P.E.K.I.T. Security Syllabus rev. 1.0

1 Concetti di base 3

1.1 Concetti di base di sicurezza informatica 3

1.1.1 I principi di base della sicurezza informatica 3

1.1.2 Gestione del rischio 3

1.1.3 Organizzazione della sicurezza 3

1.1.4 Standard ed enti di standardizzazione 3

1.2 Nozioni di base sul funzionamento delle reti 3

1.2.1 Classificare le reti 3

1.2.2 Il modello ISO/OSI 3

1.3 L'hardware di rete 4

1.3.1 I principali tipi di segnale e di mezzo trasmissivo 4

1.3.2 La scheda di rete 4

1.3.3 Gli apparati di connessione 4

1.4 I principali protocolli di rete 4

1.4.1 I protocolli di rete locale 4

1.4.2 L'architettura TCP/IP 5

1.5 Diagnostica di rete e strumenti utili 5

1.5.1 Comandi e funzionalità utilizzati per amministrare la rete 5

2 Gli attacchi informatici 6

2.1 Nozioni generali sugli attacchi informatici 6

2.1.1 la figura dell'hacker 6
2.1.2 Le fasi di un attacco informatico 6
2.2 Il malware 6
2.2.1 Principali tipologie di malware 6
2.2.2 Gli antivirus 6
2.3 Classificazione degli attacchi 6
2.3.1 Le categorie generali di attacco 7
2.3.2 Le principali tecniche di attacco 7
3 Sicurezza informatica 8
3.1 L'utilizzo delle password 8
3.1.1 Scegliere e gestire una password 8
3.1.2 Gli attacchi alle password 8
3.2 Crittografia 8
3.2.1 Le tecniche di crittografia 8
3.2.2 Gestire le chiavi 8
3.2.3 Principali algoritmi di crittografia 8
3.3 Soluzioni di sicurezza in rete 9
3.3.1 I firewall 9
3.3.2 Altri dispositivi di sicurezza 9
4 L'attività di Ethical Hacking 10
4.1 Concetti di base sull'attività di Ethical Hacking 10
4.1.1 Il penetration test 10
4.1.2 Modalità di svolgimento del penetration test 10
4.1.3 Apetti legali, contrattuali e normative 10
4.1.4 I report relativi all'attività svolta 10
4.2 Strumenti utilizzati nelle attività di penetration test 10
4.2.1 Le distribuzioni Linux dedicate al penetration test 10
4.2.2 I principali programmi utilizzati per le attività di penetration test 10

