



BEYAZ ŞAPKALI HACKER EĞİTİMİ (C.E.H)

EĞİTİM SÜRESİ

Beş (5) Gün

NELER KATACAK?

Eğitim sonrası her bir katılımcı hacking amaçlı kullanılan yöntem ve araçların ne amaçla nasıl kullanıldığını öğrenerek güvenlik konusunda daha bilinçli yaklaşacaktır.

İŞLEYİŞ VE EĞİTİM NOTLARI

Eğitim boyunca öğrenilen konular her hafta yapılacak Online CTF Hacking yarışmalarıyla pekiştirilecek ve katılımcılar her ay güncellenen Türkçe eğitim notlarından faydalanabileceklerdir.

Beyaz Şapkalı Hacker eğitimi hackerların sistemlere sızmada kullandığı yöntemleri ve araçları detaylı ve uygulamalı bir şekilde anlatılarak proaktif güvenlik anlayışı kazandırma amaçlı bir eğitimidir. Benzeri eğitimlerden farkı eğitim içeriğinde gerçek dünyaya uygun uygulamaların kullanılması ve pratiğe önem verilmesidir. Beyaz şapkalı hacker eğitimi **Ec-Council Certified Ethical Hacker v6 ile uyumludur.**

KİMLER KATILMALI?:

Bilgi güvenliği departmanı çalışanları, IT denetim birimi çalışanları, sistem ve ağ yöneticileri, hacking ve güvenlik konusuna meraklılar.

ÖN GEREKSİNİMLER:

Ağ ve güvenlik yöneticileri için Linux, Uygulamalı TCP/IP ve Ağ Güvenliği eğitimleri ya da eşdeğer seviyede bilgi/tecrübe.

EĞİTİM İÇERİĞİ:

Linux sistem yönetimi ve güvenliği

1. Linux işletim sistemi ve Linux dağıtımları
 - 1.1. Backtrack Linux dağıtımı ve temel bileşenleri
 - 1.2. Paket yönetimi, sistem ayarları
2. Linux dosya sistemi
 - 2.1. Güvenlik açısından önemli dosya ve dizinler
3. Temel sistem yönetimi komutları
4. Kullanıcı yönetimi ve parola güvenliği
5. Dosya, izin erişim güvenliği
6. Sistem güvenliğini ilgilendiren komutlar
7. Güvenlik açısından loglama
 - 7.1. Kullanıcı denetim logları(auditd)
8. Su/sudo kullanımı
9. Gereksiz servislerin kapatılması ve Linux sistemlerin sıkılaştırılması

TCP/IP Protokol Ailesi Zafiyet Analizi

1. Temel TCP/IP Protokolleri Analizi
2. TCP/IP kaynaklı Açıklıklar
3. IP ve ARP protokolleri zayıflık incelemesi
4. Ip parçalanması ve kötüye kullanımı
5. ICMP 'nin kötü amaçlı kullanımı

BEYAZ ŞAPKALI HACKER EĞİTİMİ (C.E.H)

EĞİTİM SÜRESİ

Beş (5) Gün

NELER KATACAK?

Eğitim sonrası her bir katılımcı hacking amaçlı kullanılan yöntem ve araçların ne amaçla nasıl kullanıldığını öğrenerek güvenlik konusunda daha bilinçli yaklaşacaktır.

İŞLEYİŞ VE EĞİTİM NOTLARI

Eğitim boyunca öğrenilen konular her hafta yapılacak Online CTF Hacking yarışmalarıyla pekiştirilecek ve katılımcılar her ay güncellenen Türkçe eğitim notlarından faydalanabileceklerdir.

