Struttura Corso

Prerequisiti

- Informatica di base e termini specifici: nozione di software, hardware, rete informatica, file, bug…

Risultano utili anche alcune nozioni di:

- Sistemi operativi: FileSystem, System Calls,…
- Reti: LAN, reti wireless, router,…

Scopo

- Introduzione al tema della sicurezza in ambito informatico
- In particolare ci si è voluti soffermare su temi che possono essere utili per la prova di informatica

Contesto e Articolazione

- **Classi**: V ITC Indirizzo Programmatori
- **Durata**: 18h, incluse verifiche…all'incirca 3h per ogni UD
- **Luogo**: laboratorio
- **Strumenti**: videoproiettore, pc dotati di connessione ad Internet
- **Articolazione**: 12h di lezione + 6h dedicate alle verifiche sommative

Modalità di lavoro

- **Metodologie**
  - Lezione frontale e partecipata,
- **Modalità di presentazione argomenti**
  - Slides pdf
  - Video di approfondimento
  - Link a fonti di approfondimento attinenti l'attualità…
- **Ambiente didattico**
  - Basato sul Web e sulla multimedialità per aumentare il grado di coinvolgimento
- **Contenuti**
  - materiale didattico

Verifiche: Tipologia

Tipologia:

- Test a risposta multipla (v. formative, v.prerequisiti)
- Test a risposta multipla + 5 domande a risposta aperta (v. sommative)
- Domande aperte (v. sommativa orale)

Verifiche «scritte» : modi e tempi

Effettuate attraverso la **piattaforma di e-learning** (Moodle o Docebo)

- **Test**
  - 12 domande somministrate in ordine casuale
  - Le domande sono le stesse sia per le verifiche formative che sommative, da qui il tempo molto ridotto per il test «sommativo»
- **Domande aperte** mirate a valutare :
  - la capacità di esposizione, rielaborazione e approfondimento dei contenuti appresi
  - Capacità di cogliere nessi logici con le UD precedenti

Verifiche «scritte»: modi e tempi

- **Verifica prerequisiti**(10min)
  - 12 domande a risposta multipla, all'inizio corso,
  - servono ad accertare non solo il possesso dei prequisiti ma anche il livello di partenza della classe
- **Verifica formativa** (10-15 min)
  - in classe al termine della lezione sull'argomento svolto,
  - online da casa (numero illimitato di tentativi)
- **Verifica sommativa** (45 min)
  - 45 min = 5 min (Test) + 40 min (5 domande aperte)
  - Prima di iniziare la nuova UD

Osservazioni...

- La scelta di utilizzare lo stesso test sia per la verifica sommativa che formativa ha i seguenti obiettivi :
  - stimolare lo studente a sfruttare le potenzialità della piattaforma per studiare in maniera più efficace le risposte fornite e colmare le lacune rivedendo e approfondendo gli argomenti trattati
  - Ridurre il grado di difficoltà percepita dalla studente nei confronti della prova
  - Permettere di effettuare un'analisi più approfondita delle competenze dello studente in un tempo limitato

Valutazione: indicatori

- **Test** (Punteggio convertito in decimi)
  - 1 punto a domanda, 0 penalità
- 5 **Domande Aperte** (Punteggio base = 2.5 + 1.5 punti a domanda)
  - Completezza
  - Livello di rielaborazione e approfondimento dimostrato
  - Ordine e coerenza logica
  - Chiarezza espositiva
  - Utilizzo lessico specifico
- **Voto finale** = 0.3 * **Voto TEST** + 0.7 * **Voto Domande**

Recupero: modalità

- Il recupero verrà attuato in itinere
  - In aula… attraverso una l'analisi dei risultati della verifica formativa e sommativa
  - A casa… grazie alla piattaforma di e-learning (verifiche formative , forum e chat, materiale didattico e link di approfondimento) sfruttando sempre il carattere collaborativo della piattaforma(saranno gli studenti stessi, oltre al docente, a fornire supporto ai compagni più in difficolta)

