CYBERBOOK

Il glossario di sicurezza cibernetica

PRESIDENZA DEL CONSIGLIO DEI MINISTRI

Sistema di informazione per la sicurezza della Repubblica

CYBERBOOK

Il glossario di sicurezza cibernetica

Estratto dal videogioco

“CYBERCITY CHRONICLES"

A

Accesso Root
Root in inglese significa “radice”, è utilizzato nei sistemi operativi per indicare l’utente che ha i diritti di amministratore. L'utente con il permesso di “Accesso Root” è dunque l'utente che dispone del massimo controllo sul sistema, ed è il solo che può compiere operazioni non consentite ad altri utenti standard.

Agente
Termine che indica sia un appartenente ad un servizio di informazione (Sicurezza Nazionale), quanto un soggetto esterno da questo reclutato, addestrato ed impiegato per operare a suo favore.

AI
Abbreviazione di Artificial Intelligence (Intelligenza Artificiale), disciplina che si occupa dello studio di funzioni tipiche dell’intelligenza umana e della loro possibile replicazione mediante metodi e strumenti informatici.

Algoritmo
Procedimento che consente la risoluzione di problemi di carattere logico e matematico, o pratico.

Antivirus
Software che riconosce la presenza di virus informatici nei file e nelle memorie di massa e cerca di rimuoverli o di neutralizzarli.

APT
(Advanced Persistent Threat). Minaccia consistente in un attacco mirato, volto ad installare una serie di malware all’interno delle reti bersaglio, al fine di riuscire a mantenere attivi i canali impiegati per la fuoriuscita di informazioni pregiate dalle infrastrutture IT del target.

Area Controllata
Area predisposta in prossimità di un’area riservata, dove possono essere trattate solo informazioni classificate a livello RISERVATO. Deve essere dotata di misure di protezione tali da consentire l’accesso alle sole persone autorizzate per motivi attinenti al loro impiego, incarico o professione.

Attacco DDoS
Un attacco combinato di numerose macchine pensato per portare al collasso siti web o server, la maggior parte delle volte condotto per mezzo di Botnet

Attribution
Termine che identifica l’attribuzione di un attacco cyber come, ad esempio, una campagna di cyber-spionaggio, ad un determinato attore ostile.

Avatar
Identità fittizia, soprannome, immagine virtuale in rete.

B

Backdoor
In inglese indica la porta di servizio, quella di solito sul retro di un edificio. Viene chiamato così un sistema, spesso nascosto, utilizzato per aggirare la normale procedura di autenticazione a un sistema informatico e ottenerne l'accesso. In alcuni casi le backdoor sono installate volutamente dall'amministratore del sistema per agevolarne la manutenzione in caso di problemi. Spesso però vengono installate furtivamente e utilizzate da hacker per poter continuare ad avere accesso al sistema che hanno compromesso.

Backup
Salvataggio, totale o parziale, dei contenuti di una memoria.

Blue Box
La "scatola blu" è storicamente uno dei primi strumenti usati per "violare" i sistemi telefonici, sfruttando la tecnologia e le falle di sicurezza degli stessi.
Si trattava di un dispositivo elettronico che emetteva segnali sonori, o "toni", corrispondenti ai messaggi di segnalazione, e questi venivano mandati direttamente sulla linea telefonica. L'uso più comune che veniva fatto era per telefonare gratuitamente. Tramite la blue box era infatti possibile alterare la segnalazione tra le centrali telefoniche, e dirottare la chiamata verso la destinazione desiderata pur chiamando un numero differente. In questo modo veniva ingannato il sistema di tariffazione del gestore telefonico. Un famoso hacker delle linee telefoniche era "Captain Crunch", che aveva ottenuto originariamente questo risultato con un fischietto omaggio nelle scatole dei cereali Cap'n Crunch (da cui deriva il suo nickname).

Bot
Programmi che sono in grado di riprodurre il comportamento umano on-line come, ad esempio, popolare un profilo social ed inviare messaggi in una chat.

Botnet
Una rete di computer utilizzata per attacchi da remoto formata da computer infetti spesso appartenenti a persone inconsapevoli e gestiti a distanza. Tali macchine infettate nel gergo vengono o chiamate zombie.

Bring Your Own Device (BYOD)
Insieme di policy interne ad un'or- ganizzazione, sia essa pubblica o privata, volte a regolare l'impiego di dispositivi digitali personali all'interno della stessa, da parte dei relativi dipendenti.

Bug
Errore in una procedura informatica.