6. TCP ve UDP Zayıflık İncelemesi

6.1. TCP/UDP'ye dayalı saldırı yöntemleri

7. DNS Protokolü Zafiyetleri

7.1. Dns cache snooping

7.2. Dns cache poisoning

8. DHCP Protokolü zafiyetleri

9. Http/HTTPS protokolü zafiyetleri

Paket Analizi, Sniffing

1. TCP/IP Paket Yapısı ve Analizi

2. Sniffing Kavramı

3. Sniffing için protokoller

4. Sniffing Çeşitleri

4.1. Aktif Modda Sniffing

4.2. Pasif Modda Sniffing

5. Paket analizi ve sniffing için kullanılan araçlar

5.1. Wireshark, tcpdump, tshark, snop, snort, dsniff, urlsnarf, mailsnarf, sshmitm

6. Wireshark & tcpdump ile paket analizleri

6.1. Kaydedilmiş örnek paket incelemeleri

6.2. Bağlantı problemi olan ağ trafiği analizi

6.3. DNS & DHCP Trafiği Paket Analizi

7. Ağ Trafiğinde adli bilişim analizi çalışmaları

7.1. Ngrep ile ağ trafiğinde sızma tespiti

7.2. İkili verilerden(pcap formatında) orijinal verileri elde etme

7.3. Network miner, Netwitness araçlarıyla ağ trafiği analizi

8. Yerel Ağlarda Snifferleri Belirleme ve Engelleme

Güvenlik Testlerinde Bilgi Toplama

1. Bilgi toplama çeşitleri

1.1. Aktif bilgi toplama

1.2. Pasif bilgi toplama

2. İnternete açık servisler üzerinden Bilgi Toplama

2.1. DNS Aracılığı ile

2.2. HTTP Aracılığı ile

2.3. SMTP üzerinden bilgi toplama

2.4. SNMP aracılığıyla bilgi toplama

3. Arama motorlarını kullanarak bilgi toplama

3.1. Bir şirkete ait e-posta bilgilerinin bulunması

3.2. Bir şirkete ait alt domain isimlerinin bulunması

4. Google Hacking yöntemleri ve hazır araçlar

5. İnternete açık web sayfaları, e-posta listelerinden bilgi toplama

6. Yeni nesil bilgi toplama aracı Maltego

BEYAZ ŞAPKALI HACKER EĞİTİMİ (C.E.H)

EĞİTİM SÜRESİ

Beş (5) Gün

NELER KATACAK?

Eğitim sonrası her bir katılımcı hacking amaçlı kullanılan yöntem ve araçların ne amaçla nasıl kullanıldığını öğrenerek güvenlik konusunda daha bilinçli yaklaşacaktır.

İŞLEYİŞ VE EĞİTİM NOTLARI

Eğitim boyunca öğrenilen konular her hafta yapılacak Online CTF Hacking yarışmalarıyla pekiştirilecek ve katılımcılar her ay güncellenen Türkçe eğitim notlarından faydalanabileceklerdir.

TCP/IP İletişiminde Oturuma Müdahale

1. TCP/IP Ağlarda Araya girme ve oturuma müdahale
2. Çeşitli oturum müdahale yöntemleri
 - 2.1. ARP Spoofing
 - 2.2. IP Spoofing
 - 2.3. DNS Spoofing
 - 2.4. MAC Flooding
 - 2.5. Sahte DHCP Sunucuları ile bağlantı yönlendirme
 - 2.6. ICMP redirect paketleriyle oturuma müdahale
3. Oturum Müdahale Araçları
 - 3.1. Ettercap, Dsniff, Cain & Abel
 - 3.2. Oturum Müdahale Örnekleri
 - 3.2.1. Telnet oturumuna müdahale
 - 3.2.2. http oturumuna müdahale
 - 3.2.3. SSL oturumunda araya girme
 - 3.2.4. SSH bağlantılarında araya girme

Yönlendirici(Router) Güvenliği

1. Routing protokolleri güvenlik analizi
2. Cisco Routerlarda Güvenlik açıkları
3. Cisco spesifik protokollerin analizi
4. Cisco IOS Parola güvenliği ve parola kırma saldırıları
5. DOS saldırıları ve Router üzerinde korunma yöntemleri
6. ACL yazımında dikkat edilecek hususlar
7. Linux/BSD Sistemleri Router olarak kullanmak
8. Nipper kullanarak router konfigürasyonları üzerinde denetim

9. CIS kuralları ile router konfigürasyonlarında denetim.

Güvenlik Duvarları(Firewall)

