DOCENTE

Ingegnere elettronico, membro del C3I (Comitato Italiano Ingegneria dell'Informazione), board member di A3I (Associazione Italiana Ingegneri dell'Informazione), Coordinatore del Gruppo di lavoro di Informatica dell'Ordine degli Ingegneri della Provincia di Parma. Si occupa da anni di sicurezza informatica come consulente per aziende ed enti della Pubblica Amministrazione, per cui ha svolto attività di formazione e consulenza. Svolge inoltre attività di informatica forense in qualità di Consulente Tecnico di Parte e Consulente Tecnico d'Ufficio del Tribunale di Parma.

Destinatari
Utenti
Dipendenti aziendali
Manager

Obiettivi
Rendere edotti gli utenti sui potenziali rischi insiti nell'uso di strumenti informatici, fornendo gli strumenti adeguati per l'identificazione e il trattamento delle più rilevanti problematiche in ambito user security. Al termine del corso si avrà una conoscenza dei principali aspetti legati alla sicurezza informatica, si sarà in grado di identificare rischi e minacce, e di determinare le più adeguate tipologie di contromisure da mettere in atto.

Sicurezza informatica per utenti

(Durata: 8 h)

La sicurezza informatica: presentazione

I problemi

- Infezione da Virus «Crypto Ransomware»
  - E-Mail con il «contratto da firmare»
  - E-Mail con messaggio in segreteria di Whatsapp
  - E-Mail con la fattura
  - E-Mail con il link al sito del corriere per spedizione SDA
  - E-Mail con notifica di accesso anomalo al proprio conto corrente
- Furto di credenziali
- Furto di dati
- Possesso dei sistemi per ulteriori attacchi
- Attacco a siti Internet noti per propagare Malware
- SPAM
- Phishing
- Drive by Download
- Social Engineering
- Virus
- Worm

Punti deboli

- Impreparazione tecnica
- Complessità delle minacce
- Mancata formazione

Normative di Legge

- Il quadro normativo
- D. Lgs. 196/2003 – Codice in materia di protezione dei dati personali
- D. Lgs. 231/2001 – Reati informatici

Linee Guida per una navigazione più attenta

- Aggiornare il proprio sistema
- Adoperare soluzioni di «endpoint-security»
- Phishing
- link interni ad una e- mail di dubbia origine

Le applicazioni vulnerabili

- Quali sono le applicazioni più a rischio?
- Strumenti di Protezione
  - Sulla postazione
  - In Azienda e in Rete

Uso consapevole di Internet

Come arginare i rischi incombenti sui dati

- Le linee guida sulla sicurezza informatica
- Vulnerability Assessment
- Penetration Testing
- Antivirus
- Firewall
- IDS
- Sistemi di disaster recovery

DOCENTE

Ingegnere elettronico, membro del C3I (Comitato Italiano Ingegneria dell'Informazione), board member di A3I (Associazione Italiana Ingegneri dell'Informazione), Coordinatore del Gruppo di lavoro di Informatica dell'Ordine degli Ingegneri della Provincia di Parma. Si occupa da anni di sicurezza informatica come consulente per aziende ed enti della Pubblica Amministrazione, per cui ha svolto attività di formazione e consulenza. Svolge inoltre attività di informatica forense in qualità di Consulente Tecnico di Parte e Consulente Tecnico d'Ufficio del Tribunale di Parma.

Destinatari
Manager

Obiettivi Nel corso vengono individuati i principi base legati alla Sicurezza dei Servizi Cloud. Vengono inoltre descritte le relative clausole contrattuali standard, e definite le best practice in ottica Security & Compliance.
Obiettivi del corso: Al termine del corso si avrà una buona competenza delle principali minacce correlate all'utilizzo del Cloud. Verranno quindi individuate le clausole contrattuali più adeguate e gli standard de facto, con particolare riferimento al contenimento dei rischi ed al rispetto delle normative vigenti.
Prerequisiti: Il corso è rivolto a personale con elevate responsabilità decisionali, anche senza una specifica preparazione e conoscenza della materia informatica, e con una comprensione ad alto livello della giurisprudenza. Non sono richieste conoscenze pregresse specifiche.

