Reverse Engineering Bootcamp Eğitim İçeriği

1. Reverse Engineering

- Reverse Code Engineering
- Dökümantasyonu Olmayan Bileşenler (Undocumented Functions)
- Yazılım Mimarisinin Anlaşılması
- Kapalı Kaynak Kod
- Hata Ayıklama
- Yama Analizi
- Dijital Adli Analiz

*Reverse Engineer Toolbag

- PE Explorer
- Sysinternals Suite
- Process Explorer, Strings, TCPView
- Debuggers (WinDBG, OllyDbg)
- Disassembler (IDA)

*Reverse Engineering Teknikleri

- Static Analiz
- Dinamik Analiz

*Reverse Engineering ve Zorlukları

- Anti-Debug
- EntryPoint Obfuscation, Packers
- Anti-Virtualization

* x86 Mimarisi ve Assembly

- İşlemci Mimarisi
- Yazmaçlar (Registers)
- Bellek Yönetimi
- Real Mode (Gerçek Mod)
- Flat Memory (Düz Bellek)
- Dinamik Erişim
- 16 Bit Registers & 32 Bit Registers
- Fonksiyon Çağrıları (Near & Far)

** IA32 Komut Seti*

- IA32 Veri Taşıma Komutları
- IA32 Yığın Komutları (Stack Instructions)
- IA32 Aritmetik İşlemler
- IA32 Mantıksal Komutlar (Logical)
- IA32 Çevirme ve Döndürme Komutları
- IA32 Bit İşlemleri
- IA32 Şart ve Dallanma Komutları
- IA32 Döngü İfadeleri
- IA32 Alt Programlar (Subroutines)
- IA32 Katar (string) Komutları
- IA32 Segment Komutları
- IA32 Diğer Komutları
- IA32 Şart Ekleri Tablosu

** Windows Uygulama Programlama Arabirimi (WinAPI)*

- Data Storage (Veri Saklama)
- Indirection Dereferencing
- Pointers
- Structures
- Windows API ve Kullanımı
- Virtual Address Structure
- Loaders (Yükleyici)

** Çalıştırılabilir Dosya Formatları*

-Executable & Linkable (ELF)
- ELF Başlıklar (Headers)
- ELF Bölümler (Sections)
- Portable Executable (PE)
- PE Başlıklar (Headers)
- PE Bölümler (Sections)

2. Malware / Zararlı Yazılım Analizi

**Malware Kategorizasyonu*

- Exploit,
- Virus,
- RAT,
- Backdoor
- Rootkit
- Worm

*Malware Platformları

- Windows
- Linux
- Android
- WinCE

*Atak Vektörleri

- Exploitler
- File Infectors
- USB, Bluetooth, Emails, Web
- Boot Sector / MBR

*Malware Kod Türleri

- Hybrid
- Polymorphism
- Metamorphism
- Stealth
- Memory based activity

*Enfeksiyon Belirtileri

-Enfeksiyon Tespiti ve Zararlı Yazılımın Örneklenmesi
- Windows Registry
- Registry Rootkeys
- MSCONFIG
- Services (Servisler)
- Network Trafigi
- WireShark
- NetStat
- TcpView
- Hosts Dosyası
- Dosya Sistemi
- Kullanıcı Hesapları
- Olay Kayıtları (Event Log)

* Malware Analiz Ortamı (Lab Setup)

- Sanal ortamın kurulması
- Tersine mühendislik araçlarının kurulması

*Windows Zararlı Kod Analizi

- Statik Analiz Uygulaması
- Dinamik Analiz Uygulaması
- Otomatize Analiz
- Manual ve Otomatize Unpacking
- Rootkit Analizi
- Client-side Malware Analiz
- Browser Exploit Analizi
- Malformed Domain Listesi
- Office Malware Analizi
- Encrypted Shellcode
- Decrypting Shellcode

*Linux Zararlı Kod Analizi

- Mitler
- Gerçekler
- Gereksinimler
- Implementasyon
- Rootkit
- Worm
- Analiz Ortamı
- Statik Analiz Araçları
- Programlama Arabirimleri
- Dinamik Analiz Araçları
- TCPDump
- GDB
- Linux Malware: Uygulama (“gdb”)
- Linux Payload: Uygulama Shellcode Analiz (“Radare”)
- Linux Payload: Uygulama Shellcode Analiz (“objdump”)

*Zararlı Yazılım İmzası Oluşturma

- ClamAV Anti-Virüs
- ClamAV İmza Formatları
- ClamAV için İmza Oluşturmak
- YARA ve YARA Kuralları Oluşturma

3. Zafiyet Araştırma ve Exploit Geliştirme

*Kavramsal Bilgiler

- Exploit nedir?
- Remote, Local, Client-Side ve Server-Side Exploitler

- Zeroday Exploitler
- Exploit Paylaşım Portalları
- Zafiyet ve Exploit Ekonomisi
- Marketler (Etik ve Underground)

*Exploit Geliştirme için Diller

- C
- Perl
- Python

*Zafiyet Türleri

- Stack Buffer Overflow
- Heap Overflow
- Signedness Errors
- Use After Free
- Double Free
- Logical Errors

*Zafiyet Avcılığı

- Dinamik Reversing
- Server-side Uygulamalarda Zafiyet Avcılığı
- Client-side Uygulamalarda Zafiyet Avcılığı
- Fuzzing

*Exploit Geliştirme

- Shellcode Oluşturma
- Return Address Overwrite
- SEH Overflow
- Heap Spraying
- Bypassing DEP/ASLR

SIGNALSEC Information Security Consulting, Software and Technology Services Ltd.
SignalSEC Ltd. is a research company that provides information security services.The main mission of SignalSEC is providing effective vulnerability intelligence services to the customers.

SignalSEC Research team is an active team in international infosec community. Researchers of SignalSEC speak at international security conferences, discover vulnerabilities and publish security advisories.

Phone: +90 232 433 0DAY
Fax: +90 232 469 85 62
Email: info@signalsec.com
Web: www.signalsec.com