1. Güvenlik Duvarı Temelleri
 - 1.1. Firewall(güvenlik duvarı) nedir, ne değildir?
 - 1.2. Paketlere hangi seviyeye kadar müdahale edebilirler
 - 1.3. Nat Kavramı
 - 1.4. NAT, Çeşitleri ve Uygulama alanları
2. Packet Filtering
 - 2.1. Stateful packet filtering
 - 2.2. Stateless Packet Filtering
3. Authentication(Yetkilendirme)
4. Firewall Çeşitleri
 - 4.1. Uygulama seviyesi
 - 4.2. Bridge mode firewall
 - 4.3. Kişisel güvenlik duvarları
 - 4.4. Donanımsal/yazılımsal güvenlik duvarları
 - 4.5. Proxy mod güvenlik duvarı
5. Firewall ürünleri
 - 5.1. Açık kaynak kodlu
 - 5.1.1. Linux iptables
 - 5.1.2. OpenBSD Packet Filter
 - 5.1.3. Pfsense

BEYAZ ŞAPKALI HACKER EĞİTİMİ (C.E.H)

EĞİTİM SÜRESİ

Beş (5) Gün

NELER KATACAK?

Eğitim sonrası her bir katılımcı hacking amaçlı kullanılan yöntem ve araçların ne amaçla nasıl kullanıldığını öğrenerek güvenlik konusunda daha bilinçli yaklaşacaktır.

İŞLEYİŞ VE EĞİTİM NOTLARI

Eğitim boyunca öğrenilen konular her hafta yapılacak Online CTF Hacking yarışmalarıyla pekiştirilecek ve katılımcılar her ay güncellenen Türkçe eğitim notlarından faydalanabileceklerdir.

- 5.2. Linux Iptables ile güvenlik duvarı uygulamaları
 - 5.2.1. İptables çalışma mantığı
 - 5.2.2. Port açma, port kapama
 - 5.2.3. Belirli ip adreslerine belirli servisler için erişim izni verme
 - 5.2.4. L7 filter ile uygulama seviyesi güvenlik duvarı kullanımı
 - 5.2.5. Etables ile L2 seviyesi güvenlik duvarı kullanımı
- 5.3. Ticari güvenlik duvarı ürünleri
 - 5.3.1. Checkpoint, Netscreen, Fortinet, Kerio, Cisco ASA
- 5.4. Firewall Testleri
 - 5.4.1. Antispoof testi
 - 5.4.2. Parçalanmış paketleri geçirme testleri
 - 5.4.3. Dayanıklılık testleri
 - 5.4.4. Isic, hping, Nmap ile test çalışmaları
- 5.5. Firewall kural testleri
 - 5.5.1. Ftester, hping, firewallk ile test çalışmaları
6. IDS/IPS Yerleşim Planlaması
7. Açık Kaynak kodlu IDS/IPS Yazılımları
 - 7.1. Snort, Brologs, Suricata
8. Snort Saldırı Tespit ve Engelleme Sistemi
 - 8.1. Snort IDS Kurulumu
 - 8.2. Snort'u (N)IDS Olarak yapılandırma
 - 8.3. Snort kurallarını anlama ve yorumlama
 - 8.4. Snort'a saldırı kuralı yazma
 - 8.5. Saldırı loglarını inceleme ve yorumlama
 - 8.6. Snort'u IPS olarak Kullanma
 - 8.7. Snort yönetim araçları
9. Tuzak (HoneyPot) Sistemler
 - 9.1. Kfsensor ile honeypot uygulaması
 - 9.2. Honeyd ile honeypot çalışmaları

Firewall, IDS/IPS ve İçerik Filtreleme Sistemlerini Atlatma

Saldırı Tespit ve Engelleme Sistemleri

1. IDS, IPS, NIDS, NIPS, HIPS Tanımları
2. IDS/IPS(SALDIRI TESPİT VE ENGELLEME) Teknolojileri
3. Host tabanlı IDS/IPS Sistemleri
 - 3.1. Ossec Kullanımı
4. Ağ Tabanlı IDS/IPS Sistemleri
5. Ağ tabanlı IDS'lerin çalışma yöntemleri
1. Firewall atlatma teknikleri
 - 1.1. Mac spoofing Yöntemi ile
 - 1.2. IP Spoofing Yöntemi ile
 - 1.3. Tersine kanal açma yöntemi
 - 1.4. Protokol Tünelleme Yöntemleri
 - 1.5. SSh Tünelleme
 - 1.6. VPN Tünelleri
2. IPS/IDS atlatma teknikleri
 - 2.1. Şifreli bağlantılar ve IPS Sistemler

BEYAZ ŞAPKALI HACKER EĞİTİMİ (C.E.H)

EĞİTİM SÜRESİ

Beş (5) Gün

NELER KATACAK?

