Avogadro Security Course

Documento di presentazione del progetto

I.I.S Avogadro 2020/2021 Pimen Flavian Dei

Sommario

Introduzione

Descrizione del corso

Il progetto “Avogadro Security Course” (o ASC) nasce per permettere a ragazzi dell’Istituto Amedeo Avogadro di Torino di avvicinarsi al mondo della sicurezza informatica, uno dei campi dell’Information Technology con una richiesta sempre più crescente. Il corso si concentra sulla parte offensiva della sicurezza informatica così da permettere ai ragazzi di intraprendere una carriera sia nell’ambito offensivo, come per esempio Penetration Tester o Red Teaming, oppure nell’ambito difensivo, come per esempio Incident Responder o SOC.

In tutti e due i casi è richiesta una solida conoscenza di come gli attacchi informatici, dai più semplici a quelli più avanzati, funzionano. Infatti, conoscendo le tecniche usate dai malintenzionati, risulterà estremamente più semplice mettere in sicurezza le infrastrutture e rilevare possibili attacchi.

Perché la Sicurezza Informatica?

Già dall’antichità i messaggi importanti venivano criptati per impedire che nemici potessero comprendere il significato del testo. Basti pensare al *Cifrario di cesare*, uno dei cifrari più noti e che fu creato proprio sotto l’impero di Giulio Cesare!

Ai giorni d’oggi questa necessità è aumentata notevolmente. Ormai usiamo internet per molte attività: comunicare con persone a noi care, guardare le notizie dell’ultima ora, trasferire soldi e molte volte anche lavorare. La necessità di tenere tutti i nostri di dati (e quelli dei possibili clienti) è più che importante: è vitale. Per una piccola azienda basterebbe un singolo attacco informatico per mandare in rovina tutta l’attività.
Grazie a questo, i posti di lavoro nel settore della Cyber Security stanno aumentando notevolmente negli ultimi anni, tanto da far diventare gli esperti in questo settore i più ricercati nel settore IT.

Requisiti

Agli studenti è richiesto:

- Conoscenza base di reti informatiche
- Conoscenza di almeno un linguaggio di programmazione
- Conoscenza base dei sistemi Windows
- Capacità collaborativa
- La conoscenza di linux è consigliata ma non obbligatoria
- Un computer con almeno 4 GB di RAM
- Voglia di imparare

Struttura del Corso

Struttura generale

Gruppi

Gli studenti saranno divisi in gruppi per consentire loro di collaborare durante tutto il corso. I gruppi verranno creati per essere equilibrati tra di loro: prima dell'inizio del corso, gli studenti dovranno fare un test per determinare il loro livello di conoscenza su alcuni argomenti, tra cui programmazione, reti informatiche e basi di sicurezza informatica. Questo permetterà di creare gruppi con persone allo stesso livello.

E' stata presa la decisione di creare dei gruppi per far collaborare le persone durante gli esercizi pratici, e per consenti di avere un ambiente più piacevole e divertente.

Moduli

Il corso sarà diviso in 5 diversi moduli (questa struttura potrebbe subire modifiche):

1. Introduzione
2. Raccolta di informazioni
3. Network Security
4. Web Application Security
5. System Security

*La descrizione dettagliata di ogni modulo si può trovare nella sezione **Argomenti**.*

Esercizi

Il corso offrirà agli studenti la possibilità di provare con mano gli argomenti trattati, attraverso laboratori virtuali e macchine virtuali a disposizione 24/7 agli studenti, cosi da permettere agli studenti di esercitarsi anche fuori dalle ore di lezione.

*Una descrizione dettagliata dei laboratori e degli esercizi si può trovare nella sezione **Materiali Didattici**.*

Materiali Didattici

Il materiale didattico si divide in tre categorie:

1. PDF
2. Video
3. Esercizi e Laboratori

Tutti i materiali saranno sempre disponibili agli studenti.

Piattaforma online

Agli studenti verrà concesso l'accesso ad una piattaforma online contenente tutti i materiali didattici (PDF, Video e Laboratori virtuali). Gli studenti dovranno creare un account per impedire a persone esterne dalla scuola di interagire con i laboratori virtuali installati all'interno della scuola.

PDF

Teoria

Sulla piattaforma sarà possibile scaricare un pdf unico contenente tutte le spiegazioni teoriche del corso. Il PDF conterrà immagini per semplificare la spiegazione e presenterà alla fine di ogni capitolo una sezione contenente link a materiali (Libri, Ricerche, Corsi ecc.) dove andare ad approfondire gli argomenti.

Pratica

All'interno della piattaforma sarà presente una sezione contenente diversi PDF da scaricare per avere i dettagli dei singoli esercizi da svolgere. Ogni PDF conterà la descrizione dell'esercizio, gli strumenti da utilizzare,
un'eventuale guida sul setup da seguire, una serie di task per guidare lo studente e

una soluzione finale nel caso lo studente non riesca ad andare avanti, con dettagli di ogni singolo passaggio.

