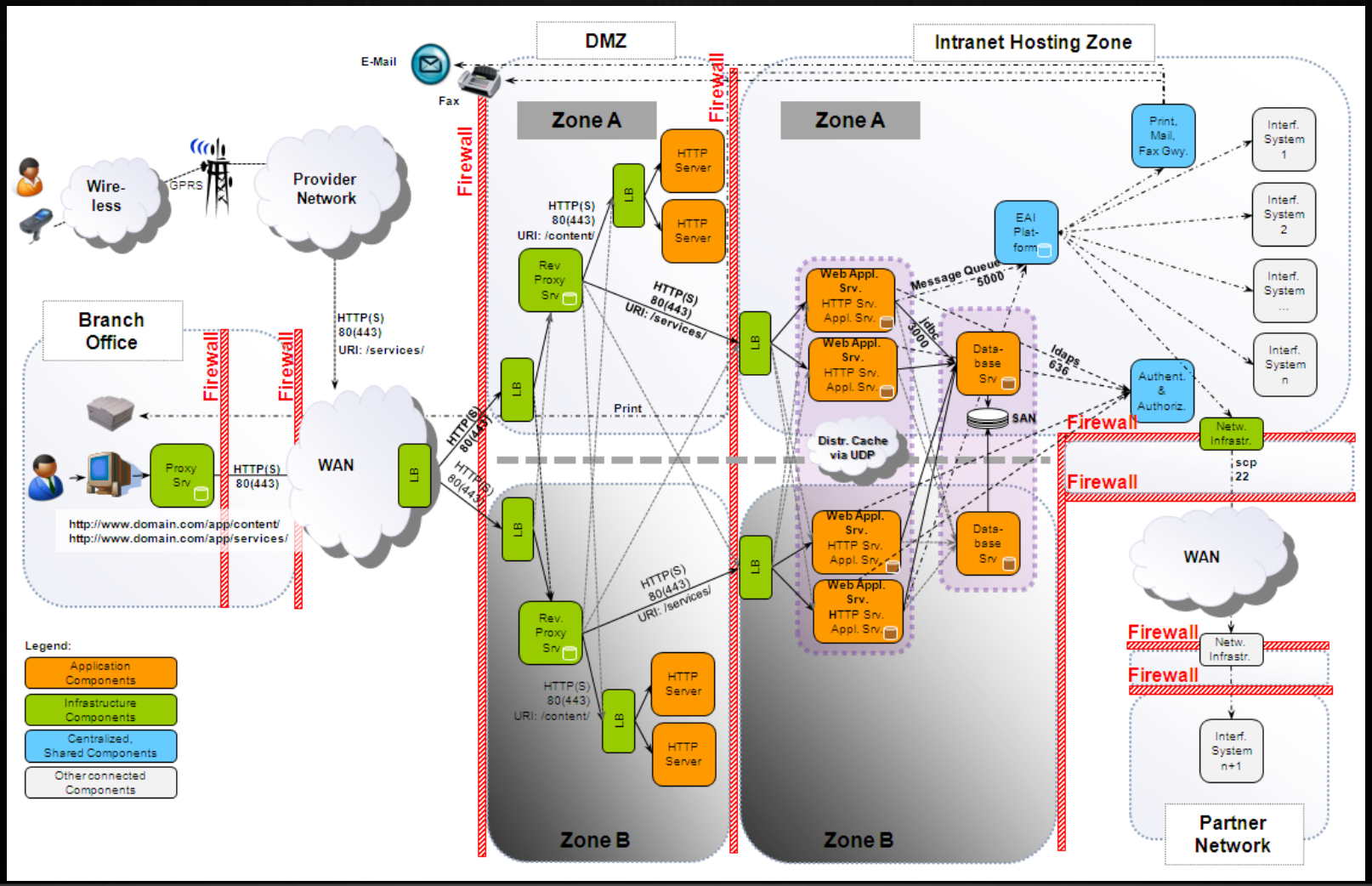
MESLEĞİM ?

Finans sektörünün ihtiyaçlarına ve günün teknolojilerine uygun hizmetler sunan, ürünler meydana getiren, NBG Grup şirketlerinden Finansbank'ın Bilgi Teknolojileri iştiraki olan IBTech firmasında Bilişim Güvenliği Uzmanı (Senior Penetration Tester / Ethical Hacker) olarak çalışmaktayım.

http://www.finansbank.com.tr

http://www.ibtech.com.tr

NEDEN PENETRASYON TESTİ ?



NEDEN PENETRASYON TESTİ ?

Regülasyonlara (PCI, BDDK vs.) uyum için.

Müşterilerinizin güvenliği için.

İtibarınız için.

Kurum içi farkındalığı arttırmak için.

Sistemlerinizi savunmak için. (En iyi savunma saldırıdır!)

SIZMA TESTİ GENELGESİ

bulunmayan bağımsız ekiplere düzenli aralıklarla sızma testleri yaptırılır. Güvenlik alanındaki güncel gelişmeler ve yeni açıklar takip edilir, gerekli yazılım güncellemeleri yapılır, gerekli yamalar uygulanır."

hükmü ile sızma testleri bankacılık sektörü için zorunlu hale getirilmiştir.

Bilgi sistemlerine yönelik olarak elektronik ortamda gerçekleştirilebilecek saldırı türlerinin de hızlı bir değişim ve gelişim göstermesi nedeniyle 27.01.2011 tarih ve 4022 sayılı Bankacılık Düzenleme ve Denetleme Kurulu Kararı ile Tebliğ'in söz konusu 7 nci maddesinin üçüncü fıkrasının (ç) bendinde yer alan hüküm ile zorunlu kılınan ve düzenli aralıklarla yapılması istenilen sızma testinin sıklığının yılda en az bir defa yapılması şeklinde belirlenmesine karar verilmiştir.

Tebliğ'in 7 nci maddesinin üçüncü fıkrasının (ç) bendi uyarınca, 2012 yılından itibaren sızma testlerinin yaptırılmasında işbu Genelge ile çerçevesi çizilen usul ve esaslar dikkate alınır.

1) Amaç

Sızma testlerinin amacı, banka bilgi sistemlerinde yetkisiz erişim elde edilmesine veya hassas bilgilere ulaşılmasına neden olabilecek güvenlik açıklarının istismar edilmeden önce tespit edilmesi ve düzeltilmesidir.

Atatürk Bulvarı No:191 Kavaklıdere 06680 ANKARA Tel: (312) 455 67 80 Faks: (312) 424 17 49
İnternet adresi: www.bddk.org.tr

2) Kapsam

Sızma testleri, **temel sızma testleri** ile bu testler sonrası uygulanacak **detaylı sızma testlerinden** oluşur. Sızma testleri kapsamında gerçekleştirilecek testler asgari olarak aşağıdaki başlıkları kapsar:

a) İletişim Altyapısı ve Aktif Cihazlar
b) DNS Servisleri
c) Etki Alanı ve Kullanıcı Bilgisayarları
ç) E-posta Servisleri
d) Veritabanı Sistemleri
e) Web Uygulamaları
f) Mobil Uygulamalar
g) Kablosuz Ağ Sistemleri
ğ) ATM Sistemleri
h) Dağıtık Servis Dışı Bırakma Testleri
i) Sosyal Mühendislik Testleri

PCI DSS v2.0

PCI Security Standards Council

PCI DSS Requirements	Testing Procedures
11.3 Perform external and internal penetration testing at least once a year and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment). These penetration tests must include the following:	**11.3.a** Obtain and examine the results from the most recent penetration test to verify that penetration testing is performed at least annually and after any significant changes to the environment.
	11.3.b Verify that noted exploitable vulnerabilities were corrected and testing repeated.
	11.3.c Verify that the test was performed by a qualified internal resource or qualified external third party, and if applicable, organizational independence of the tester exists (not required to be a QSA or ASV).
11.3.1 Network-layer penetration tests	**11.3.1** Verify that the penetration test includes network-layer penetration tests. These tests should include components that support network functions as well as operating systems.
11.3.2 Application-layer penetration tests	**11.3.2** Verify that the penetration test includes application-layer penetration tests. The tests should include, at a minimum, the vulnerabilities listed in Requirement 6.5.
11.4 Use intrusion-detection systems, and/or intrusion-prevention systems to monitor all traffic at the perimeter of the cardholder data environment as well as at critical points inside of the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up-to-date.	**11.4.a** Verify the use of intrusion-detection systems and/or intrusion-prevention systems and that all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment is monitored.
	11.4.b Confirm IDS and/or IPS are configured to alert personnel of suspected compromises.
	11.4.c Examine IDS/IPS configurations and confirm IDS/IPS devices are configured, maintained, and updated per vendor instructions to ensure optimal protection.