Eğitim sonrası her bir katılımcı hacking amaçlı kullanılan yöntem ve araçların ne amaçla nasıl kullanıldığını öğrenerek güvenlik konusunda daha bilinçli yaklaşacaktır.

İŞLEYİŞ VE EĞİTİM NOTLARI

Eğitim boyunca öğrenilen konular her hafta yapılacak Online CTF Hacking yarışmalarıyla pekiştirilecek ve katılımcılar her ay güncellenen Türkçe eğitim notlarından faydalanabileceklerdir.

- 2.2. Şifreli bağlantılar üzerinden atlatma testleri
 - 2.2.1.SSH tünelleme
 - 2.2.2.Opelssl
 - 2.2.3.Nssl
 - 2.2.4.HTTPS/SSL VPN kullanımı
 - 2.3. Parçalanmış paketlerle IDS atlatma
 - 2.4. Tuzak sistemler aracılığı ile port tarama
 - 2.5. Proxy sistemler üzerinden port tarama
 3. İçerik filtreleme atlatma teknikleri
 - 3.1. HTTPS bağlantıları üzerinden atlatma
 - 3.2. Google & Yahoo araçlarını kullanarak atlatma teknikleri
 - 3.3. Proxy kullanarak içerik filtreleyicileri atlatma
 - 3.3.1.Cgi-Proxy(http/https)
 - 3.3.2.SSH Socks Proxy
 - 3.3.3.Açık Proxyler kullanılarak atlatma
 - 3.4. Protokol Tünelleme Yöntemleri
 - 3.4.1.Tek port, protokol açıksa tüm portlar açıktır ilkesi
 - 3.4.2.Mail Trafiği üzerinden HTTP Trafiği aktarımı
 - 3.4.3.DNS protokolü üzerinden tüm trafiğin aktarımı
 - 3.4.4.SSH Protokolü üzerinden tüm trafiğin aktarımı
 - 3.4.5.AntiSansür yazılımları aracılığı ile atlatma teknikleri
 - 3.4.6.TOR & Ultrasurf
 - 3.5. Atlatma Yöntemlerine karşı korunma Yolları
- ### Host/Ağ/Port Keşif Ve Tarama Araçları
1. Host keşfetme ve Port Tarama
 2. Host/Port Açıklık Kavramları
 - 2.1. Bir host/port hangi durumda açık gözükür, hangi durumda kapalı
 3. Host/Port Tarama Neden Önemlidir?
 4. Tarama Çeşitleri
 - 4.1.1.TCP üzerinden port tarama
 - 4.1.1.1. SYN Tarama, FIN Tarama, XMAS , ACK, NULL ...
 - 4.1.2.UDP Port tarama
 - 4.1.3.IP ve ICMP Tarama
 5. İşletim Sistemi Belirleme ve versiyon belirleme
 6. Port Tarama Araçları
 - 6.1.1.Hping ile Port tarama uygulamaları
 - 6.1.2.Nmap ile Port tarama uygulamaları
 7. Nmap ile gelişmiş port tarama yöntemleri
 8. Nmap Scripting Engine(NSE) Kullanımı
 9. Diğer bilinen port tarama araçları
 - 9.1.1.Unicornscan
 - 9.1.2.Scanrand
 - 9.1.3.Xprobe
 10. Saldırı Tespit Sistemleri Port taramalarını nasıl algılar ve engeller

BEYAZ ŞAPKALI HACKER EĞİTİMİ (C.E.H)

EĞİTİM SÜRESİ

Beş (5) Gün

NELER KATACAK?

Eğitim sonrası her bir katılımcı hacking amaçlı kullanılan yöntem ve araçların ne amaçla nasıl kullanıldığını öğrenerek güvenlik konusunda daha bilinçli yaklaşacaktır.