Piano di lavoro UD1

Fasi	Articolazione	Strategie e contenuti	Strumenti	Tempo
1	Introduzione Corso	Presentazione… - Obiettivi del corso, - Struttura del corso, - Materiale didattico, - Modalità di verifica	Videoproiettore, Presentazione, Moodle	10 min
2	Verifica Prerequisiti, Livello di Partenza + Analisi risposte	Test a risposta multipla	Moodle	10 min (Test) 20 min (Analisi risposte)
3	Introduzione alla sicurezza	Lezione frontale e partecipata: - Minacce e Danni - Risorse da proteggere - Profilo del pirata informatico - Evoluzione del cyber-crimine	Videoproiettore, Presentazione, Video, Link Approfondimento	50 min
4	Verifica Formativa, analisi delle risposte e recupero	Test a risposta multipla(10 domande)	Moodle	10 min(Test) 20 min (Discussione)
5 CASA	Studio - Esercitazione sulla piattaforma	Test a risposta multipla(lo stesso) Forum, Chat tra gli studenti	Moodle	
6	Verifica Sommativa	Test a risposta multipla(lo stesso) + 3 domande a risposta aperta	Moodle	5 min(Test) 40 min(domande)

Piano di lavoro UD2

Fasi	Articolazione	Strategie e contenuti	Strumenti	Tempo
1	Introduzione alla sicurezza	Lezione frontale e partecipata: Obiettivi - Riservatezza - Integrità - Disponibilità - Autenticazione - Tracciabilità - Monitoraggio - Non ripudio	Videoproiettore, Presentazione, Video, Link Approfondimento	40 min
2	Verifica Formativa, analisi delle risposte e recupero	Test a risposta multipla(10 domande)	Moodle	10 min(Test) 20 min (Discussione)
3	Studio - Esercitazione sulla piattaforma	Test a risposta multipla(lo stesso) Forum, Chat tra gli studenti	Moodle	
4	Verifica Sommativa	Test a risposta multipla(lo stesso) + 3 domande a risposta aperta	Moodle	5 min(Test) 35 min(domande)

Piano di lavoro UD3

Fasi	Articolazione	Strategie e contenuti	Strumenti	Tempo
1	Introduzione alla sicurezza	Lezione frontale e partecipata: - analisi dei rischi, - politiche di sicurezza, - Disaster Recovery Plan	Videoproiettore, Presentazione, Video, Link Approfondimento	40 min
2	Verifica Formativa, analisi delle risposte e recupero	Test a risposta multipla(10 domande)	Moodle	10 min(Test) 20 min (Discussione)
3	Studio - Esercitazione sulla piattaforma	Test a risposta multipla(lo stesso) Forum, Chat tra gli studenti	Moodle	
4	Verifica Sommativa	Test a risposta multipla(lo stesso) + 3 domande a risposta aperta	Moodle	5 min(Test) 40 min(domande)

Piano di lavoro UD4

Fasi	Articolazione	Strategie e contenuti	Strumenti	Tempo
1	Introduzione alla sicurezza	Lezione frontale e partecipata: - Tipologie di attacco - Malware - Ingegneria Sociale - Denial of Service	Videoproiettore, Presentazione, Video, Link Approfondimento	50 min
2	Verifica Formativa, analisi delle risposte e recupero	Test a risposta multipla(15 domande)	Moodle	15 min(Test) 30 min (Discussione)
3	Studio - Esercitazione sulla piattaforma	Test a risposta multipla(lo stesso) Forum, Chat tra gli studenti	Moodle	
4	Verifica Sommativa	Test a risposta multipla(lo stesso) + 3 domande a risposta aperta	Moodle	5 min(Test) 40 min(domande)

Piano di lavoro UD5

Fasi	Articolazione	Strategie e contenuti	Strumenti	Tempo
1	Introduzione alla sicurezza	Lezione frontale e partecipata: Contromisure: - Tipologie, - Efficacia, - Password, - Firewall, - IDS/IPS, - Backup, - Formazione personale	Videoproiettore, Presentazione, Video, Link Approfondimento	50 min
2	Verifica Formativa, analisi delle risposte e recupero	Test a risposta multipla(10 domande)	Moodle	10 min(Test) 20 min (Discussione)
3	Studio - Esercitazione sulla piattaforma	Test a risposta multipla(lo stesso) Forum, Chat tra gli studenti	Moodle	
4	Verifica Sommativa	Test a risposta multipla(lo stesso) + 3 domande a risposta aperta	Moodle	5 min(Test) 40 min(domande)