PENETRASYON TESTİ NEDİR ?

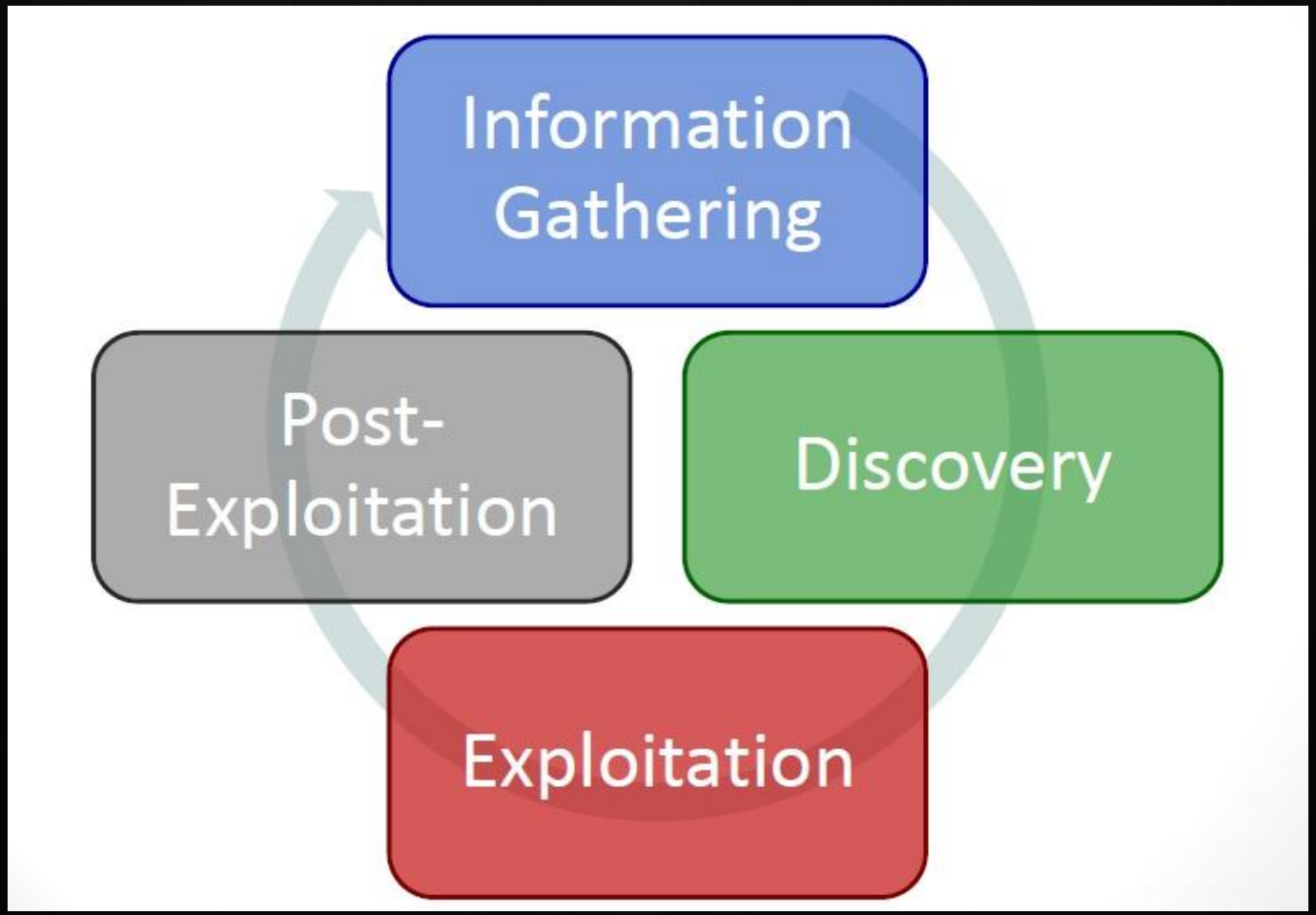
Pentest, hedef sistemlerin, ağların güvenliğinin hacker gözüyle denetlenmesi, tespit edilen zafiyetlerin istismar edilmesi ve zafiyetleri ortadan kaldıracak çözüm önerilerinin üretilmesidir.

Türleri: Whitebox, Blackbox, Greybox

Zafiyet değerlendirme testlerinden farklı olarak bu testlerde tespit edilen zafiyetler istismar edilir.

Bu testler sayesinde birden fazla düşük seviye bulgu bir araya getirilerek kritik seviyede bulgu ile sonuçlanabilir.

PENTEST DÖNGÜSÜ



PENETRASYON TESTİ NE DEĞİLDİR ?

Sadece otomatize araçlar ile « Tara ve Geç » şeklinde gerçekleştirilen testlerden değildir.

Zafiyet değerlendirme testleri gibi yüzlerce sayfalık raporlardan oluşmayabilir bu nedenle raporun sayfa sayısına göre değerlendirilmemelidir.

Amaç kapsama bağlı kalarak istismar edilebilen zafiyetlerin tespit edilmesi ve raporlanmasıdır, kapsam dışına çıkılması beklenmemelidir.

Regülasyonlara uyum nedeniyle yapmış olmak için yapılmamalıdır.

Katma değer için işin ehli kişi veya kişilerce gerçekleştirilmelidir.