1 Concetti di base

1.1 Concetti di base di sicurezza informatica

1.1.1 I principi di base della sicurezza informatica

1.1.1.1 Riservatezza

1.1.1.2 Integrità

1.1.1.3 Disponibilità

1.1.1.4 Autenticazione

1.1.2 Gestione del rischio

1.1.2.1 Analisi del rischio

1.1.2.2 Controllo e contromisure

1.1.3 Organizzazione della sicurezza

1.1.3.1 Le politiche di sicurezza

1.1.3.2 I processi

1.1.3.3 Le responsabilità

1.1.4 Standard ed enti di standardizzazione

1.1.4.1 I principali enti e il loro ruolo

1.1.4.2 Normative relative alla sicurezza

1.2 Nozioni di base sul funzionamento delle reti

1.2.1 Classificare le reti

1.2.1.1 Commutazione di circuito ei di pacchetto

1.2.1.2 L'estensione di una rete: LAN, MAN, WAN, etc.

1.2.1.3 La topologia di rete: reti a bus, ad anello, a stella, a maglia, etc.

1.2.1.4 Architettura client/server e peer-to-peer

1.2.2 Il modello ISO/OSI

1.2.2.1 La suddivisione in strati

1.2.2.2 L'incapsulamento dei messaggi

1.2.2.3 Il livello fisico

1.2.2.4 Il livello di collegamento dati

1.2.2.5 Il livello di rete

1.2.2.6 Il livello di trasporto

1.2.2.7 Il livello di sessione

1.2.2.8 Il livello di presentazione

1.2.2.9 Il livello applicativo

1.3 L'hardware di rete

1.3.1 I principali tipi di segnale e di mezzo trasmissivo

1.3.1.1 Il cavo coassiale

1.3.1.2 Il doppino ritorto

1.3.1.3 La fibra ottica

1.3.1.4 Onde radio e microonde

1.3.2 La scheda di rete

1.3.2.1 La funzione della scheda di rete

1.3.2.2 L'indirizzo fisico della scheda di rete (indirizzo MAC)

1.3.3 Gli apparati di connessione

1.3.3.1 Il modem

1.3.3.2 L'hub e il repeater

1.3.3.3 Il bridge e lo switch

1.3.3.4 L'access point

1.3.3.5 Il router

1.4 I principali protocolli di rete

1.4.1 I protocolli di rete locale

1.4.1.1 Lo standard Ethernet

1.4.1.2 Le reti Wi-fi

1.4.2 L'architettura TCP/IP

1.4.2.1 Gli strati dell'architettura TCP/IP

1.4.2.2 Il protocollo IP

1.4.2.3 Gli indirizzi IP

1.4.2.4 Dall'indirizzo IP all'indirizzo MAC: il protocollo ARP

1.4.2.5 Il protocollo TCP

1.4.2.6 Il protocollo TCP

1.4.2.7 I numeri di porta

1.4.2.8 La configurazione dinamica degli host: DHCP

1.4.2.9 I nomi di dominio e la loro risoluzione: il sistema DNS

1.4.2.10 Il protocollo http e il web

1.4.2.11 I protocolli della posta elettronica

1.4.2.12 FTP e il trasferimento dei file

1.5 Diagnostica di rete e strumenti utili

1.5.1 Comandi e funzionalità utilizzati per amministrare la rete

1.5.1.1 Il comando ping

1.5.1.2 I comandi ipconfing e ifconfig

1.5.1.3 Il comando traceroute

1.5.1.4 Utilizzare la funzione Gestione attività in Windows

1.5.1.5 Il registro di Windows

2 Gli attacchi informatici

2.1 Nozioni generali sugli attacchi informatici

2.1.1 la figura dell'hacker

2.1.1.1 Conoscenze, competenze e attitudini di un hacker

2.1.1.2 White hat, gray hat e black hat

2.1.1.3 Cracker, script kiddies, phreaker, hacktivist

2.1.2 Le fasi di un attacco informatico

2.1.2.1 Raccogliere le informazioni sul target

2.1.2.2 Valutare le vulnerabilità

2.1.2.3 Ottenere l'accesso al sistema

2.1.2.4 Scalare i privilegi

2.1.2.5 Coprire le tracce

2.2 Il malware

2.2.1 Principali tipologie di malware

2.2.1.1 Virus e Worm

2.2.1.2 I cavalli idi troia

2.2.1.3 Spyware e keylogger

2.2.1.4 I rootkit

2.2.1.5 I ramsonware

2.2.2 Gli antivirus

2.2.2.1 Principi di base del funzionamento degli antivirus

2.2.2.2 Installare configurare e aggiornare un antivirus

2.3 Classificazione degli attacchi

2.3.1 Le categorie generali di attacco