İŞLEYİŞ VE EĞİTİM NOTLARI

Eğitim boyunca öğrenilen konular her hafta yapılacak Online CTF Hacking yarışmalarıyla pekiştirilecek ve katılımcılar her ay güncellenen Türkçe eğitim notlarından faydalanabileceklerdir.

Zaafiyet Tarama ve Bulma Sistemleri

1. Zaafiyet tanımı ve çeşitleri
2. Çeşitli ticari zaafiyet tarama araçları
 - 2.1. Qualys, McAfee Foundstone, Nexpose, EyeEye Retina
3. Açık kaynak kodlu zaafiyet tarama araçları
 - 3.1. Nessus, Inguma, W3af ..
4. Nessus ile otomatize güvenlik açığı keşfi
 - 4.1. Nessus çalışma mantığı
5. Nessus pluginleri
6. Knowledge Base mantığı
7. Nessus tarama yapısı
 - 7.1. Yerel sistem üzerinden tarama
 - 7.2. Ağ üzerinden tarama
8. Nessus ile güvenlik açığı bulma
9. Nessus tarama raporları

Exploit Çeşitleri ve Metasploit Kullanımı

1. Exploit Geliştirme ve Çalıştırma Araçları
 - 1.1. Core Impact, Canvas, Metasploit
2. Metasploit Geliştirme Süreci
 - 2.1. Metasploit Versiyonları
 - 2.2. Güncel sürüm özellikleri
 - 2.3. Yol Haritası
 - 2.4. Metasploit kullanımı ile ilgili genel terim ve tanımlar
3. Temel Metasploit kullanımı
 - 3.1. Kurulum
 - 3.2. Çalışma yapısı
 - 3.3. Bileşenleri

- 3.4. Metasploit yönetim arabirimleri

DOS/DDOS Saldırıları ve Korunma Yöntemleri

1. Denial Of Service Atakları
 - 1.1. Çeşitleri
 - 1.2. Amaçları
 - 1.3. DOS Atak Çeşitleri
 - 1.3.1. Smurf, Ping Of Death, TearDrop, SYN Flood, UDP Flood
2. DDOS Atakları
3. DDOS Çeşitleri ve Araçları
 - 3.1. SYN Flood, UDP Flood, icmp flood, smurf, fraggle, http flood
4. DDOS amaçlı kullanılan WORMlar.
5. Ircbot, zombie, BotNet Kavramları
6. Botnet kullanım alanları
7. Fast-Flux networkler ve çalışma yapıları
8. DNS sunuculara yönelik DDOS saldırıları
9. Kablosuz Ağlara yapılan DOS saldırıları
10. DOS/DDOS Saldırılarından Korunma Yolları
 - 10.1. Syn cookie, syn proxy, syn cache yöntemleri

Kablosuz Ağlar Ve Güvenlik

1. Kablosuz Ağlara Giriş
 - 1.1. Tanımlar
 - 1.2. Kablosuz Ağ Çeşitleri
 - 1.3. Kablosuz Ağ Standartları
 - 1.4. Linux/Windows işletim sistemi ile kablosuz ağ kullanımı

BEYAZ ŞAPKALI HACKER EĞİTİMİ (C.E.H)

EĞİTİM SÜRESİ

Beş (5) Gün

NELER KATACAK?

Eğitim sonrası her bir katılımcı hacking amaçlı kullanılan yöntem ve araçların ne amaçla nasıl kullanıldığını öğrenerek güvenlik konusunda daha bilinçli yaklaşacaktır.

İŞLEYİŞ VE EĞİTİM NOTLARI

Eğitim boyunca öğrenilen konular her hafta yapılacak Online CTF Hacking yarışmalarıyla pekiştirilecek ve katılımcılar her ay güncellenen Türkçe eğitim notlarından faydalanabileceklerdir.