SQLi vs WAS

Acunetix ☹

Webinspect ☹

Appscan ☹

Netsparker ☹

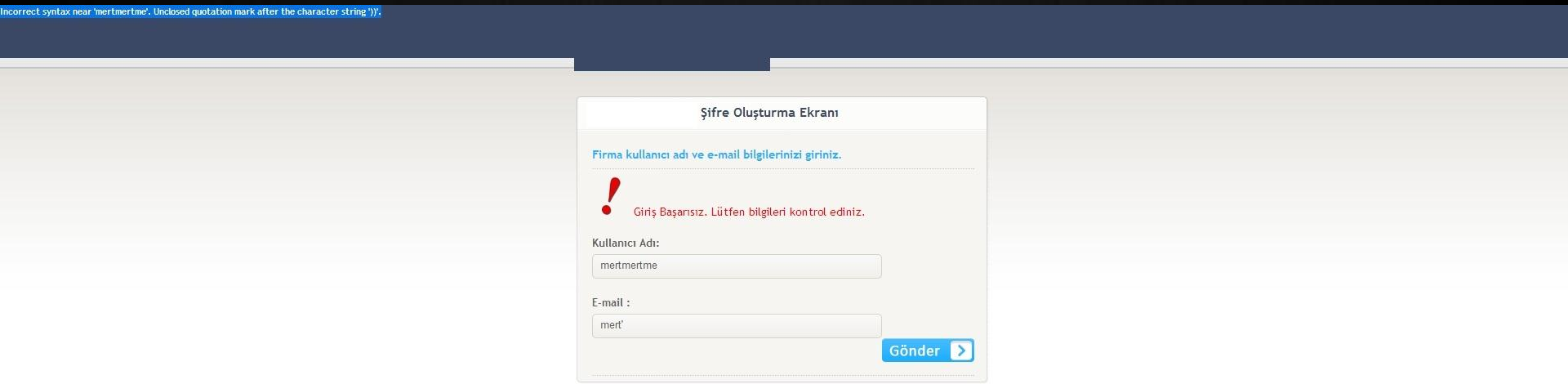
Burp Suite Pro ☹

Pentester ☺

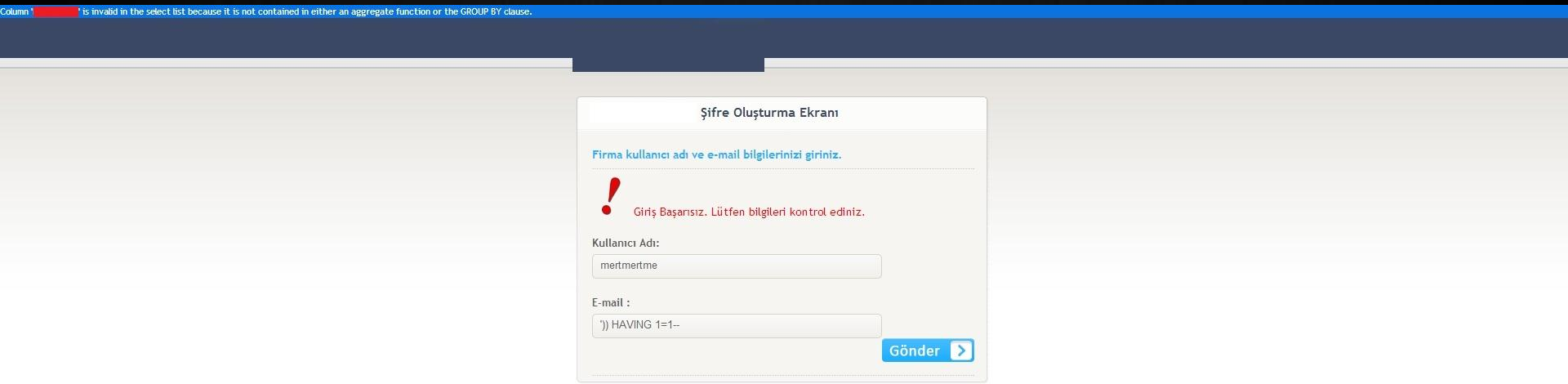
TARAYIP GEÇMEYİN!

TARAYIP GEÇMEYİN!

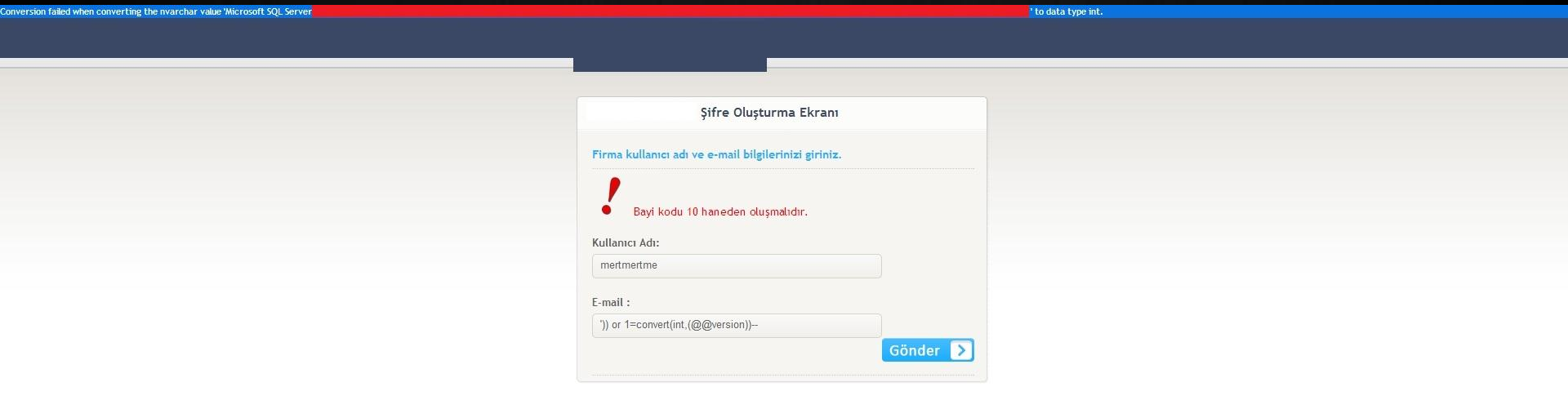
TARAYIP GEÇMEYİN!



TARAYIP GEÇMEYİN!



TARAYIP GEÇMEYİN!



NEDEN SIKI DENETİM ?

Dinamik bir yapıda yılda 1 defa sızma testi gerçekleştirilerek sistemlerin ve ağların güvenliği sağlanamaz!

Güvenlik, dış kaynaklara devredilip unutulacak bir husus değildir.

İmza tabanlı sistemlerin tamamına yakını atlatılabilmektedir.

Organize suç örgütleri artık 0. gün zafiyetlerinden faydalanmaktalar. (Elderwood Project)

En zayıf halkanız kadar güvendesiniz.

DEVRET VE UNUTUN SONU

41? 29! AJANSININ YÖNETTİĞİ FACEBOOK SAYFALARI HACKLENDİ

Alemsah Ozturk @alemsah 6 dk

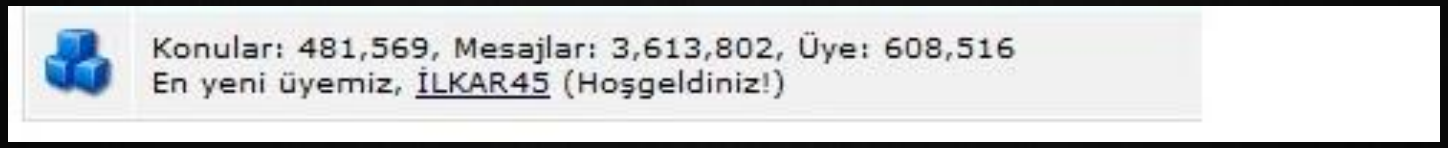
Arkadaslar, olayın ilk dakikalarından beri farkındayız, facebookla iletisim halindeyiz, herkes ayakta.

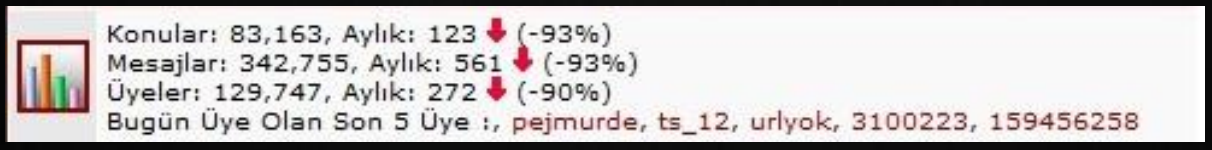
Kapat ← Yanıtla ↻ Retweetle ★ Favorilere ekle

41? 29! Ajansının yönettiği; **TTNET resmi facebook sayfası, TTNET müzik resmi facebook sayfası, Garanti Bankası resmi facebook sayfası, Bonus Card resmi facebook sayfası, DenizBank resmi facebook sayfası, Teknosa resmi facebook sayfası, Renault Türkiye resmi facebook sayfası, Acunncom resmi facebook sayfası, Ülker Çikolata resmi facebook sayfası, Metro (Ülker) resmi facebook sayfası, Dido (Ülker) resmi facebook sayfası, OMO (Kirlenmek Güzeldir) resmi facebook sayfası, Kanal D resmi facebook sayfası, Nokia Türkiye resmi facebook sayfası, Yetenek Sizsiniz Türkiye resmi facebook sayfası** ve **O Ses Türkiye resmi facebook sayfaları** dün gece PKK sempatizanı olduklarını görülen '**Amed Hack Team**' isimli bir grup tarafından hacklendi.

Olaya anında müdahale eden 41? 29! Ajansı yetkilileri, Facebook'un Londra ofisi ile birlikte çalışarak kısa bir süre içerisinde ele geçirilen sayfaların kontrolünü tekrar geri aldı. 41? 29! ajansı, sayfaların nasıl ele geçirildiği konusunda facebook yetkilileri ile birlikte çalıştıklarını ve teknik olaylar ile ilgili açıklamaları en kısa sürede paylaşacaklarını belirtti.