Piano di lavoro UD6

Fasi	Articolazione	Strategie e contenuti	Strumenti	Tempo
1	Introduzione alla sicurezza	Lezione frontale e partecipata: Crittografia - Lessico - Funzione - Storia(video) - Sistemi a chiave simm .e asimm. - SSL, Certificati, - Firma Digitale - Steganografia	Videoproiettore, Presentazione, Video, Link Approfondimento	85 min
2	Verifica Formativa, analisi delle risposte e recupero	Test a risposta multipla(10 domande)	Moodle	10 min(Test) 20 min (Discussione)
3	Studio - Esercitazione sulla piattaforma	Test a risposta multipla(lo stesso) Forum, Chat tra gli studenti	Moodle	
4	Verifica Sommativa	Test a risposta multipla(lo stesso) + 3 domande a risposta aperta	Moodle	5 min(Test) 40 min(domande)

UD1 : Conoscenze

- Conoscenza delle diverse tipologie di minacce ed i possibili danni, in ambito aziendale, derivanti da attacchi informatici
- Identificazione delle risorse da proteggere
- «Pirati informatici»: distinzione tra Hacker e Cracker, Outsiders e Insiders,evoluzione del crimine informatico

UD1: Competenze

- Saper elencare/illustrare sinteticamente minacce e danni
- Saper illustrare sinteticamente la distinzione Hacker/Cracker, Outsider/Insider, l'evoluzione del crimine informatico
- Saper esporre i contenuti appresi inserendoli in un'analisi organica ed unitaria delle motivazioni alla base della «sicurezza informatica»
- Saper riconoscere, in situazioni reali, presentate dal docente o tratte dall'esperienza dello studente quali sono le potenziali minacce e gli eventuali danni che deriverebbero dalla violazione dei sistemi analizzati

UD2 : Conoscenze

- Definizioni di…
  - Riservatezza,
  - Integrità,
  - Disponibilità,
  - Autenticazione,
  - Tracciabilità,
  - Non ripudio
- Esempi pratici

UD2 : Competenze

- Saper definire cosa si intende per riservatezza, integrità, disponibilità dell'informazione, autenticazione del mittente, non ripudio in ambito informatico presentando gli esempi trattati a lezione
- Saper riconoscere in situazioni reali se i requisiti di riservatezza, ecc… sono soddisfatti o meno.
- Saper presentare casi esemplificativi tratti dall'esperienza quotidiana dello studente.

UD3 : Conoscenze

- Conoscere i passi principali da compiere per la realizzazione di un sistema informatico sicuro:
  - analisi dei rischi,
  - definizione di politiche di sicurezza
  - pianificazione di un Disaster Recovery Plan

UD3 : Competenze

- Saper esporre sinteticamente gli obiettivi dell'analisi dei rischi, delle politiche di sicurezza e di un Disaster Recovery Plan
- Analisi dei rischi: Saper individuare in casi reali(anche se in maniera non approfondita) le risorse da proteggere, i rischi cui sono esposte ed effettuare una stima del livello di gravità dei danni conseguenti
- Politiche Sicurezza: Saper definire politiche di sicurezza in casi semplici attinenti sempre all'esperienza quotidiana dello studente e in casi presentati dal docente attinenti realtà aziendali
- Disaster Recovery Plan: Saper elaborare un piano di ripristino dell'attività in casi

UD4 : Conoscenze

Conoscere in dettaglio le principali tipologie e metodi di attacco…in particolare:

- i vari tipi di malware(worm, virus, trojan, backdoor, spyware, keylogger, adware) e le loro differenze
- l'ingegneria sociale, definizione ed esempi (phishing)
- attacchi di tipo DoS (Denial of Service), definizione e modalità

UD4 : Competenze

- Saper esporre (oralmente o in forma scritta) le principali tipologie e metodi di attacco
- Saper illustrare i principali tipi di malware
- Saper evidenziare le differenze tra i diversi tipi di malware
- Saper riconoscere correttamente i diversi tipi di malware partendo dalle loro caratteristiche
- Saper illustrare cosa si intende per Ingegneria Sociale, delineando le modalità di attacco e fornendo esempi di tecniche comunemente utilizzate
- Saper descrivere genericamente le modalità con cui avviene un attacco Denial of Service, gli obiettivi e gli strumenti

UD4 : Competenze/Abilità

- Saper cogliere nessi logici con le UD precedenti (es. in che modo i malware si riflettono negativamente su riservatezza, integrità, ecc…?)
- Saper rielaborare le conoscenze apprese (es. sapresti immaginare delle strategie per rilevare se un file è stato infettato da un virus o per evitare di essere vittime dell' Ingegneria Sociale?)
- Saper analizzare una situazione problematica (tratta dall'esperienza quotidiana o dall'esperienza dello studente) riconoscendo le possibili vulnerabilità del sistema(es. come potresti accorgerti se il tuo «pc» è stato infettato da un worm?...e da uno spyware? Quali sono i possibili rimedi?)