2. Kablosuz Ağlarda Tehlikeler
3. Sahte Access Pointler ve Zararları
4. WLAN keşif yöntemleri
 - 4.1. Aktif Keşif yöntemleri
 - 4.2. Pasif Keşif yöntemleri
5. Pasif mod Trafik Analizi
6. WLAN'lerde Temel Güvenlik
 - 6.1. SSID Gizleme
 - 6.2. MAC Adres Filtreleme
 - 6.3. WEP Şifreleme
7. Aircrack-ng test araçları ailesi
8. Kablosuz Ağlarda Denial Of service atakları
9. WEP/WPA/WPA-II Güvenliği
 - 9.1. WEP/WPA/WPA-II Analizi
 - 9.2. Temel XOR Bilgisi
 - 9.3. WEP'in kırılması
 - 9.4. WPA güvenliği
10. Halka Açık kablosuz ağlarda Tehlikeler
 - 10.1. Wifizoo ile erişim bilgilerinin kötüye kullanımı
 - 10.2. Karmasploit ile aktif kullanıcılara saldırı
11. Kablosuz Ağlarda Saldırı Tespit Sistemi Kullanımı

Web Uygulama Güvenliği ve Hacking Yöntemleri

1. Web Uygulamaları ve http
 - 1.1. http protokol detayları
 - 1.2. Web uygulama bileşenleri
2. Geleneksel güvenlik anlayışı ve web uygulama güvenliği
3. Web uygulama güvenliğinde kavramlar
 - 3.1. Hacking, Defacement, Rooting, shell vs
4. Web uygulama/site güvenliği nelere bağlıdır?
5. Web uygulamalarında hacking amaçlı bilgi toplama
 - 5.1. Web sunucu, uygulama versiyon keşfi
 - 5.2. Hata mesajlarından bilgi toplama
 - 5.3. Google kullanarak bilgi toplama
 - 5.4. Alt dizin, dosya keşfi
 - 5.5. Admin panel keşfi
6. Web güvenlik testlerinde kişisel Proxyler
 - 6.1. Paros Proxy, WEbScarab, Burp Proxy
 - 6.2. Firefox eklentileri
7. İstemci tarafı kontrolleri aşma
8. OWASP Top 10 açıklık rehberi
9. XSS, CSRF açıklıkları ve kötüye değerlendirme
 - 9.1. XSS ,CSRF nedir, ne değildir?
 - 9.2. XSS, CSRF ne amaçla kullanılır?
 - 9.3. Çeşitleri nelerdir ve nasıl engellenebilir
10. SQL Injection zafiyetleri ve hacking amaçlı kullanımları
 - 10.1. Dinamik web uygulamaları ve SQL
 - 10.2. SQLi neden kaynaklanır, çeşitleri nelerdir?

BEYAZ ŞAPKALI HACKER EĞİTİMİ (C.E.H)

EĞİTİM SÜRESİ

Beş (5) Gün

NELER KATACAK?

Eğitim sonrası her bir katılımcı hacking amaçlı kullanılan yöntem ve araçların ne amaçla nasıl kullanıldığını öğrenerek güvenlik konusunda daha bilinçli yaklaşacaktır.

İŞLEYİŞ VE EĞİTİM NOTLARI

Eğitim boyunca öğrenilen konular her hafta yapılacak Online CTF Hacking yarışmalarıyla pekiştirilecek ve katılımcılar her ay güncellenen Türkçe eğitim notlarından faydalanabileceklerdir.

- 10.3. SQLi örnekleri
- 10.4. Google'dan otomatik SQLi açıklığı arama
- 10.5. SQLi araçları ve kullanımı
 - 10.5.1. Sqlimap, SQLi Finder, Pangolin
11. File inclusion zafiyetleri ve hacking amaçlı kullanımı
 - 11.1. File inclusion çeşitleri
 - 11.1.1. Local File inclusion
 - 11.1.2. Remote file inclusion
12. Shell Çeşitleri ve kullanım amaçları
 - 12.1. Shell kavramı ve kullanımı
 - 12.2. PHP, ASP ve JSP shell çeşitleri
 - 12.3. Sık kullanılan shell yazılımları
13. Web sunucularına yönelik DOS saldırıları
14. Web uygulama güvenlik duvarı yazılımları ve çalışma yöntemleri
15. Web uygulama güvenlik test yazılımları ve örnek sayfalar
16. Http authentication yöntemleri ve karşı saldırılar
 - 3.2. TNS Listener güvenliği
4. Mysql güvenlik açıklıkları
 - 4.1. Ağ üzerinden açıklık tespiti
 - 4.2. Mysql sorgularını sniffleme, mysqlsniffer
 - 4.3. Mysql tehlikeli fonksiyonları
 - 4.4. MySqliot kullanımı
5. MSSQL güvenlik açıklık tespiti
 - 5.1. MSSQL ağ üzerinden açıklık tespiti
 - 5.2. MSSQL ile birlikte gelen tehlikeli fonksiyonlar
 - 5.3. MSSQL fonksiyonlarını kullanarak işletim sistemi ele geçirme
 - 5.4. Osqli kullanarak uzaktan sorgu
6. Veritabanı üzerinde denetim işlemleri
 - 6.1. Nessus veritabanı denetim eklentileri
7. Veritabanı güvenlik test yazılımları
 - 7.1. Nessus, Metasploit, Typhon
8. Veritabanı parola güvenliği
 - 8.1. Veritabanı sistemlerin kullandığı şifreleme algoritmaları
 - 8.2. Veritabanı yazılımlarının kullandığı öntanımlı kullanıcı ve parolalar
 - 8.3. Parola kırma yöntem ve araçları
9. Veritabanı güvenlik yazılımları
 - 9.1. GreenSQL, Imperva, Guardium