HACKING MERAKLILARI

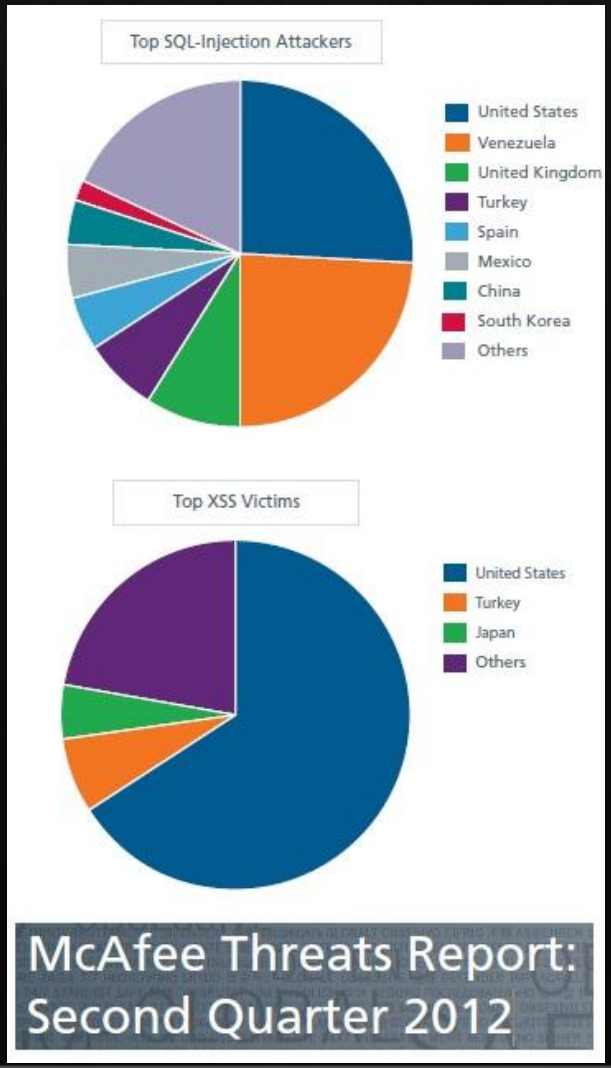




1.5

MİLYON ÜYE

MERAKTAN DA ÖTE



İSTİSMAR KİTİ vs ANTIVIRUS

Tarih: 22.06.2012

Zararlı Site Ziyaret Tarihi	URL	AV Tespit Tarihi	Ülke
18/06/2012 14:33:00 EEST	http://bell.madhousedomains.com/Set.jar	-	Rusya
18/06/2012 14:33:00 EEST	http://bowl.taxpainkiller.com/Set.jar	-	Rusya
11/06/2012 21:10:58 EEST	http://tellmeonlygoodnews.org/l/Set.jar	-	Rusya
11/06/2012 21:10:58 EEST	http://diving-pleasure.com/l/Set.jar	-	Rusya
08/06/2012 12:05:44 EEST	http://zhdrzfkzq.changeip.name/images/334857960/c17267280eeb8b395c2abca7085a2944.jar	-	-
08/06/2012 11:56:06 EEST	http://ca.miraclestove.org/Half.jar	-	Rusya
08/06/2012 11:56:»06 EEST	http://home-page.ezua.com/Half.jar	-	Kazakistan
08/06/2012 11:56:06 EEST	http://shop.rxpillcenter.com/Half.jar	-	Rusya
06/06/2012 19:20:43 EEST	http://kioiwrsd.tk/33982.jar	22.06.2012	Rusya
06/06/2012 19:20:43 EEST	http://gkiqaue.tk/33982.jar	-	-

HEDEFLENMİŞ SALDIRI

Redhack Türkiye Telefon Sistemini Hackledi!

by admin on 19 Eylül 2012

Beğen 80 +1 1 Tweetle 113

Sosyalist hacker grubu Redhack son hack eylemiyle farklı bir yöne işaret etti ve "Telefon ağlarının bağlandığı ana serverın, şifreleri ile birlikte ele geçirildiğini"duyurdu.

Redhack Türkiye'nin bütün iletişim ağı ana serveri ve tüm telefon bağlantılarının adminini ele geçirdiklerini açıklarken bunun anlamını "**istenilirse bu servera bağlı hizmet alan telefonlar kesilebilir veya birbiriyle görüştürülebilir. Ayrıca bu alt ofisleri ve bağlantılarıyla birlikte yaklaşık Türkiyenin %70 i olarak hesapladığımız bir alana hitap ediyor**" diyerek açıkladı. Bu durum sosyal medyada Redhack devleti ele geçirdi şeklinde yorumlandı.

Redhack telefon şebekesinin şifrelerini kırıp ele geçirmenin yanında 1437 Eczanenin Medula şifresini aldıklarını da: "**Eczane Medula sisteminin merkezindeki personel bilgisayarlarından bazılarına trojan sızması yaptık. bu şekilde şu an 1437 eczaenin medula giriş şifresi ele geçirildi.**" diyerek açıkladılar. Eczane sisteminin işleyişinin bir ölçüde kolayca sızılıp istendiği gibi yönlendirilebileceğini ve güvenilmez olduğunu Redhack bu eylemiyle kanıtlamış oldu.

HEDEFLENMİŞ SALDIRI

[redacted]'ye bir hacker şoku daha

Hürriyet Planet

10 Ekim 2012 | A A

Tavsiye Et 92 Tweetle 68 +1 0 e-posta

Dünyaca ünlü hacker grup Anonymous'un Türkiye kolu, [redacted] Hava Yolları'nın eyleme katıldıkları gerekçesiyle işten çıkardığı 305 personele destek vermek amacıyla [redacted]'nin sistemine sızarak, yolculara ait özel bilgileri ele geçirdiğini iddia etti.

Daha önce de [redacted]'nin sitesini altı saat boyunca hack'leyerek yüz binlerce TL zarara uğratan grup, bu kez [redacted]'nin kullandığı Troya sistemine sızdığını öne sürdü.

Sisteme sızarak özel bilgilerine ulaştıkları kişiler arasında Türk ve yabancı bakanların yanı sıra rektörler, iş adamları ve sporcuların da bulunduğunu açıklayan grup, bazı yolcuların check-in bilgilerini alıp koltuk numaralarını değiştirdiklerini ve uçak seferleri öncesi karışıklığa neden olduklarını iddia etti.

[redacted]'ye her bir dakikalık rötar için yaklaşık 2 bin 500 TL zarar verdiklerini iddia eden grup, [redacted]'nin çıkardığı işçileri geri almaması ya da tazminat vermemesi durumunda eylemlerinin süreceğini ve ellerindeki daha özel bilgileri de yayınlayacaklarını belirtti.

Hacker grubun check-in kayıtlarını yayınladığı çok sayıda isim arasında Azerbaycan hükümetine bağlı olan Dini Cemaatlerle Çalışma Komiteleri Başkanlığını yürüten Elşad İskenderov, Kazakistan Bakan Yardımcısı Akmaral Baytemirova, Ak Parti Ankara Milletvekili Reha Denemeç ve eski Bakan Onur Kumbaracıbaşı da bulunuyor.

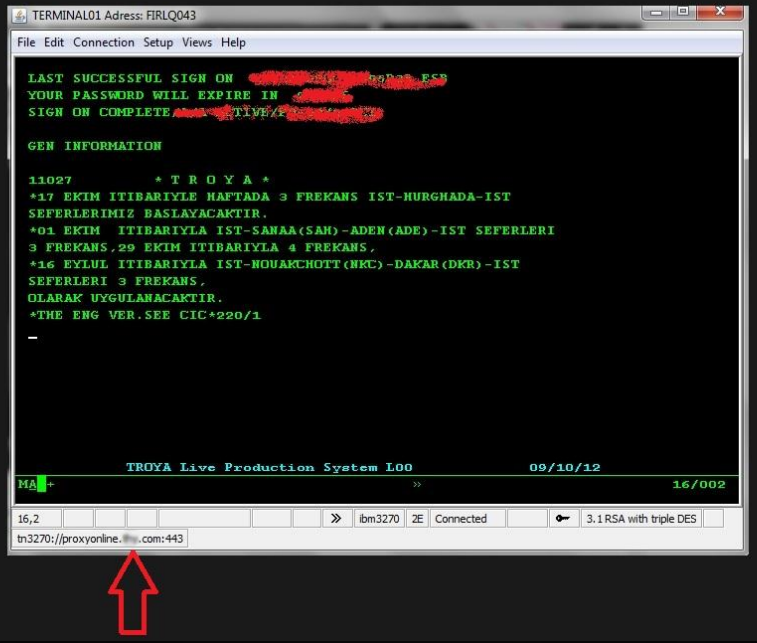
```
TK2178  09OCT IST SELECTED PAX
ISKANDAROV  ELSHAD  MR
ESB Y C S          1 Y @ 12F-M 2/53                    RM     TCKBAJ
CHECKED IN 09588D/GYD      09OCT 08.52Z                BP GROUP -B-
SECURITY NO. @084
INBOUND TK0333  1550 GYD Y OK
FQTV - * TK /ELITTK324456805
FARE BASES : ADT/25K/LY2PC
COMMENTS |UPGR| U/G ON APT BY ISTDZTK|UPGR VIP |AZERBAYCAN BAKA|
**/CHECK-IN BY VIP/**
** ET PAX TICKET: 2352210938709/C2
 PREVIOUS TRANSACTION HISTORY
09OCT/0855Z GYD/T1/09588D-RM SEAT CHG 17A -> 12F
09OCT/0905Z GYD/T1/09588D-RM -VIP ADDED    -
09OCT/1351Z IST/T1/021068-TG <TO15022> COMMENT ADDED - 1/C/A/
```

Azeri yetkili İskenderov'a ait check-in bilgileri

HEDEFLENMİŞ SALDIRI

← @AnonsTurkey's profile

Recent images by @AnonsTurkey



HEDEFLENMİŞ SALDIRI

0. Gün Zafiyeti ?

SQL Injection ?

