Progetti del Corso Cyber Security e Protezione dei Dati

Federica Paci

22 Dicembre 2023

1 Modalità d'esame

Gli studenti verranno valutati sulla base di

- un progetto pratico o di un approfondimento teorico degli argomenti del corso
- un esame orale sugli argomenti del corso.

Progetto Il progetto può essere svolto in gruppo di al massimo 2 studenti. I progetti disponibili per l'anno accademico 2023/2024 sono descritti nelle sezioni successive di questo documento. I risultati del progetto verranno riassunti in una relazione scritta e poi presentati oralmente al docente. La relazione va consegnata al docente via email **una settimana prima** dell'esame orale.

Esame Orale Durante l'esame orale, gli studenti presenteranno il progetto al docente, che farà domande sul progetto e anche su qualsiasi argomento del corso.

Registrazione per Sostenere Esame Orale Un mese prima della sessione d'esame il docente pubblicherà un file excel sulla pagina Moodle del Corso con le date e orari in cui sarà possibile sostenere l'esame orale: gli studenti devono registrarsi inserendo il proprio nome nel file excel e registrandosi su esse3 per facilitare il processo di verbalizzazione dell'esame.

Voto Finale Il voto finale è risultante dalla media aritmetica del voto assegnato al progetto e dal voto assegnato alle risposted alle domande di teoria sugli argomenti del corso. Se il progetto è stato svolto in gruppo di due studenti il voto assegnato al progetto sarà lo stesso per entrambi gli studenti.

2 Realizzazione di un documento Word Malevolo

L'obiettivo di questo progetto è quello di realizzare un documento Word malevolo che contiene una macro VBA che all'apertura del documento esegue un comando Powershell. Il comando Powershell deve scaricare un malware per Windows da una serie di URL associati a server C2, salvarlo sulla macchina ed eseguirlo. Il codice della macro VBA deve essere offuscato e il comando powershell deve essere codificato in base 64.

Il report per presentare l'implementazione del documento malevolo deve seguire il template scaricabile cliccando qui Template MalDoc

Durante l'esame orale gli studenti dovranno dimostrare che il documento malevolo scarica il malware su una macchina Windows. Per la dimostrazione verranno utilizzate due macchine virtuali: una macchina simula la macchina dove sono ospitati i server C2 e una macchina Windows che è il target dell'attacco.

3 Realizzazione di un malware per Windows

L'obiettivo di questo progetto è quello di realizzare un trojan per il sistema operativo Windows che trafuga informazioni - dati, password, file - dalle macchine delle vittime. In particolare, il malware deve implementare le seguenti tecniche della MITRE Att&ck matrix:

- Persistence - Create or Modify System Process: Windows Service [T1543.003]. Questa tecnica prevede che il malware crei un servizio che viene eseguito ogni volta che la macchina Windows viene riavviata.
- Defense Evasion - Impair Defenses ID[T1562.001] Questa tecnica prevede che il malware disabiliti Windows Defender e altri software anti-virus installati sulla macchina della vittima.
- Exfiltration - Exfiltrate Data Through Cloud Account -T1537. Questa tecnica prevede che il malware trasferisca dati e file sensibili utilizzando un account cloud quali Mega o Google.

Il report per presentare l'implementazione del malware deve seguire il template scaricabile dal seguente link: Template Malware. Durante l'esame orale gli studenti dovranno dimostrare che il malware implementa le tecniche descritte sopra utilizzando una macchina virtuale Windows.

4 Analizzare conformità dei siti web con il principio di trasparenza del GDPR

La trasparenza è un obbligo trasversale del GDPR che si esplica, in particolare, in tre aspetti:

- l'informativa resa agli interessati circa il trattamento di dati,

- le informazioni date dai titolari agli interessati sui loro diritti; e
- le modalità con cui viene consentito e facilitato l'esercizio dei diritti agli interessati.

Il principio di trasparenza trova la sua principale espressione nell'informativa privacy il cui contenuto e la modalità con cui viene presentata agli interessati devono rispettare i requisiti imposti dagli articoli 12 e 13 del GDPR.