Cloud Security and Contracting

(Durata: 8 h)

Modulo 1

- Utilizzo del cloud in ambito privato e professionale
- Rischi e minacce
- La Sicurezza del Cloud

Modulo 2

- Tipologie principali di Cloud
- Cloud Clauses
- Cloud Profiles

Modulo 3

- Clausole contrattuali standard
- Best practices

Modulo 4

- Valutazione di un contratto in termini di adeguatezza
- Valutazione di un contratto in termini di Security e di Compliance

Esempi e casistiche

DOCENTE

Ingegnere elettronico, membro del C3I (Comitato Italiano Ingegneria dell'Informazione), board member di A3I (Associazione Italiana Ingegneri dell'Informazione), Coordinatore del Gruppo di lavoro di Informatica dell'Ordine degli Ingegneri della Provincia di Parma. Si occupa da anni di sicurezza informatica come consulente per aziende ed enti della Pubblica Amministrazione, per cui ha svolto attività di formazione e consulenza. Svolge inoltre attività di informatica forense in qualità di Consulente Tecnico di Parte e Consulente Tecnico d'Ufficio del Tribunale di Parma.

Destinatari
IT Manager
Responsabile Sicurezza Informatica,
Tecnico di Sicurezza Informatica,
Consulenti Tecnici d'Ufficio,
Consulenti Tecnici di Parte

Obiettivi
Conoscere gli strumenti utilizzabili per monitorare la sicurezza della propria rete. Impostare opportune logiche di auditing per gli eventi critici di violazione della sicurezza. Ottimizzare l'utilizzo degli strumenti di rivelazione delle intrusioni per la propria rete. Conoscere le possibilità in termini di contromisure in circostanze di violazioni della sicurezza, impostabili automaticamente mediante gli IDS. Esercitarsi concretamente sulla configurazione e l'utilizzo di un potente sistema IDS.

Monitorare le reti mediante IDS Intrusion Detection Systems

(Durata: 8 h)

Perché utilizzare un IDS nella propria rete

- Ruolo e funzioni degli IDS nella sicurezza della rete
- Punti di forza e debolezze
- Dove e quando gli IDS devono essere usati
- Chi amministra gli IDS
- IDS vs. Firewall
- Insourcing vs. Outsourcing

Classificazione degli IDS

- Tipologie di Intrusion Detection Systems:
  - Network-Based
  - Host-Based
  - IDS Ibridi
  - IDS passivi e IDS attivi
  - Integrity monitors
  - Anomaly Based
  - Kernel monitors
  - Real-time vs. Pole for later

Architettura degli IDS

- Componenti di un sistema IDS
- Sensori
- Collettori
- Console di gestione
- Metatools

IDS basati su Rete (Network based IDS)

- Introduzione
- Architettura
- Sistema distribuito a nodi di rete
- Vantaggi/Svantaggi

CASE STUDY:
le principali vulnerabilità dei sistemi e possibili utilizzi degli IDS
Momento di riflessione riguardante i casi proposti dai partecipanti: verranno prese in considerazione le vulnerabilità principali solitamente riscontrate e le possibili contromisure da adottare mediante IDS

IDS basati su Host (Host based IDS)

- Introduzione
- Architettura
- Sistema distribuito basato su host
- Vantaggi/Svantaggi

Le Signature degli IDS e loro analisi

- Concetto di Signature
- Vulnerabilità comuni
- Signature di traffico normale
- Signature di traffico anomalo

IDS Open Source

- Snort, Aide, Tripwire
  - Architettura
  - Installazione
  - Configurazione
  - Logging

ESERCITAZIONE PRATICA: Installazione e Configurazione di Snort, Simulazione di un tentativo di attacco, Analisi dei log registrati.

Contromisure agli attacchi mediante gli IDS

- Monitoraggio del traffico
- Generazione di messaggi di allerta: tipologie di allertamento
- Impostazione di azioni basate su politiche di sicurezza
  - Forzare la disconnessione della sessione
  - Bloccare l'accesso alla rete alla sorgente dell'attacco
  - Bloccare tutti gli accessi alla rete

Cenni sugli IDS Commerciali (Funzionalità, vantaggi e svantaggi)

ESERCITAZIONE PRATICA:

- Installazione e Configurazione di OSSec,
- Simulazione di un tentativo di attacco,
- Analisi dei log registrati.

Gli IDS nella gestione degli attacchi: tuning dei sistemi

- Sistemi early-warning
- Procedure di escalation
- Politiche di sicurezza e procedure
- Definire l'ambito degli attacchi ed incidenti da gestire
- Definizione dei livelli di allarme degli IDS
- Le possibili fonti di risposta agli incidenti
- Integrazione di IDS e Firewall
- Sviluppare un'efficace capacità di risposta agli incidenti

Prospettive future, risorse

- Meta-IDS, NFAT tools, honeypots
- Siti informativi
- Documentazione sul web

DOCENTE

Ingegnere elettronico, membro del C3I (Comitato Italiano Ingegneria dell'Informazione), board member di A3I (Associazione Italiana Ingegneri dell'Informazione), Coordinatore del Gruppo di lavoro di Informatica dell'Ordine degli Ingegneri della Provincia di Parma. Si occupa da anni di sicurezza informatica come consulente per aziende ed enti della Pubblica Amministrazione, per cui ha svolto attività di formazione e consulenza. Svolge inoltre attività di informatica forense in qualità di Consulente Tecnico di Parte e Consulente Tecnico d'Ufficio del Tribunale di Parma.