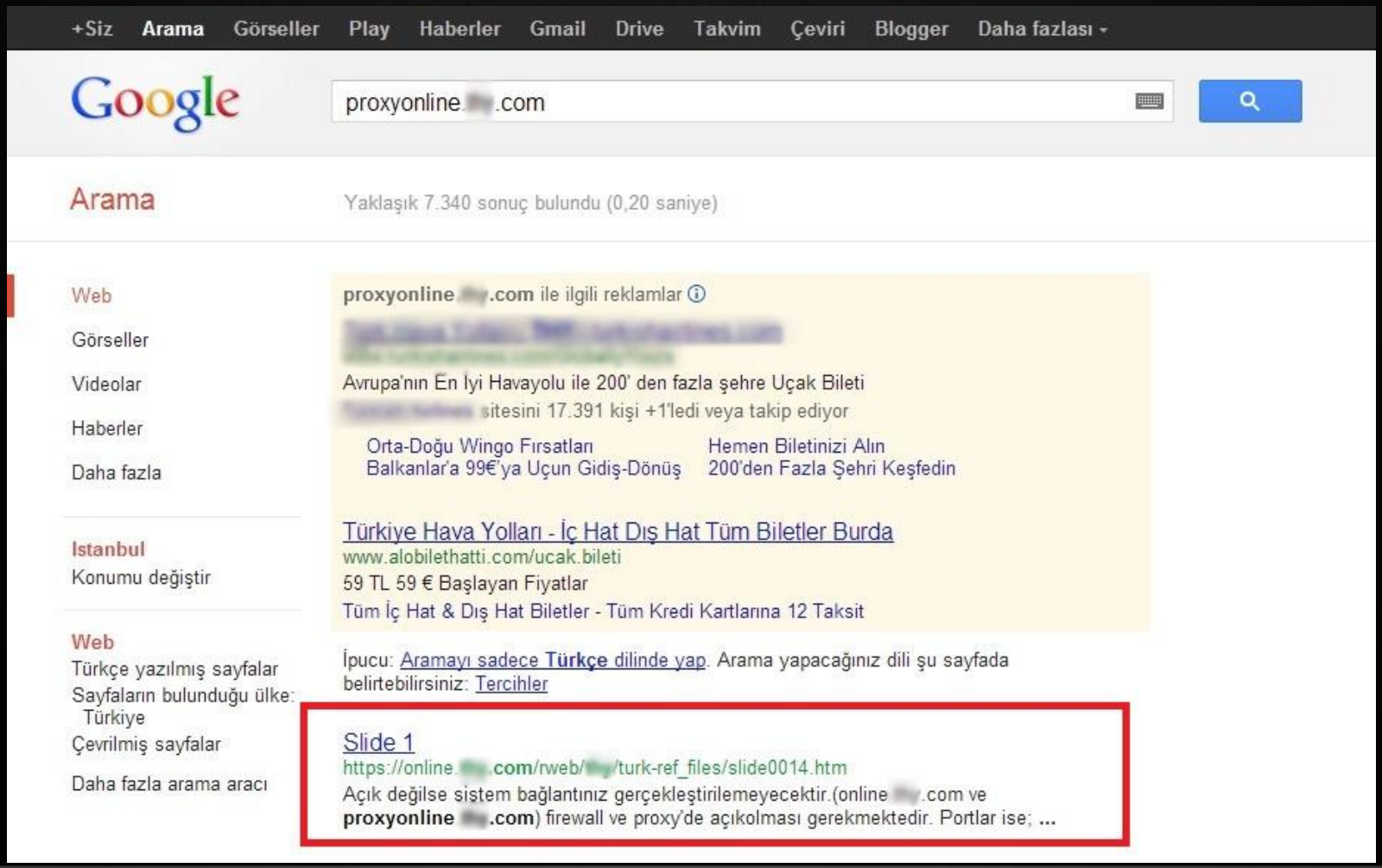
Sosyal Mühendislik ?

İç Tehdit ?

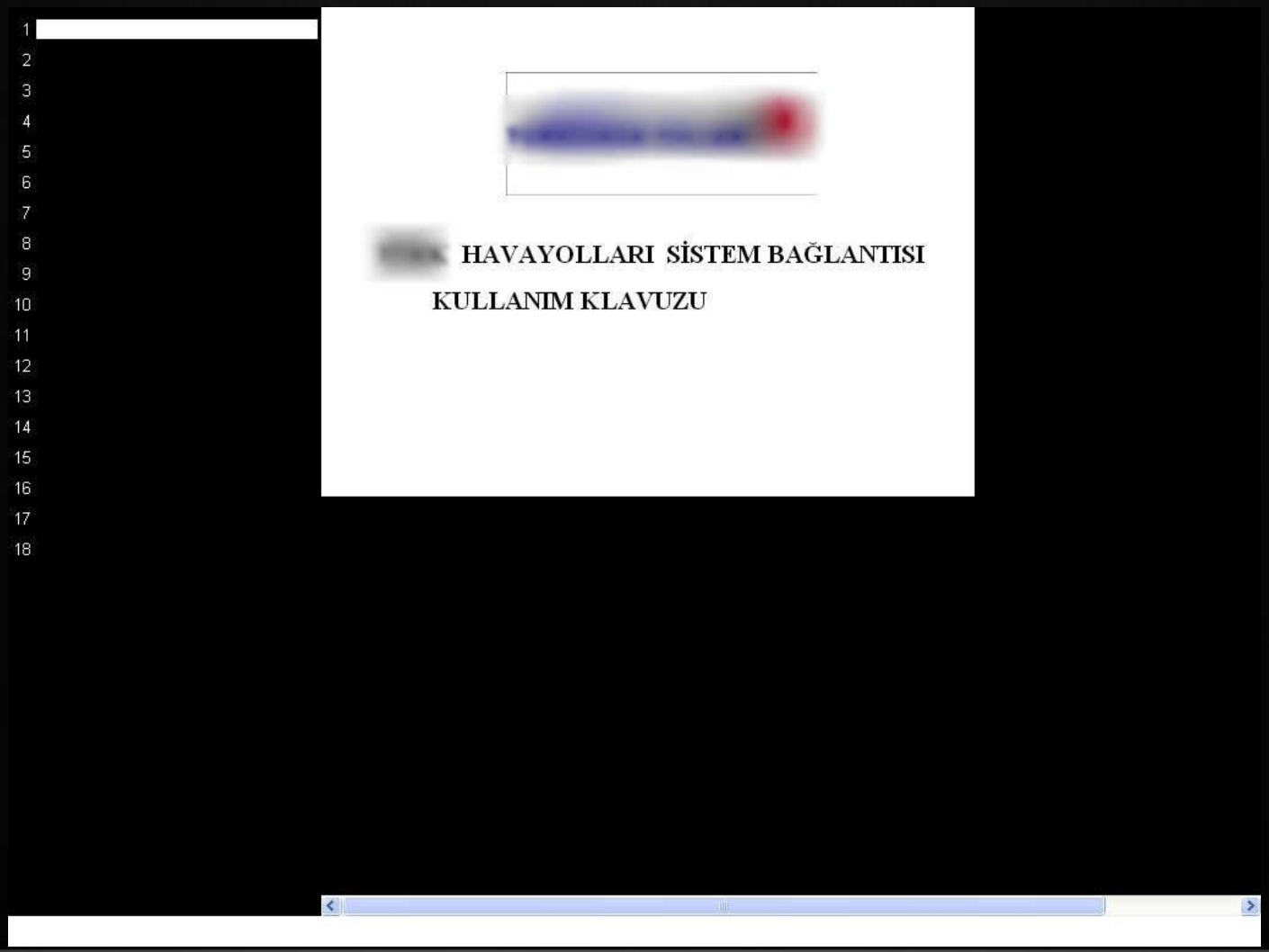
3. Parti Firma ?