Buonsenso (riferito all'utilizzo della rete)
Nel contesto della sicurezza informatica e dell'utilizzo della rete, si riferisce all'applicazione di una serie di buone pratiche e norme di base che hanno la finalità di prevenire, attutire, contrastare i rischi connessi al mondo online e agli attacchi informatici.

C

Changelist
Rappresenta l'elenco di modifiche effettuate da uno sviluppatore nell'aggiornare un software.

Codice
Si parla di codice per indicare dati che rappresentano istruzioni che un computer può eseguire.Tutto ciò che viene eseguito da un computer o da uno smartphone, ad esempio un'app, è compost da codice!

Codice Sorgente
Il codice sorgente o semplicemente sorgente è il testo di un algoritmo scritto dal programmatore in un qualsiasi linguaggio di programmazione. Si chiama sorgente perché è da qui che si parte per ottenere il programma o l'app desiderata.

Codice malevolo
Si parla di codice malevolo per indicare una serie di dati che rappresentano istruzioni potenzialmente dannose.

Confidence Building Measure (CBM)
Serie di azioni volte a prevenire possibili escala- tion derivanti da operazioni condotte nello spazio cibernetico.

Consapevolezza digitale
Prestare attenzione in maniera peculiare, piena conoscenza e capacità di utilizzo e gestione delle tecnologie IT e dei social media. Si veda la campagna e le iniziative avviate dalla Presidenza del Consiglio con il marchio "Be Aware Be Digital".

Criptovalute
Valute digitali che si basano sulla crittografia sia per la loro generazione, sia per la convalida delle transazioni.

Crisi Cibernetica Nazionale
Situazione in cui l'evento assume dimensioni, intensità o natura tali da incidere sulla sicurezza nazionale o da non poter essere fronteggiato dalle singole Amministrazioni

competenti in via ordinaria, ma con l'assunzione di decisioni coordinate in sede interministeriale.

CRITTOGRAFIA
Tecnica che permette di nascondere il contenuto di un messaggio. Ciò in modo che esso possa essere correttamente compreso solo da chi ne possiede la chiave di decifrazione.

CSIRT (*Computer Security Incident Response Team*)
Unità organizzativa deputata a coordinare la risposta ad incidenti informatici, a mitigarne gli effetti ed a prevenire il verificarsi di ulteriori eventi.

CYBER-ATTACCO
Si riferisce ad una manovra di attacco informatico da parte di uno o più individui verso un sistema, con la finalità di accedere, modificare, distruggere o rubare informazioni e dati.

CYBER-BULLISMO
Manifestazione in rete di un fenomeno piu ampio e meglio conosciuto come bullismo. Quest'ultimo e caratterizzato da azioni violente e intimidatorie esercitate da un bullo, o un gruppo di bulli, su una vittima. Le azioni possono riguardare molestie verbali, aggressioni fisiche, persecuzioni, generalmente attuate in ambiente scolastico. Oggi la tecnologia consente ai bulli di infiltrarsi nelle case delle vittime, di materializzarsi in ogni momento della loro vita, perseguitandole con messaggi, immagini, video offensivi inviati tramite smartphone o pubblicati sui siti web tramite Internet. Il bullismo diventa quindi cyberbullismo. Il cyberbullismo definisce un insieme di azioni aggressive e intenzionali, di una singola persona o di un gruppo, realizzate mediante strumenti elettronici (sms, mms, foto, video, email, chat rooms, istant messaging, siti web, telefonate), il cui obiettivo e quello di provocare danni ad un coetaneo incapace a difendersi.

CYBER-CRIME
Qualsiasi reato o comportamento delittuoso svolto nell'ambito delle procedure informatiche.

CYBER-DEFENSE
L'insieme della dottrina, dell'organizzazione e delle attività volte a prevenire, rilevare, limitare e contrastare gli effetti degli attacchi condotti nel e tramite il cyber-space ovvero in danno di uno o più dei suoi elementi costitutivi.

CYBER-SECURITY
Condizione in cui il cyber-space risulti protetto rispetto ad eventi, di natura volontaria od accidentale, consistenti nell'acquisizione e nel trasferimento indebiti di dati, nella loro modifica o distruzione illegittime ovvero nel blocco dei sistemi informativi, grazie ad idonee misure di sicurezza fisica, logica e procedurale.