Veritabanı Sistemlerine Yönelik

Saldırıları

1. Bilinen veritabanı sistemleri
 - 1.1. Mysql, MSSQL, Oracle, Postgresql, Sqlite
2. Veritabanlarını hedef almış güvelik açıklıkları ve exploitler
3. Oracle güvenlik açıklıkları
 - 3.1. Ağ üzerinden açıklık tespiti

VPN ve Şifreleme Teknolojileri

1. Şifreleme algoritmaları
2. Şifreleme algoritmalarına yönelik saldırılar

BEYAZ ŞAPKALI HACKER EĞİTİMİ (C.E.H)

EĞİTİM SÜRESİ

Beş (5) Gün

NELER KATACAK?

Eğitim sonrası her bir katılımcı hacking amaçlı kullanılan yöntem ve araçların ne amaçla nasıl kullanıldığını öğrenerek güvenlik konusunda daha bilinçli yaklaşacaktır.

İŞLEYİŞ VE EĞİTİM NOTLARI

Eğitim boyunca öğrenilen konular her hafta yapılacak Online CTF Hacking yarışmalarıyla pekiştirilecek ve katılımcılar her ay güncellenen Türkçe eğitim notlarından faydalanabileceklerdir.

3. Parola ve şifre kavramı neden artış var?
4. Şifreleme ve kodlama farklılıkları 4. Son kullanıcıya yönelik saldırı çeşitleri
5. Parola çeşitleri 4.1. Phishing
6. Şifreleme saldırıları 4.2. USB disklerdeki güvenlik problemi
7. Brute force ataklar, rainbow table kullanımı, hibrid ataklar
8. Linux, Windows, Cisco sistemlerin parola güvenliği
9. Parolaların hashlenmesi ve salt değeri kullanımı
10. Parola kırma araçları
11. Sayısal Sertifikalar
12. Disk Şifreleme
13. SSL Protokolü inceleme
- 13.1. SSL Protokol yapısı
- 13.2. SSL TLS farkları
14. SSL Protokolünde araya girme ve veri okuma
15. VPN Teknolojileri ve Çalışma yöntemleri
16. OpenVPN ile SSL VPN Uygulamaları
17. SSH Protokolü
18. SSH ile Tünelleme
19. SSL VPN uygulamalarında araya girme

Güvenlik Amaçlı Kullanılan Firefox Eklentileri

1. User Agent Switcher
2. Tamper Data eklentisi
3. HTTP Live Headers
4. HackBar Eklentisi
5. FoxyProxy Eklentisi
6. Fire Encrypter
7. TrashMail.net Eklentisi
8. Xss-Me/SqlInject-Me eklentileri
9. Passive Recon Eklentisi
10. ProxySel Eklentisi
11. Firebug Eklentisi
12. User Agent Switcher
13. Firecat Framework

Son Kullacıya Yönelik Saldırı Çeşitleri ve Yöntemleri

1. Son kullanıcı tanımı
2. Sunuculara yönelik saldırılar & istemcilere yönelik saldırılar
3. Son kullanıcıya yönelik saldırılarda