Belki de sadece Google Hack ?

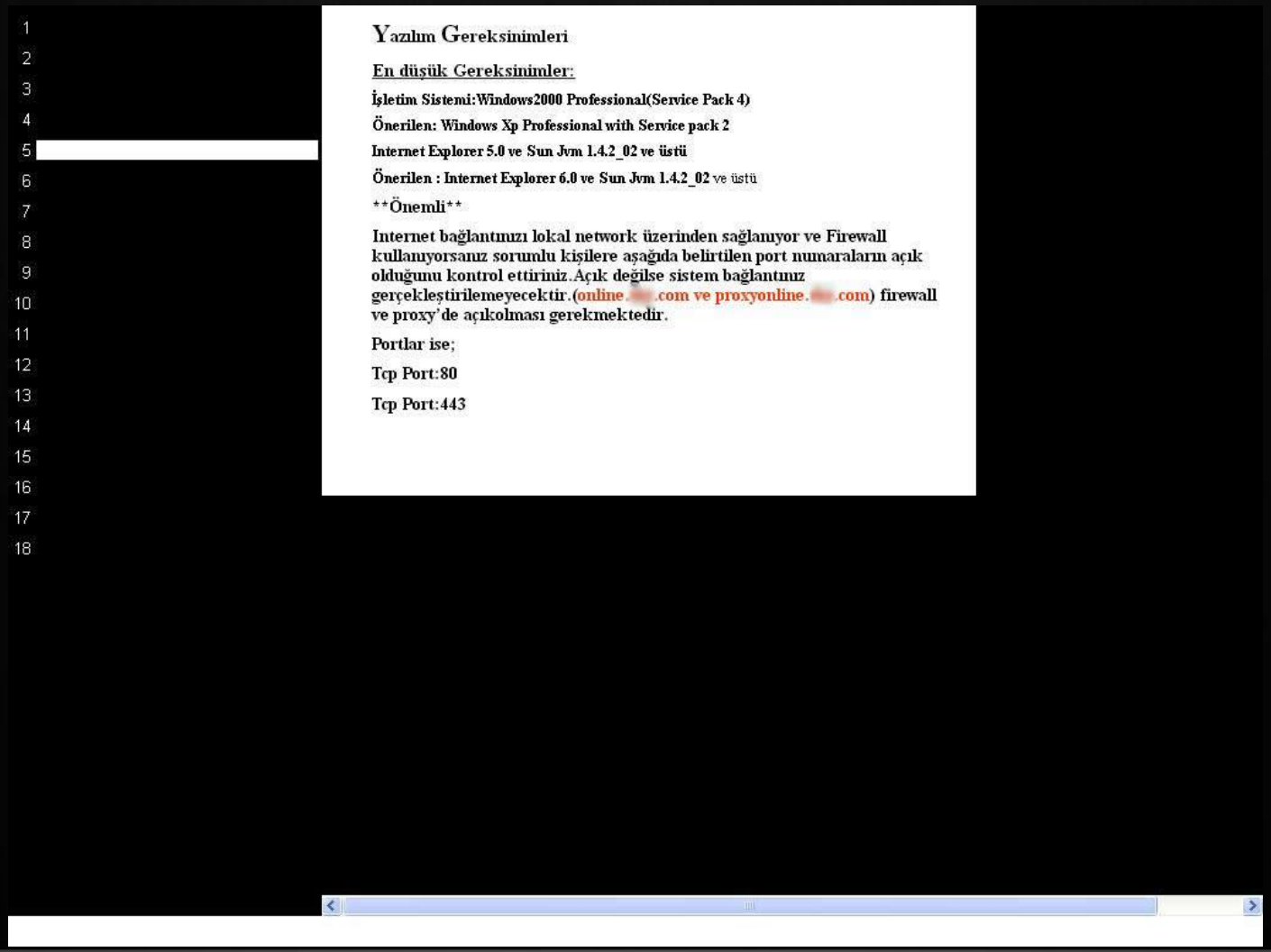
HEDEFLENMİŞ SALDIRI



HEDEFLENMİŞ SALDIRI



HEDEFLENMİŞ SALDIRI

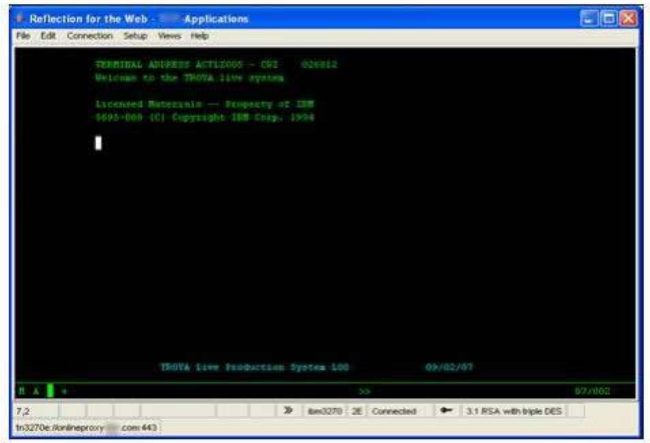


HEDEFLENMİŞ SALDIRI

Adres kısmına http://online.[redacted].com yazıp ;

USERNAME VE ŞİFRENİZİ GIRINIZ VE SUBMIT BUTONUYLA GIRIS YAPINIZ.ILK KURULUM OLACAGI ICIN UYGULAMANIN DOWNLOAD EDILMESI ICIN Bİ SURE BEKLEYINIZ

HEDEFLENMİŞ SALDIRI



Ilk basta karsınıza siyah ekran gelecektir bir sure bekleyiniz bi sure sonra troya ekranı açılacaktır

DÜNYA NE YAPIYOR ?

Twitter hires Apple Hacker Charlie Miller for Security Team

Posted by EHN Reporter on Saturday, September 15, 2012 | 0 comments

+1 0 5 retweet Like 0 Send Submit Share

What is the best way to improve the company's security ? Simple, Hire a Hacker who know how to break the security. He will find the vulnerabilities and help you to fix it. That appears to have been Twitter's reasoning for hiring well-known apple's iPhone hacker Charlie Miller.

In a twitter post , Miller wrote , "Monday I start on the security team at Twitter. Looking forward to working with a great team there!"

Miller, a former National Security Agency(NSA) analyst who works as a researcher with Accuvant, is well known in hacking and Apple circles for his exploits of iPhone and Mac vulnerabilities.

At the end of last year, Miller discovered a bug in Apple's iOS platform, allowing him to execute downloaded code on iPhones, iPads and iPod touch units. At the time, he was due to present at a security conference in Taiwan, but found his membership to the iOS Developer Program revoked and his apps removed from the App Store.

He's also found a way to bypass Google's automated malware scanner(Bouncer) and discovered security flaws in Near-field communication(NFC) features on Samsung and Nokia devices.

Twitter issued a short statement noting that Miller's title will be that of Software Engineer, but declined to discuss any further details.

Follow @BreakTheSec

RECENT POSTS COMMENTS

- Twitter hires Apple Hacker Charlie Miller for Security Team
- CVE-2009-0927 : PDF Exploit targets Aviation Defense Industry
- ADP spam mail leads to BlackHole Exploit kit v2.0
- Blackhole exploit kit v2.0 : Good news for Cyber Criminals,bad news for AV
- Jewish Agency for Israel Site hit by DDoS attack
- Bank of Swiss Hacked by Bangladesh Grey Hat Hackers
- **Anonymous** says:thats scary
- **Anonymous** says:i just had exact same email everything seems to be a scam these days you cant trust no-one.
- **EHN Reporter** says:CVE-2012-4681 has been fixed but other 0-days are still there.
- **Anonymous** says:There is still no patch for this vulnerability...?
- **Anonymous** says:The passwords are in plain text O_O
- **Fernando Fernandez** says:What is Microsoftdoing about this

Become a Fan

Facebook'ta bizi bulun

E Hacking News [EHN]

Beğen

7,648 kişi **E Hacking News [EHN]**'i beğendi.