Cyber-space (cyberspazio)
L'insieme delle infrastrutture informatiche interconnesse, comprensivo di hardware, software, dati ed utenti nonché delle relazioni logiche, comunque stabilite, tra di essi. Include tra l'altro internet, reti di comunicazione, sistemi attuatori di processo ed apparecchiature mobili dotate di connessione di rete.

Cyber-war
L'insieme delle operazioni condotte nel e tramite il cyber-space al fine di negare all'avversario – statuale o non – l'uso efficace di sistemi, armi e strumenti informatici o comunque di infrastrutture e processi da questi controllati. Include anche attività di difesa e "capacitanti" (volte cioè a garantirsi la disponibilità e l'uso del cyber-space).

D

Dark Web
Contenuti del web nelle darknet (reti oscure) che possono essere raggiunti esclusivamente con software specifici.

Data Breach
Violazione dei dati: nel campo della sicurezza informatica si riferisce alla violazione della sicurezza dei dati, che può avvenire per errore o intenzionalmente, mediante la distruzione, la perdita, la modifica, la divulgazione o l'accesso ai dati personali di uno o più persone.

Deep Web (web profondo)
Porzione di Internet che non viene indicizzata dai tradizionali motori di ricerca.

Disinformazione
Diffusione di notizie infondate o distorte al fine di danneggiare l'immagine pubblica di un avversario e/o di influenzarne le scelte.

Distributed Denial of Service (DDoS)
Attacco DoS lanciato da un gran numero di sistemi compromessi ed infetti (botnet), volto a rendere un sistema informatico o una risorsa non disponibile ai legittimi utenti attraverso la saturazione delle risorse ed il sovraccarico delle connessioni di rete dei sistemi server.

DNS Poisoning
Noto anche come DNS Cache Poisoning, è la compromissione di un server Domain Name System (DNS) comportante la sostituzione dell'indirizzo di un sito legittimo con quello di un altro sito, ad esempio, infettato dall'attaccante.

Doxing
Deriva dall'inglese "documents", abbreviato in "dox", ed è la pratica di diffondere pubblicamente online le informazioni private e sensibili di una persona.

E

Encryption/crittografia
E' la conversione di dati in una forma che può essere decodificato solo da chi possiede una chiave di lettura o da chi è in grado di violare il meccanismo di cifratura.

Exploit
Una porzione di "codice" che sfruttando una vulnerabilità permette, nelle dovute circostanze e con le giuste capacità, di accedere ad un sistema informatico.

F

False Flag
Si tratta di operazioni, generalmente condotte nello spazio cibernetico ma non solo, poste in essere usando cautele tali da indurre l'avversario in errore circa la reale riconducibilità delle stesse ad uno specifico attore ostile.

Fattore Umano
La sicurezza informatica è caratterizzata dalla presenza di una serie di componenti hardware e software. Con la dicitura "Fattore Umano" in questo contesto ci si rivolge ad un altro importante aspetto della catena della sicurezza informatica stessa: la presenza dell'uomo. L'intervento dell'uomo è infatti presente e determinante sia dal lato di chi ha intenzioni malevole, come ad esempio un Hacker, sia da parte di chi protegge i propri dati, o scrive programmi utilizzati nell'ambito della sicurezza. In tema di difesa dagli attacchi da parte degli Hacker, l'insieme delle buone norme di condotta da adottare da parte degli individui o delle organizzazioni è un aspetto cruciale per prevenire o attenuare le conseguenze degli attacchi stessi.

Firewall
Dall'inglese "porta antincendio" è un dispositivo che permette di proteggere reti informatiche da accessi indesiderati, ma come tutte le tecnologie a volte è possibile aggirarla!

Firmware
Firmware deriva da "firm" e "software", ovvero componente software permanente, ed è un insieme di istruzioni integrate direttamente in un componente elettronico programmato, che consentono ad un dispositivo di avviarsi e di interagire con altri dispositivi. Pur trattandosi di istruzioni permanenti, i dispositivi moderni permettono l'aggiornamento del firmware.

Follower
Nei Social Network, chi decide di seguire, come in Twitter, le comunicazioni di un utente, diventandone seguace.

Flamer
Deriva dal termine inglese “flame”, fiamma. Nel gergo di Internet è chi “infiamma” le discussioni online provocando litigi.

Ftp
Il File Transfer Protocol (FTP), è un protocollo Internet che facilita il caricamento o il download di file digitali.

G

GDPR
A partire dal 25 maggio 2018 è direttamente applicabile in tutti gli Stati membri europei il Regolamento Ue 2016/679, noto come GDPR (General Data Protection Regulation) – relativo alla protezione delle persone fisiche con riguardo al trattamento e alla libera circolazione dei dati personali.