2.3.1.1 Il buffer overflow

2.3.1.2 Cos'è un exploit

2.3.1.3 Gli attacchi zero-day

2.3.1.4 Il concetto di spoofing

2.3.1.5 Gli attacchi DOS (Denial of Service)

2.3.1.6 Gli attacchi Man-in-the-middle

2.3.1.7 Lo sniffing

2.3.1.8 Il code injection

2.3.1.9 Il port scanning

2.3.1.10 L'ingegneria sociale

2.3.2 Le principali tecniche di attacco

2.3.2.1 ARP poisoning

2.3.2.2 DNS cache poisoning

2.3.2.3 Ping of death

2.3.2.4 Syn flooding

2.3.2.5 Smurfing

2.3.2.6 SQL injectio

2.3.2.7 Cross-site scripting

2.3.2.8 Phishing

2.3.2.9 War-dialing

2.3.2.10 War-driving

3 Sicurezza informatica

3.1 L'utilizzo delle password

3.1.1 Scegliere e gestire una password

3.1.1.1 Lunghezza di una password

3.1.1.2 L'alfabeto dei caratteri delle password

3.1.1.3 Annotare e memorizzare una password

3.1.1.4 Necessità di modificare la password e frequenza di cambiamento

3.1.2 Gli attacchi alle password

3.1.2.1 Attacco a forza bruta

3.1.2.2 Attacco a dizionario

3.1.2.3 Spyware keylogger e sniffer

3.2 Crittografia

3.2.1 Le tecniche di crittografia

3.2.1.1 Crittografia simmetrica

3.2.1.2 Crittografia asimmetrica

3.2.1.3 Le funzioni di hash

3.2.2 Gestire le chiavi

3.2.2.1 Metodi di distribuzione delle chiavi segrete nella crittografia simmetrica

3.2.2.2 L'infrastruttura a chiave pubblica (PKI)

3.2.2.3 Le Certification Authority e i certificati digitali

3.2.2.4 PGP

3.2.2.5 I servizi di directory e LDAP

3.2.2.6 Sicurezza delle chiavi, crittoanalisi e possibili attacchi

3.2.3 Principali algoritmi di crittografia

3.2.3.1 I principali algoritmi simmetrici: DES, 3DES, AES, etc.

3.2.3.2 I principali algoritmi asimmetrici: RSA, DSS, etc.

3.2.3.3 I principali algoritmi di hash: MD5, SHA, etc.

3.3 Soluzioni di sicurezza in rete

3.3.1 I firewall

3.3.1.1 Tipi di firewall

3.3.1.2 Architetture basate su firewall

3.3.2 Altri dispositivi di sicurezza

3.3.2.1 IDS e IPS

3.3.2.2 I proxy

3.3.2.3 Le VPN

4 L'attività di Ethical Hacking

4.1 Concetti di base sull'attività di Ethical Hacking

4.1.1 Il penetration test

4.1.1.1 Natura e scopo del penetration test

4.1.1.2 Differenza tra penetration test e vulnerability assessment

4.1.2 Modalità di svolgimento del penetration test

4.1.2.1 Test overt e covert

4.1.2.2 Gli approcci black box (zero-knowledge), gray box (partial-knowledge) e white box (full-knowledge)

4.1.3 Apetti legali, contrattuali e normative

4.1.3.1 Le regole d'ingaggio

4.1.3.2 Gli obiettivi

4.1.3.3 Pianificazione temporale

4.1.3.4 Rischi associati all'attività di penetration test

4.1.3.5 Responsabilità dell'attività di penetration test

4.1.4 I report relativi all'attività svolta

4.1.4.1 Caratteristiche generali della reportistica fornita

4.1.4.2 L'executive summary

4.1.4.3 Il report tecnico

4.2 Strumenti utilizzati nelle attività di penetration test

4.2.1 Le distribuzioni Linux dedicate al penetration test

4.2.1.1 Caratteristiche delle diverse distribuzioni dedicate al penetration test

4.2.2 I principali programmi utilizzati per le attività di penetration test

4.2.2.1 Strumenti, programmi e comandi utilizzati per raccogliere informazioni sul target

4.2.2.2 Gli scanner di vulnerabilità

4.2.2.3 Gli strumenti di exploiting

4.2.2.4 Strumenti utilizzati per gli attacchi alle password

4.2.2.5 Strumenti utilizzati per testare le applicazioni web

4.2.2.6 Strumenti utilizzati per testare le infrastrutture (sistemi VOIP, reti wireless e dispositivi hardware

4.2.2.7 Strumenti utilizzati per testare i dispositivi mobili