Mark Sébastien Prasanth Jovana Shah

Ebrahim Sagnik Harpreet Arakan Ash Amr

Facebook sosyal eklentisi

DÜNYA NE YAPIYOR ?

Position Information

Top Message	**Both current Ohio State employees and the general public may apply for this unclassified professional position.**
Identified Candidate Message	
Number of Positions Available	1
University Title	SR Systms Dev/Eng-Sap
Working Title	Sr. Systems Security Analyst
Department	OCIO Security
Department Location	Columbus
Requisition Number	370296
Summary of Duties	The Senior Security Analyst for Information Risk Management will conduct risk and security assessments to test and verify the appropriate security controls are in place and are effective in ensuring the confidentiality, availability and integrity of University systems and data. As part of a Red Team, identify and exploit security control weaknesses through external and internal penetration testing and provide detailed security assessment reports in support of C&A activities. Work directly with IT admin staff in recommending remediation steps and assisting in mitigation. Conduct risk assessments on critical systems to identify threats, vulnerabilities, likelihood and impact and develop risk treatment plans to identify the proper security controls to address risk. Lead and advise on system security designs for new projects and capabilities. Lead improvements to security infrastructure to increase defense in breadth and depth. Drive security initiatives and the tight integration of security requirements into the SDLC. Assist in reviewing and updating University security policy and standards.
Additional Information	
Pre Employment Screening	Requires successful completion of a background check.
Required Qualifications	Bachelor's in Information Systems, Computer Science or equivalent; minimum of six years of experience in IT; strong IT security infrastructure background; strong IT architecture background; minimum of three years of experience in external and internal web, db, application and network penetration testing using such tools as Metasploit, Burp, Backtrack, CANVAS, etc.; experience in conducting risk assessments; knowledge of regulations such as HIPAA, PCI, FERPA, GLBA, etc..
Desired Qualifications	At least one security certification (GPEN, GSEC, CISSP, CISM, CEH); experience in programming; experience with FISMA/NIST or ISO framework; four years or more experience in IT security for network, host, database, application and endpoints.
Target Salary	$91,000 - $99,000 Annually

BİZ NE YAPIYORUZ ?

BİLGİ GÜVENLİĞİ ANALİSTİ / ANALİST YRD.
(Ref:BLG2120)

Genel Nitelikler:
Uluslararası bir finans grubunun [redacted]
[redacted] görevlendirmek üzere;

- Üniversitelerin tercihen Bilgisayar, Elektronik, Matematik v.b lisans diploması veren bölümlerinden mezun,
- Faizsiz bankacılık sektöründe çalışmaya istekli,
- Tercihen CISSP, CEH, LPT ve benzeri güvenlik uzmanlığı sertifikalardan birine sahip,
- Bilgi güvenliği, ISO 27001, COBIT Standartlarının uygulanması konusunda tecrübe sahibi,
- İşletim sistemleri, Network altyapı ve Veritabanı güvenliği konusunda bilgili,
- Problem çözme kabiliyeti yüksek, analitik düşünen, takım çalışmasına yatkın,
- Gelişime açık, sözlü ve yazılı iletişim becerisi yüksek
- Çok iyi derecede İngilizce bilgisine sahip,
- 30 yaşını aşmamış,
- Erkek adaylar için askerliğini tamamlamış ya da en az 2 yıl tecilli,

'Bilgi Güvenliği Analisti / Analist Yrd. ' aranmaktadır.

İş Tanımı:

- DLP, IDM, SIEM, Vulnerability Scanning ürünlerinin yönetilmesi,
- Bilgi Güvenliği risk analiz ve değerlendirmelerini yapmak,
- Sızma ve zafiyet tarama testleri konularında görev almak,
- Bilgi Güvenliği izleme ve denetim fonksiyonunu gerçekleştirmek,
- Bilgi Güvenliği Yönetim Sistemi gereksinimlerini karşılayacak prosedür ve politikaları oluşturmak,
- Yürütülen projelerde güvenlik danışmanlığının sağlanması,

BİZ NE YAPIYORUZ ?

BAŞVUR

IT GÜVENLİK UZMANI
(Ref:ITGVNUZ)

Genel Nitelikler:
Bilgi teknolojileri güvenliği konusunda en az iki yıl tecrübeye sahip,
- Analitik düşünme yetisine sahip,
- Takım çalışmasından keyif alan,
- Esnek çalışma saatlerine uyum sağlayabilecek,
- Yurt içi ve yurt dışı seyahat engeli bulunmayan
- Üniversitelerin Bilgisayar Mühendisliği veya ilgili bölümlerinden mezun,
- Teknik bilgi olarak:
  - İşletim sistemleri (Windows, Linux, UNIX işletim sistemlerinden en az biri),
  - Bilgisayar ağları,
  - Bilişim güvenliği,
  - Bilişim sistemleri hakkında bilgi edinme,
  - Bilişim sistemlerine saldırı yöntemleri,
  - Microsoft Office kullanımı

Konularında yeterli teknik bilgiye sahip olması,

- İyi seviyede İngilizce bilgisine sahip olması,
- Tercihen Certified Ethical Hacker (CEH)
- Askerlikle en az iki yıl ilişkisi olmaması beklenmektedir.

İş Tanımı:
Internet Security Checkup ve Intranet Security Checkup (Penetrasyon testleri) yapmak,
- Bilişim güvenliği projelerine teknik destek sağlamak,
- ISO 27001, PCI-DSS, vb standartlara uyumluluk konusunda destek olmak,
- İlgilendiği iş süreçlerinin gerçekleştirilmesi, geliştirilmesi, yazılı hale getirilmesi ve
- Sorumlu olduğu süreçlerin yönetilmesini sağlamak.

Şehir/Ülke: İstanbul(Avr.) (Bağcılar)
İlan Tarihi: 31.08.2012
Personel Sayısı: 2

Firmanın Diğer İlanları
- Proje Yöneticisi
- MAĞAZA YÖNETİCİ ADAYI - TÜM TÜRKİYE
- SATIŞ DANIŞMANI - BURSA FOMARA
- SATIŞ DANIŞMANI - İSTANBUL MARMARA PARK AVM
- [redacted] Mağazacılık ilanlarını görüntüle

IT Güvenlik Uzmanı ilanları
- Güvenlik Destek Uzmanı
- Güvenlik Destek Uzmanı
- Güvenlik Sistemleri Yöneticisi
- IT SECURITY ENGINEER
- Tüm IT Güvenlik Uzmanı ilanları

İşlemler
- Arkadaşıma gönder
- Bu ilanı yorumla
- Bu ilanı işaretle

İş Arama İşlemleri
- Takibimdeki İlanlar
- İncelediğim İlanlar
- Takibimdeki Firmaların İlanları
- Size Uygun İlanlar

En çok okunan 5 makale

İş başvurularında ön yazı neden gerekli?

Kariyer.net üzerinden yapılan

PENTESTER'IN KATMA DEĞERİ

Hacklenme riskinizi azaltır.

Projelerde güvenlik danışmanlığı yapar.

Güvenlik ürünü seçiminde en doğru kararı vermenizi sağlar.

Bilgisayar olayları müdahalesinde kilit rol oynar.

Süre ve maaliyet kısıtları olmaksızın gerçekleştirdiği testler ile daha fazla zafiyet tespit ederek güvende olmanızı sağlar.

PENTESTER OLMAK İÇİN

Herşeyden önce İngilizce dilini iyi bilmek! (Yerli kaynak sıkıntısı)

Çok çok okumak, bol bol pratik yapmak

Sistem bilgisi (Hack edeceğiniz sistemi iyi bilmeniz gerekir)

Programlama bilmek (Araçlar her zaman işinizi görmeyebilir)

Eğitim Şart

PENTESTER OLMAK İÇİN

Penetrasyon testi haberleşme gerçekleştiren her cihaza yapılabilir.

OSI katmanlarını ve protokollere hakim olmak şart.

Giriş seviyesi için C ve Python (Ruby veya Perl) programlama dili bilmeniz, ileri seviye için ise Assembly bilmeniz şart.

Yaratıcı düşünme şart. (Ben siyah şapka olsaydım ne yapardım ?)

Teknolojiyi yakından takip edin. (Mobile Pentest / NFC vs.)