H

Hacker
Di per se l’hacker non è ne buono ne cattivo, si tratta solo di persone, ragazze, ragazzi estremamente curiose, capaci di studiare e scoprire cose nuove, nonché utilizzi “diversi” di ciò che si trovano davanti, in italiano potrebbero essere chiamati “smanettoni”. Di solito vengono suddivisi in black o white hat a seconda se siano “hacker buoni” o “hacker cattivi”, ma è una definizione che ai veri hacker non piace!

Hacktivista
Termine che deriva dall’unione di due parole, hacking e activism e indica chi pone in essere le pratiche dell’azione diretta digitale in stile hacker. Nell’ambito dell’hacktivism le forme dell’azione diretta tradizionale sono trasformate nei loro equivalenti elettronici, che si estrinsecano prevalentemente, ma non solo, in attacchi DDoS e web defacement.

Hater
Proviene dal verbo inglese “to hate”, odiare. E’ un termine usato su Internet per indicare gli utenti che di solito disprezzano, diffamano o criticano una persona con intento distruttivo.

HTTP
L'HyperText Transfer Protocol (HTTP), ovvero il protocollo di trasferimento di un ipertesto, è un protocollo, uno standard, usato come principale sistema per trasferire informazioni sul web.
L'HTTP si basa su un sistema di comunicazione tra “client” e “server”: il client esegue una richiesta e il server restituisce la risposta. Nell'uso comune il client

corrisponde al browser con cui si naviga su internet (ad esempio Chrome, Edge, Firefox, Opera, Safari), il server è la macchina su cui risiede il sito web.

HTTPS
Aggiungendo una "S", che racchiude il significato di Sicurezza, al protocollo HTTP, otteniamo l'HTTPS. Questo è infatti protocollo per la comunicazione attraverso una rete di computer utilizzato su Internet, all'interno di una connessione sicura, criptata. HTTPS permette di verificare che il sito visitato sia autentico, fornisce una protezione maggiore della privacy e garantisce che i dati scambiati tra l'utente e il sito web non vengano intercettati o manomessi.

I

Indicators of Compromise (IoC)
Indicatori impiegati per la rilevazione di una minaccia nota e generalmente riconducibili ad indirizzi IP delle infrastrutture di Comando e Controllo (C&C), hash (MD5, SHA1, ecc.) e moduli del malware (librerie, dropper, ecc.).

Indirizzo IP
E' un codice univoco, composto da quattro set di cifre comprese tra 0 e 255 che identifica ogni dispositivo direttamente connesso ad internet.

Industrial Control System (ICS)
I sistemi di controllo industriale includono i sistemi di controllo di supervisione e acquisizione dei dati (Supervisory Control and Data Acquisition-SCADA), i sistemi di controllo distribuiti (Distributed Control Systems-DCS) e i controllori a logica programmabile (Programmable Logic Controller-PLC), impiegati usualmente negli impianti industriali.

Ingegneria sociale
Tecniche di manipolazione psicologica affinché l'utente compia determinate azioni o riveli informazioni sensibili come, ad esempio, credenziali di accesso a sistemi informatici.

Internet of Things (IoT)
Neologismo riferito all'interconnessione degli oggetti tramite la rete Internet, i quali possono così comunicare dati su se stessi e accedere ad informazioni aggregate da parte di altri, offrendo un nuovo livello di interazione. I campi di impiego sono molteplici: dalle applicazioni industriali (processi produttivi), alla logistica e all'infomobilità, o all'efficienza energetica, all'assistenza remota, alla tutela ambientale e alla domotica.

IT
Information Technology (tecnologia dell'informazione), ossia l'insieme di tutte le tecnologie che afferiscono al trattamento dell'informazione, normalmente inteso come trattamento digitale dell'informazione.

K

KEYLOGGER
È uno strumento che permette di registrare tutto ciò che viene digitato su una tastiera all'insaputa della vittima.

L

LANDING PAGE
Landing Page E' la pagina che il visitatore raggiunge dopo aver cliccato un link o una pubblicità.

LINK
Un tipo di collegamento attivo, agendo sul quale si viene automaticamente rimandati a una ulteriore informazione o approfondimento.

LINUX
E' il più diffuso sistema operativo libero. Modificabile e distribuibile liberamente. In poche parole il sistema operativo preferito da hacker, scienziati, smanettoni e da chiunque si occupi di sicurezza informatica, per essere precisi andrebbe chiamato GNU/Linux.