Destinatari

IT Manager
Responsabile Sicurezza Informatica
Tecnico di Sicurezza Informatica

Obiettivi

Difendersi adeguatamente dagli attacchi, comprendendo le tecniche di hacking utilizzate per penetrare nelle reti informatiche.
Ottimizzare il proprio livello di sicurezza ed evitare il superamento delle barriere di protezione
Considerare i bug dei sistemi operativi e dei dispositivi di rete per i quali esistono exploit che consentono di ottenere accesso alle reti
Esercitarsi concretamente grazie alle simulazioni pratiche di Penetration Test

Effettuare il Penetration Test di reti LAN e WLAN

Verificare la sicurezza della propria rete informatica da attacchi esterni ed adottare le opportune contromisure (Durata: 24h)

Definire le fasi di un Penetration Test

- Introduzione: tipologie di Penetration Test
- Metodologie e standard, aspetti normativi
- Fase1. Il Footprinting della rete target
- Fase2. Effettuare la Scansione delle porte
- Fase3. L'Enumerazione di account, risorse, servizi
- Fase4. Identificare le vulnerabilità
- Fase5. L'hacking dei sistemi
- Fase6. Elaborare il report delle varie fasi con vulnerabilità Riscontrate
- La Suite Kali Linux

Individuare gli strumenti utilizzati dagli hacker per il footprinting della rete Target
Analizzare alcuni tra i molteplici strumenti (ricerche Whois, Maltego, etc.):

- per recuperare informazionisull'organizzazione
- per indagare sui domini
- per recuperare informazioni sulla rete (indirizzi IP)
- per la perlustrazione della rete

Interrogazione dei DNS

- Imparare ad utilizzare gli strumenti per interrogazione dei DNS: Nslookuo, Dig,etc
- Capire le vulnerabilità dovute ai trasferimenti di zona
- Analizzare i record A, MX, SRV, PTR
- Quali contromisure impiegare in questa fase

Identificazione dell'architettura della rete target

- Strumenti di tracerouting
- Tracert, e Traceroute
- Tracerouting con geolocalizzazione

Tecniche di Footprinting mediante motori di ricerca

- Footprinting con Google: utilizzo di campi chiave di ricerca
- Utilizzo di strumenti frontend per ricerche su motori: Sitedigger
- Footprinting su gruppi di discussione

Introduzione a TOR (The Onion Router)

- Comprendere le tecniche utilizzate dagli hacker per rendersi anonimi
- Tor-Browser
- Proxychains

ESERCITAZIONE PRATICA: simulare la fase di footprinting di una rete target
I partecipanti, con la guida del docente, simuleranno la fase di footprinting per esaminare quali informazioni è possibile reperire sulla rete target.

Introduzione alla fase di scansionamento delle reti

- Tipologie di scansionamento
- Aspetti legali inerenti lo scansionamento di porte
- TCP, UDP, SNMP scanners
- Strumenti Pinger
- Information Retrieval Tools
- Attuare contromisureagli scansionamenti

Tools per lo scansionamento

- Query ICMP
- Utilizzo di Nmap e SuperScan
- Tools di scansionamento presenti nella distribuzione Kali Linux
- Scanner per dispositivi mobile

ESERCITAZIONE PRATICA: simulare la fase di scansionamento di una rete target
Introduzione alla fase di Enumerazione.

Capire il funzionamento degli strumenti perl'enumerazione delle reti
- Enumerazione di servizi "comuni": FTP, TELNET, SSH, SMTP, NETBIOS, etc
- Enumerazione SNMP
- Ricercare le condivisioni di rete
- Ricerca di account di rete
- Conoscere le contromisure più efficaci per l'enumerazione

Conoscere l'Hacking dei sistemi per rendere sicure le reti
- Conoscere le principali tecniche di attacco ai sistemi
- Quali sono le principali tipologie di vulnerabilità Sfruttabili
- Ricerca di vulnerabilità inerenti i servizi rilevati nella fase di enumerazione:
  - Ricerca "Manuale"
  - I Vulnerability Scanner

ESERCITAZIONE PRATICA: Ricerca di Vulnerabilità in modo manuale e mediante Vulnerability Scanner

Comprendere l'Hacking dei sistemi operativi Microsoft Windows
- Hacking di Windows: le vulnerabilità più recenti
- Attacchi senza autenticazione
- Attacchi con autenticazione: scalata di privilegi (tecniche e tools)