Sosyal medyayı yakından takip edin. (Twitter)

PENTEST EĞİTİMLERİ

Exploitation -Network Sniffing)

- İş Sürekliliği/Felaket Kurtarma Planlaması Eğitimi

PenTest Eğitimleri (Ethical Hacking/Offensive Security)

Sertifikalı/Lisanslı Pentest Uzmanlığı Eğitimi

Güncel penetration test (sızma testleri) araç ve yöntemlerinin %100 uygulamalı olarak işlendiği eğitimdir. Eğitim, ECSA/LPT ve CPT ile paralel işlenmektedir. **Detaylı bilgi**

Beyaz Şapkalı Hacker(C.E.H) Eğitimi

Beyaz Şapkalı Hacker(Certified Ethical Hacker) yetiştirme amaçlı bir eğitimdir. Diğer CEH tarzı eğitimlerden en önemli farkı Türkçe içerikli ve uygulamalı olmasıdır. **Detaylı bilgi**

Network Pentest Eğitimi

Ağ güvenliğine yönelik güncel saldırı yöntem ve çeşitlerinin uygulamalı olarak işlendiği eğitimdir. **Detaylı bilgi**

Wireless Pentest Eğitimi

Kablosuz ağlara yönelik güncel saldırı çeşit ve yöntemlerinin uygulamalı olarak işlendiği eğitimdir. **Detaylı bilgi**

Web Application Pentest Eğitimi

Web uygulamalarına yönelik güncel saldırı çeşit ve yöntemlerinin uygulamalı olarak işlendiği eğitimdir. **Detaylı bilgi**

Nessus Vulnerability Assessment Eğitimi

Ücretsiz olarak kullanılabilen popüler zayıflık tarama aracı Tenable Nessus'un iş ortamlarında ve güvenlik testlerinde etkin kullanımını amaçlayan bir eğitimdir. **Detaylı bilgi**

Metasploit Framework Eğitimi

Exploit Geliştirme Çatıları arasında popüler olan ve başarılı sızma deneyimleri sonrası sistemlerde ek işlemler yapmak için bir çok araç barındıran metasploit exploit frameworkünün pentest çalışmalarında ve kurumsal ortamlarda etkin kullanımı amaçlı uygulamalı eğitimdir . **Detaylı bilgi**

İleri Seviye Eğitimler (Advanced Security)

Güvenli Yazılım Geliştirme Eğitimi

Daha güvenli ve kontrol edilebilir yazılım geliştirmek için gereken mantığı kavratan ve pratik bilgiyi aktaran eğitimdir. **Detaylı bilgi**

Siber Güvenlik Uzmanı Eğitimi

Bu eğitimle katılımcılar siber dünyanın sınırlarını tanıyarak gerçekleştirilebilecek saldırı tiplerini ve korunma yöntemlerini teorik ve pratik yönleriyle öğreneceklerdir. Eğitim sonunda her bir katılımcı siber dünyadaki suç türlerini, siber savaş, siber suç, siber istihbarat toplama yöntemlerini, siber terorizm ve siber casusluk konularında uzmanlaşacaktır. **Detay bilgi**

İleri Seviye Network Pentest Eğitimi

Beyaz Şapkalı Hacker ve Network pentest eğitimlerinde işlenen konuların hazırlanmış gerçek ortamlarda "Capture The Flag" tarzı senaryolarla işlendiği eğitimdir. Bootcamp tarzında bir eğitim olup %100 uygulamalıdır. ~~Detaylı bilgi~~

Exploit Geliştirme Eğitimi

Sistemlere sızmak için geliştirilen exploitlerin temel mantığını anlatan ve uygulamalı olarak exploit yazılımını gösteren eğitimdir. **Detay bilgi**

Malware Analizi Eğitimi

Internet dünyasının korkulu rüyası Malware(zararlı yazılım)ların çalışma yapısı, alınan önlemler ve bu önlemlerin nasıl

Offensive Security Certified Professional

The Offensive Security Certified Professional (OSCP) is the world's first completely hands on offensive information security certification. The OSCP challenges the students to prove they have a clear practical understanding of the penetration testing process and lifecycle through an arduous twenty four (24) hour certification exam.

The OSCP exam consists of a dedicated vulnerable network, which is designed to be compromised within a 24-hour time period. The exam is entirely hands-on and is completed with the examinee submitting an in-depth penetration test report of the OSCP examination network and PWB labs. The coveted OSCP certification is awarded to students who successfully gain administrative access to systems on the vulnerable network.

> "The truism "anything worth having doesn't come easy" is one I have often remembered when on a particularly difficult path to a goal. Never have the words rung quite so true when applied to my quest for [the] OSCP certification. – ProactiveDefender, http://proactivedefender.blogspot.com/2012/01/oscp-my-review.html"

Real World Exams

The OSCP examination consists of a virtual network containing varying configurations and operating system. The successful examinee will demonstrate their ability to research the network (information gathering), identify any vulnerabilities and execute tools, including modifying exploit code, all with the goal to compromise the systems and gain administrative access. The candidate is expected to submit a comprehensive penetration test report, containing in-depth notes and screen shots detailing their findings. Points are awarded for each compromised host, based on their difficulty and level of access obtained.

Real World Benefits

An OSCP, by definition, is able to identify existing vulnerabilities and execute organized attacks in a controlled and focused manner, write simple bash or python scripts and modify existing exploit code to their advantage, perform network pivoting and data exfiltration, and compromise poorly written PHP web applications. The twenty-four hour examination also demonstrates that OSCP's have a certain degree of persistence and determination. Perhaps more importantly, an OSCP has demonstrated their ability to think "outside the box" and "laterally."

OSCP HOLDERS CAN

- Use information gathering techniques to identify targets.
- Write scripts and tools to aid in penetration testing.
- Analyze, correct, modify and port exploit code.
- Deploy tunneling techniques to bypass firewalls.
- Demonstrate creative problem solving and lateral thinking.

> "The OSCP certification, in my opinion, proves that it's holder is able to identify vulnerabilities, create and modify exploit code, exploit hosts, and successfully preform tasks on the compromised systems over various operating systems. – Trenton, http://www.hackyeah.com/2010/12/brief-review-of-the-pwb-class-and-the-oscp-certification/"

PENTEST EĞİTİMLERİ

Security

Course	Price	Options †	Free Demo
SEC401: Security Essentials Bootcamp Style	$4,175	GSEC $549	SEC401 Demo
SEC504: Hacker Techniques, Exploits & Incident Handling	$4,175	GCIH $549	SEC504 Demo
SEC560: Network Penetration Testing and Ethical Hacking	$4,365	GPEN $549	SEC560 Demo
SEC542: Web App Penetration Testing and Ethical Hacking	$4,175	GWAPT $549	SEC542 Demo
SEC503: Intrusion Detection In-Depth	$4,175	GCIA $549	SEC503 Demo
SEC660: Advanced Penetration Testing, Exploits, and Ethical Hacking	$4,365	GXPN $549	SEC660 Demo
SEC505: Securing Windows	$4,175	GCWN $549	SEC505 Demo
SEC566: Implementing and Auditing the Twenty Critical Security Controls - In-Depth	$3,750	—	SEC566 Demo
SEC617: Wireless Ethical Hacking, Penetration Testing, and Defenses	$4,175	GAWN $549	SEC617 Demo
SEC301: Intro to Information Security	$3,750	GISF $549	SEC301 Demo

Home
Courses & Prices
Specials
Bundles
About
Student Info
FAQ

What Students Say

I love the fact that you can do these courses online whenever you want.
Phil Hardcastle, Centra Software

Additional

- OnDemand System Requirements

OKUNASI KİTAPLAR

Hacking Exposed serileri

Hackers Handbook serileri

Linked'in hesabımda okuduğum kitaplar.

SONUÇ

Yedekten dönemeyeceğiniz tek bir şey vardır o da itibarınız.

Bilgi güçtür ve Pastebin'e asıldıkça azalır ☺

Hacklenmediğiniz için rehavete kapılmayın çünkü henüz sıra size gelmemiş olabilir, önleminizi şimdiden alın.

Yetişmiş Pentester bulamıyorsanız yetiştirmeye bakın.

Pentesterınıza mutlaka yatırım yapın o sıradan bir iş yapmıyor.

No news is s/good news/APT/g


SORULAR?

TEŞEKKÜRLER