LOGIN
Procedura con cui si accede a una sezione riservata di un sito Internet.

M

MALWARE
Software pirata inserito in un sistema informatico, generalmente in modo clandestino, con l'intenzione di compromettere la riservatezza, l'integrità o la disponibilità dei dati, delle applicazioni o dei sistemi operativi dell'obiettivo.

MINACCIA CIBERNETICA
Espressione impiegata per indicare l'insieme delle condotte controindicate che possono essere realizzate nel e tramite il cyber-space ovvero in danno di quest'ultimo e dei suoi elementi costitutivi. Si sostanzia in attacchi cibernetici: azioni di singoli individui o organizzazioni, statuali e non, finalizzate a distruggere, danneggiare o

ostacolare il regolare funzionamento dei sistemi e delle reti e/o dei sistemi attuatori di processo da essi controllati, ovvero a violare integrità e riservatezza di dati/ informazioni.

N

Netiquette
L'insieme delle regole del corretto comportamento degli utenti in rete. Mira a garantire il corretto scambio di dati e informazione nel rispetto delle norme di civiltà e dell'opinione altrui.

Noob
Abbreviazione di newbie, ovvero di chi è alle prime armi! Attenzione a non farla passare per un'offesa, tutti nella vita sono passati per essere dei noob!

O

Open Source
E' quel software di cui è disponibile il codice sorgente, questo a differenza della maggior parte dei programmi commerciali. Viene chiamato più precisamente "Software Libero" perché risulta liberamente consultabile, modificabile e ridistribuibile da tutti gli utenti. Ricorda sempre: "Sharing is caring!"

P

Password
Sequenza di caratteri nota solo al legittimo proprietario: la sua introduzione consente l'accesso a parti di programmi o di siti, confermando che il richiedente ha le abilitazioni necessarie.

Phishing
Attacco informatico avente, generalmente, l'obiettivo di carpire informazioni sensibili (userid, password, numeri di carte di credito, PIN) con l'invio di false email generiche a un gran numero di indirizzi. Le email sono congegnate per convincere i destinatari ad aprire un allegato o ad accedere a siti web fake. Il phisher utilizza i dati acquisiti per acquistare beni, trasferire somme di denaro o anche solo come "ponte" per ulteriori attacchi.

Proxy
E' un server che può essere usato per mascherare il proprio IP.

Q

QR Code
Codice a barre bidimensionale (o codice 2D), ossia a matrice, impiegato per memorizzare informazioni generalmente lette attraverso un mobile o uno smartphone. Ma è anche uno strumento di Mobile Marketing che consente di ottenere in modo continuo nuovi flussi di contatti qualificati e targhettizzati.

R

Ransomware
Malware che cripta i file presenti sul computer della vittima, richiedendo il pagamento di un riscatto per la relativa decrittazione. I ransomware sono, nella maggioranza dei casi, dei trojan diffusi tramite siti web malevoli o compromessi, ovvero per mezzo della posta elettronica. Questi si presentano come allegati apparentemente innocui (come, ad esempio, file PDF) provenienti da mittenti legittimi (soggetti istituzionali o privati). Tale elemento induce gli ignari utenti ad aprire l'allegato, il quale riporta come oggetto diciture che richiamano fatture, bollette, ingiunzioni di pagamento ed altri oggetti similari.

Reverse engineering
E' un processo che letteralmente significa ingegneria inversa, e consiste nell'analizzare dettagliatamente il funzionamento di un oggetto, come ad esempio un dispositivo, un componente digitale o un software, al fine di ottenere tutte le informazioni necessarie per produrre un nuovo dispositivo o software che abbia un funzionamento simile a quello originario.

Rootkit
Software malevolo, a volte molto sofisticato, capace di accedere ad un computer e garantire l'accesso all'attaccante, aggirare il controllo da parte dell'amministratore di sistema riuscendo anche a nascondere la propria presenza.

S

Script kiddie
Pur non essendo legato direttamente all'età della persona, Script Kiddie deriva da "programma" (script), e "ragazzo" (kid) in inglese, ed è un termine dispregiativo che indica quelle persone che usano codici o appunto programmi, scritti in gran parte da altri, per far credere di essere esperti di informatica.