Video

Molti argomenti saranno accompagnati da video contenenti spiegazioni pratiche degli argomenti e degli strumenti spiegati all'interno del PDF principale. I video saranno in HD e con audio pulito, cosi da consentire una visione perfetta allo studente.

Esercizi e Laboratori

All'interno del corso saranno presenti esercizi e materiali per consentire agli studenti di esercitarsi sugli argomenti trattati.
Gli esercizi si suddividono in:

- Esercizi teorici
- Laboratori virtuali
- Macchine Virtuali
- Laboratori esterni

Esercizi teorici

Gli esercizi teorici verranno creati in formato PDF con all'interno domande (a scelta multipla, domande aperte,) teoriche sull'argomento teorico, così da consentire agli studenti di capire i propri punti di pagine dove poter andare a studiare gli argomenti della domanda nel caso in cui lo studente volesse.

Laboratori virtuali

Ogni studente avrà la possibilità di avviare, attraverso la piattaforma, un collegamento con una macchina virtuale collegata all'interno di una **rete completamente isolata**, cosi da permettere di eseguire gli attacchi informatici più dannosi senza nessun pericolo o preoccupazione. Ci saranno diverse macchine virtuali e diverse reti che gli studenti potranno usare all'interno del corso e tutti i laboratori potranno essere avviati direttamente dalla piattaforma.

Macchine Virtuali

Saranno messe a disposizione agli studenti delle **macchine virtuali** così da permettergli di avviarle e seguire gli esercizi su di essa senza l'uso di infrastrutture esterne.

Laboratori esterni

Verranno usati, durante il corso, diversi laboratori virtuali messi a disposizione da aziende o enti esterni (PortSwigger Ltd. , Hack The Box Ltd, The OWASP Foundation …). I laboratori sono completamente gratuiti.

Argomenti

Gli argomenti posso ricevere delle modifiche durante la creazione del corso.

1. Introduzione

In questo modulo gli studenti verranno introdotti nel mondo della sicurezza informatica. Verranno spiegati aspetti teorici del **Penetration Testing** e della sicurezza informatica in generale, come per esempio: termini tecnici, metodologie, i diversi tipi di consulenza ecc.

Argomento nel Dettaglio

1. Cos'è la sicurezza informatica
   1.1. La sicurezza nella storia
   1.2. La sicurezza oggi
   1.3. Data Breach
   1.4. Termini Tecnici
   1.5. Gli elementi della sicurezza informatica
   1.6. Il triangolo della Sicurezza, Funzionalità e Usabilità
2. Vettori di attacco e Threads
   2.1. Motivi, obiettivi e obbiettivi di un attacco informatico
   2.2. Tipi di attacchi
3. Tipi, concetti e fasi di un hackeraggio
   3.1. Hacker
   3.2. Hacking
   3.3. Fasi di un hacking
4. Penetration Testing
   4.1. Cos'è un Penetration Testing
   4.2. L'importanza di un Penetration testing
   4.3. Tipi di Penetration testing
   4.4. Fasi di un Penetration Testing
5. Sicurezza fisica
6. Metodologie

2. Raccolta di Informazioni

In questo modulo gli studenti studieranno e metteranno in pratica tecniche usate per raccogliere informazioni su un Target come un'azienda e/o infrastrutture attraverso tecniche di **OSINT** (*Open Source INTelligence*), cioè la raccolta di informazioni attraverso internet.

Argomento nel Dettaglio

1. Cos'è L'OSINT
   1.1. Da chi è usato
   1.2. Storia
   1.3. Perché è importante la raccolta di informazioni
2. Raccogliere informazioni sull'azienda
   2.1. Il sito
   2.2. I partner
   2.3. I dipendenti
   2.4. I prodotti e i servizi
   2.5. E-mail
   2.6. Numeri di telefono
   2.7. Indirizzi
3. Whois
4. Social Network
   4.1. Facebook
   4.2. Linkedin
   4.3. Twitter
   4.4. **Tool:** TheHarvester
5. Siti pubblici
   5.1. Siti Governativi
   5.2. CrunchBase
6. Motori di ricerca
   6.1. Saper cercare su internet
   6.2. Google dorks
   6.3. Trovare file sensibili
7. Enumerazione dei sottodomini

3. Network Security

In questo modulo gli studenti studieranno le metodologie e i tipi di attacchi usati contro una rete informatica. Verranno insegnati agli studenti diversi strumenti per facilitare svariati compiti durante un test su una o più reti informatiche.