ESERCITAZIONE PRATICA: effettuare la simulazione dell'hacking di un sistema Windows con Metasploit

Attacchi di tipo Man-In-The-Middle
- Dirottamento di sessioni
- Attacchi di tipo ARP Poisoning
- Tools per attacchi MitM: Cain&Abel

Cenni sull' Hacking dei Firewall
- Identificare i firewall di rete
- Sfruttare gli errori di configurazione
- Contromisure per evitare le vulnerabilità dei firewall

Comprendere l'Hacking del Web: hacking dei server web ed hacking delle applicazioni
- Identificare la tipologia del server web target
- Verificare le vulnerabilità di IIS e Apache
- Individuare vulnerabilità in applicazioni ASP, PHP, JSP
- Hacking mediante SQL Injection, Cross-Site Scripting, Cross-Site Request Forgery, etc
- Predisporre efficaci contromisure

ESERCITAZIONE PRATICA: effettuare l'hacking di un web server
Verrà simulato un tentativo di violazione di un sito web per verificarne la corretta configurazione in termini di sicurezza

Cenni all'Hacking di Unix/Linux
- Cercare l'utente root
- Quali sono le principali tipologie di intrusione in sistemi Unix
- Sapere come evitare le intrusioni

Hacking di reti Wireless: le principali vulnerabilità
- Strumenti per effettuare la scansione delle reti wireless
- Packet Sniffer wireless, hacking di WEP, WPA e WPA2
- Strumenti di hacking delle WLAN inclusi in Kali Linux

Cenni all'Hacking nel mondo mobile
- Introduzione al rooting di dispositivi Android
- Introduzione al rooting di dispositivi iOS
- Laboratorio: hacking di un dispostivo Android

DOCENTE

Ingegnere elettronico, membro del C3I (Comitato Italiano Ingegneria dell'Informazione), board member di A3I (Associazione Italiana Ingegneri dell'Informazione), Coordinatore del Gruppo di lavoro di Informatica dell'Ordine degli Ingegneri della Provincia di Parma. Si occupa da anni di sicurezza informatica come consulente per aziende ed enti della Pubblica Amministrazione, per cui ha svolto attività di formazione e consulenza. Svolge inoltre attività di informatica forense in qualità di Consulente Tecnico di Parte e Consulente Tecnico d'Ufficio del Tribunale di Parma.

Destinatari

IT Manager
Responsabile Sicurezza Informatica,
Tecnico di Sicurezza Informatica,
Consulenti Tecnici d'Ufficio,
Consulenti Tecnici di Parte

Obiettivi

Conoscere le minacce a cui possono essere soggetti i dispositivi mobili (smartphone e tablet). Utilizzare strumenti e metodologie per eviatare tali minacce e sanare le vulnerabilità.

Sicurezza dei dispositivi mobili

(Durata: 8 h)

Le principali minacce incombenti sui dispositivi mobili

- Classificazione ENISA dei principali rischi di sicurezza di smartphone e tablet:
  - Data leakage
  - Unintentional discolure
  - Attacks on decommissioned smartphones
  - Phishing attacks
  - Spyware attacks
  - Network spoofing attacks o Surveillance attacks
  - Diallerware attacks
  - Financial malware attacks o Network congestion

Strumenti per la sicurezza attiva di dispositivi mobili

- Antivirus per dispositivi mobili
- Firewall per dispositivi mobili

Individuazione di vulnerabilità nei dispositivi mobili

- Vulnerability scanner

Root di dispositivi Android

- Vantaggi e svantaggi
- Il problema di malware nella App

Jailbreak di dispositivi iOS

- Rischi e pericoli del jailbreak

Root di dispositivi Windows Phone

- Vantaggi e svantaggi

CASE STUDY: **le principali vulnerabilità dei dispositivi Android**

- Momento di riflessione riguardante dispositivi mobile Android: verranno prese in considerazione le vulnerabilità principali solitamente riscontrate e le possibili contromisure da adottare per smartphone e tablet Android

CASE STUDY: **le principali vulnerabilità dei dispositivi iOS**

- Momento di riflessione riguardante dispositivi mobile iOS: verranno prese in considerazione le vulnerabilità principali solitamente riscontrate e le possibili contromisure da adottare per smartphone e tablet iOS

CASE STUDY: **le principali vulnerabilità dei dispositivi Windows Phone**

- Momento di riflessione riguardante dispositivi mobile Windows Phone: verranno prese in considerazione levulnerabilità principali solitamente riscontrate e le possibili contromisure da adottare per smartphone e tablet Winphone