L'obiettivo di questo progetto è di valutare la conformità di un campione di 30 siti web con il principio di trasparenza imposto dal GDPR. In particolare, il progetto ha l'obiettivo di dare una risposta alla seguente domanda di ricerca:

- RQ_1Le politiche di privacy dei siti web sono conformi con il GDPR (articolo 12 e articolo 13)?

4.1 Metodologia per svolgere il progetto

Contattare il docente per avere l'elenco dei 30 siti da analizzare.

Raccolta Dati Per ciascun sito è necessario salvare una copia della politica di privacy in formato pdf e indicare il percorso fatto in termini di numero clicks per trovare la politica di privacy.

Analisi Dati Per ciascun sito rispondere alle domande riportate nel documento excel disponibile a questo link: Template Analisi Politiche Salvate una copia del documento excel e rispondete alle domande presenti. Il documento e' organizzato in diverse sezioni: la prima sezione contiene domande sul contenuto della politica, la seconda sezione domande sull'accessibilita' del documento, la terza sul linguaggio utilizzato per scrivere la politica, la quarta sulla leggibilita' della politica e una sezione sull'interfaccia web adottata per presentare la politica. L'ultima sezione Violazioni spiega quando la risposta ad un domanda nelle sezioni precedenti rappresenta una violazione del GDPR.

Presentazione Risultati Per ciascuna sezione del documento excel bisogna creare una tabella dove vengono riportare le domanda presenti nella sezione e affianco la percentuale di siti web la cui politica di privacy viola il requisito del GDPR specificato dalla domanda. Inoltre, per ciascuna sezione del documento excel bisogna ripotare la percentuale di siti web che vieno almeno uno dei requisiti imposti dal GDPR esplicitati dalla correspondente domanda. Il template del report per presentare i risultati e' scaribile da qui:Report Template

5 Analizzare conformità dei siti web con il diritto di accesso

L'obiettivo di questo progetto è di valutare la conformità di un campione di 30 siti web con i requisiti imposti dall'articolo 15 del GDPR dell'esercizio del diritto di accesso da parte dei soggetti interessati. In particolare, il progetto ha l'obiettivo di dare una risposta alla seguente domanda di ricerca:

- RQ_1 Le modalità adottate dai fornitori di servizi web per consentire il diritto di accesso ai dati sono conformi con il GDPR?

5.1 Metodologia per svolgere il progetto

Contattare il docente per avere l'elenco dei 30 siti da analizzare.

Raccolta Dati Per ciascun sito è necessario creare un'account e fornire le relative informazioni personali quali nome, cognome, indirizzo, eta' e genere. Interagite con il sito web per una periodo di due settimane in modo tale da consentire la raccolta di altre informazioni personali oltre a quelle fornite durante la fase di registrazione. Mantenete un elenco delle informazioni personali fornite a ciascun sito sia durante la fase di creazione dell'account che nelle successive interazioni. Dopo di che, e' necessario verificare quali sono i metodi proposti dal sito per richiedere l'accesso ai propri dati personali. Le opzioni possibili di solito sono via email diretta al **DPO** aziendale o figure simili, ma a volte vi era la possibilità di usufruire di un servizio apposito per il **download dei dati** direttamente dal profilo utente o di **Form** appositi da compilare. Se richiede l'acceso ai dati mediante email utilizzate il template riportato **??**enete traccia della modalita' proposta dal sito per richiedere l'accesso ai dati, della relativa risposta e della copia dei dati forniti dal fornitore del servizio.

Analisi Dati Per ciascun sito rispondere alle domande riportate nel documento excel disponibile a questo link: Template Diritto di Accesso. Salvate una copia del documento excel e completate le risposte alle domande presenti. Il documento e' organizzato in tre sezioni con domande relative alla conformita' della richiesta di accesso, della risposta e della copia dei dati con gli articoli 12 e 15 del GDPR. La maggior parte delle domande prevede una risposta Si/No. Assumete che ci sia una violazione quando la risposta alla domanda e' No.

Presentazione Risultati Per la sezione sulla risposta del fornitore del servizio creare una tabella dove vengono riportare le domande presenti

nella sezione e affianco la percentuale di siti web che violano il requisito del GDPR specificato dalla domanda. Per le sezioni relative alla richiesta e alla copia dei dati seguire le indicazioni presenti nel template del report scaribile da qui:Report Template