Argomento nel Dettaglio

1. Introduzione
   1.1. ISO/OSI
   1.2. TCP/IP
   1.3. DNS
   1.4. Routing
2. Enumerazione di una rete
   2.1. Determinare gli host online
   2.2. **Tool:** nmap
   2.3. **Tool:** hping3
   2.4. Tecniche di evasione
3. Scanning di un host
   3.1. Determinare le porte aperte
   3.2. Determinare i servizi
   3.3. Determinare il sistema operativo
4. Enumerazione
   4.1. NETbios
   4.2. SMB
   4.3. SNMP
   4.4. Protocolli Linux
5. Active Directory *(?)*
   5.1. Come funziona
   5.2. Enumerazione
   5.3. Tecniche di attacco
6. Metasploit
7. Vulnerabilty Auditing
   7.1. Cos'è
   7.2. **Tool:** Nessus
   7.3. MS-17-10
8. Bruteforce
9. Sniffing e MITM
   9.1. Come funziona lo sfinnig

9.2. HTTP e HTTPS
9.3. **Tool:** Wireshark
9.4. MITM
9.5. Arp Poisoning

4. Web Security

In questo modulo gli studenti impareranno a testare un'applicazione web per trovare vulnerabilità sfruttabili dai malintenzionati.

Argomento nel Dettaglio

1. Introduzione
   1.1. Il protocollo HTTP
   1.2. Cookies
   1.3. SOP
2. Raccolta di informazioni
   2.1. Sottodomini
   2.2. Pagine web
   2.3. Salvare le informazioni
3. XSS
   3.1. Cos'è
   3.2. I diversi tipi di XSS
   3.3. Come trovare un XSS
   3.4. Reflected XSS
   3.5. Stored XSS
   3.6. DOM XSS
4. SQL Injection
   4.1. Cos'è
   4.2. I diversi tipi di SQL injection
   4.3. Come trovare un SQL Injection
   4.4. **Tool:** SQL Injection
5. CSRF
6. RFI e LFI

5. System Security

In questo modulo gli studenti studieranno come testare un sistema informatico dopo la compromissione e come raccogliere informazioni utili per continuare i propri test.

Argomento nel Dettaglio

1. Come Lavora windows
   1.1. File System
   1.2. Password Hash
2. Raccolta di informazioni
   2.1. Servizi
   2.2. Rete
   2.3. File
   2.4. Shares
   2.5. Credenziali
3. Privilege Escalation
   3.1. Metasploit
   3.2. UAC Bypass
   3.3. Unquoted Service Paths
4. Mantenimento dell'accesso
   4.1. Pass the hash
   4.2. Mimikatz
   4.3. Windows Credentials Editor (WCE)
   4.4. RDP
   4.5. Backdoor
   4.6. Nuovo utente
   4.7. DLL Injection/Preloading
5. Windows Password Cracking
   5.1. Remote
   5.2. Local
   5.3. Live host
   5.4. Offline
   5.5. Pass the hash
   5.6. Cracking
   5.7. **Tool:** John The Ripper
6. Pillaging
   6.1. DNS Tunneling
7. Pivoting

7.1. Mappare la rete
7.2. Scanning

Visione generale degli argomenti

1. Introduzione
   1.1. Cos'è la sicurezza informatica
      1.1.1. La sicurezza nella storia
      1.1.2. La sicurezza oggi
      1.1.3. Data Breach
      1.1.4. Termini Tecnici
      1.1.5. Gli elementi della sicurezza informatica
      1.1.6. Il triangolo della Sicurezza, Funzionalità e Usabilità
   1.2. Vettori di attacco e Threads
      1.2.1. Motivi, obiettivi e obbiettivi di un attacco informatico
      1.2.2. Tipi di attacchi
   1.3. Tipi, concetti e fasi di un hackeraggio
      1.3.1. Hacker
      1.3.2. Hacking
      1.3.3. Fasi di un hacking
   1.4. Penetration Testing
      1.4.1. Cos'è un Penetration Testing
      1.4.2. L'importanza di un Penetration testing
      1.4.3. Tipi di Penetration testing
      1.4.4. Fasi di un Penetration Testing
   1.5. Sicurezza fisica
   1.6. Metodologie
2. Raccolta di informazioni
   2.1. Cos'è L'OSINT
      2.1.1. Da chi è usato
      2.1.2. Storia
      2.1.3. Perché è importante la raccolta di informazioni
   2.2. Raccogliere informazioni sull'azienda
      2.2.1. Il sito
      2.2.2. I partner
      2.2.3. I dipendenti
      2.2.4. I prodotti e i servizi

5.2. Raccolta di informazioni
    5.2.1. Servizi
    5.2.2. Rete
    5.2.3. File
    5.2.4. Shares
    5.2.5. Credenziali
5.3. Privilege Escalation
    5.3.1. Metasploit
    5.3.2. UAC Bypass
    5.3.3. Unquoted Service Paths
5.4. Mantenimento dell'accesso
    5.4.1. Pass the hash
    5.4.2. Mimikatz
    5.4.3. Windows Credentials Editor (WCE)
    5.4.4. RDP
    5.4.5. Backdoor
    5.4.6. Nuovo utente
    5.4.7. DLL Injection/Preloading
5.5. Windows Password Cracking
    5.5.1. Remote
    5.5.2. Local
    5.5.3. Live host
    5.5.4. Offline
    5.5.5. Pass the hash
    5.5.6. Cracking
    5.5.7. **Tool:** John The Ripper
5.6. Pillaging
    5.6.1. DNS Tunneling
5.7. Pivoting
    5.7.1. Mappare la rete
    5.7.2. Scanning