UD4: Competenze minime

- Saper elencare/illustrare sinteticamente le caratteristiche di **alcuni tipi di malware**
- Saper illustrare cosa si intende per **Ingegneria Sociale**, delineando le modalità di attacco e fornendo esempi di tecniche comunemente utilizzate
- Saper definire le finalità di un attacco **Denial of Service**
- Saper **applicare le conoscenze apprese** in casi reali presentati dal docente(ad es. cosa fare per ridurre la probabilità di essere infettati da un virus)

UD4: Competenze minime e Assi Culturali

- Le competenze sono in parte specifiche all'asse culturale scientifico-tecnologico e all'indirizzo (anche se queste sono definite solo per il **biennio**) ed in parte includono competenze trasversali come la capacità di comprendere un testo

UD4: Interdisciplinarietà

- **Inglese = Video** in lingua originale con sottotitoli e **lessico specifico**, **letture di approfondimento**(Wikipedia)

- **Diritto**: **reati informatici**, **dati sensibili**, **privacy**, **obblighi di legge**,… questi argomenti sono richiamati ed introdotti esplicitamente nelle altre unità didattiche che compongono il corso

Domande a risposta aperta

Conoscenze-Competenze	Domande a risposta aperta
Malware	Descrivi cos'è un…. Virus Informatico / Trojan / Backdoor…
Differenze Malware	Illustra le differenze tra…. Virus e Worm / Trojan / Backdoor…
Ingegneria Sociale, Denial of Service	▪ Cosa si intende per Ingegneria Sociale? Illustra le modalità di attacco e riportane degli esempi ▪ Descrivere genericamente le modalità con cui avviene un attacco Denial of Service

Domande a risposta aperta

Competenze	Domande a risposta aperta
Nessi Logici con Unità Precedenti	▪ **UD1,UD2**: In che modo i malware si riflettono negativamente su riservatezza, integrità, ecc… e quali danni possono provocare in ambito aziendale? ▪ **UD3**: Quali politiche potrebbero essere adottate per prevenire i danni derivanti dai malware? ▪ **UD3**: Quali politiche potrebbero essere adottate per prevenire attacchi di Ingegneria Sociale?
Analisi situazione problematica	▪ come potresti accorgerti se il tuo «pc» è stato infettato da un worm?...e da uno spyware? Quali sono i possibili rimedi? ▪ descrivi delle situazioni tratte dalla vita quotidiana ad alto rischio per la sicurezza informatica…

UD5 : Conoscenze

Conoscere le principali contromisure per rilevare o ridurre il rischio di violazioni informatiche, in particolare per quanto riguarda:

- Sistemi di autenticazione
- Firewall
- IDS e IPS
- Backup
- Formazione del personale

UD5 : Competenze

- Mettere in relazione le tecniche di attacco con le contromisure per contrastarle
- Pianificare le strategie da adottare ai vari livelli per ridurre i rischi/danni legati ad eventuali violazioni della sicurezza in casi reali

UD6 : Conoscenze

- Conoscere la storia, la funzione e le principali tecniche crittografiche(chiave simmetrica e asimmetrica)
- Conoscere il significato dei termini : crittologia, crittografia, crittoanalisi, crittazione, decrittazione, steganografia, ecc…

.

UD6 : Competenze

- Saper definire i termini : crittografia, crittoanalisi, crittazione, decrittazione, messaggio cifrato/criptato, chiave di cifratura/decifratura
- Saper illustrare la differenza tra algoritmi a chiave simmetrica e asimmetrica
- Saper illustrare il funzionamento dei sistemi a chiave asimmetrica(pubblica) e di firma digitale
- Saper tracciare in maniera sintetica l'evoluzione delle tecniche crittografiche
- Saper presentare casi esemplificativi tratti dall'esperienza quotidiana dello studente in cui è utile ricorrere a tali tecniche.