Sniffing
Si chiama così quell'attività che prevede di "intercettare" i dati che passano su una rete, comprese comunicazioni, password

Sicurezza Nazionale
Condizione in cui ad un paese risultino garantite piene possibilità di sviluppo pacifico attraverso la salvaguardia dell'intangibilità delle sue componenti costitutive, dei suoi valori e della sua capacità di perseguire i propri interessi fondamentali a cospetto di fenomeni, condotte ed eventi lesivi o potenzialmente tali. È un bene costituzionale che gode di tutela prioritaria.

Smartphone
Tipo di telefono cellulare che, oltre alle funzioni di telefono, integra la gestione di dati personali, il collegamento a Internet, la posta elettronica, ecc.

Social Engineering
Arte di manipolare psicologicamente le persone affinché compiano determinate azioni o rivelino informazioni confidenziali, come le credenziali di accesso a sistemi informatici.

Spam
Messaggi di posta elettronica indesiderati, generalmente pubblicitari o malevoli.

Spear-Phishing
Attacco informatico di tipo phishing condotto contro utenti specifici mediante l'invio di email formulate con il fine di carpire informazioni sensibili dal destinatario ovvero di indurlo ad aprire allegati o link malevoli.

Spoofing
Manipolazione di dati telematici quali l'indirizzo IP o l'email del mittente, così come l'estensione di file, tali da farli apparire innocui o, comunque, provenienti da soggetti noti o che non generano sospetti.

Spyware
Tipo di software malevolo che "spia" le attività in rete di un utente per carpirne codici, azioni, ecc.

SQL injection
Tecnica mirata a colpire applicazioni web che si appoggiano su database programmati con linguaggio SQL, tramite lo sfruttamento di vulnerabilità quali l'inefficienza dei controlli sui dati ricevuti in input e l'inserimento di codice malevolo all'interno delle query. Tali attacchi consentono di accedere alle funzioni di amministrazione del sistema oltre che di sottrarre o alterare i dati.

Stuxnet
E' un virus informatico creato e diffuso nel 2006. Consisteva in una serie di attacchi digitali contro l'Iran. Lo scopo del software era il sabotaggio della centrale nucleare

iraniana di Natanz. Il sabotaggio avveniva facendo girare le centrifughe della centrale ad una velocità eccessiva per disabilitarle, impedendo l'individuazione dell'anomalia.

T

TAG RFID

Radio Frequency IDentification: è un dispositivo senza fili e senza batterie, contenente informazioni di vario genere, lo si può trovare nelle carte di credito per pagare contact-less o nei biglietti dell'autobus. Con un opportuno dispositivo è possibile leggere e/o modificare le informazioni contenute al suo interno.

TYPOSQUATTING

Consiste nella registrazione a dominio di un nome molto simile a quello di un dominio noto. La differenza è di solito minima e concepita in maniera tale da non essere graficamente distinguibile dall'utente (ad esempio, la "l" minuscola è spesso sostituita dal numero "1").

TROJAN

Tipo di software malevolo, che si annida nel PC ospite camuffandosi da programma innocuo, come il mitico Cavallo di Troia, che fu portato all'interno delle mura della città, causandone la distruzione.

TROLL

Nelle leggende scandinave il troll è un abitante demoniaco di boschi, montagne, luoghi solitari: è l'equivalente dell'"orco" di altre tradizioni popolari europee.
Nel gergo di Internet, il troll è l'utente di una comunità virtuale che intralcia il normale svolgimento di una discussione inviando messaggi provocatori, irritanti o fuori tema.

U

UNDERGROUND

Con tale termine si intende l'ambiente, solitamente digi- tale, frequentato per l'acquisto o la condivisione di strumenti di hacking.

URL

Sequenza di caratteri che identifica in modo univoco l'indirizzo in Internet di una pagina, di un documento o di una risorsa.

USERNAME

Il nome identificativo dell'utente che è normalmente visibile, diversamente dalla password.

V

VIRUS
Software malevolo che può infestare un PC, inserendosi in un programma applicativo, causando danni diretti o indiretti, e che può propagarsi da questo ad altri PC tramite file condivisi, email, ecc.

VOIP (VOICE OVER IP)
Protocollo che permette la trasmissione in Internet, con protocollo IP, della voce. Permette di ottenere la fonia su Internet.

W

WEB
Servizio di Internet che permette di navigare e di usufruire dei contenuti multimediali della Rete.

WEB DEFACEMENT (defacciare)
Attacco condotto contro un sito web e consistente nel modificare i contenuti dello stesso limitatamente alla homepage ovvero includendo anche le sottopagine del sito.

WEBMASTER
In un sito Internet, il responsabile del corretto funzionamento del sito e dei suoi contenuti.

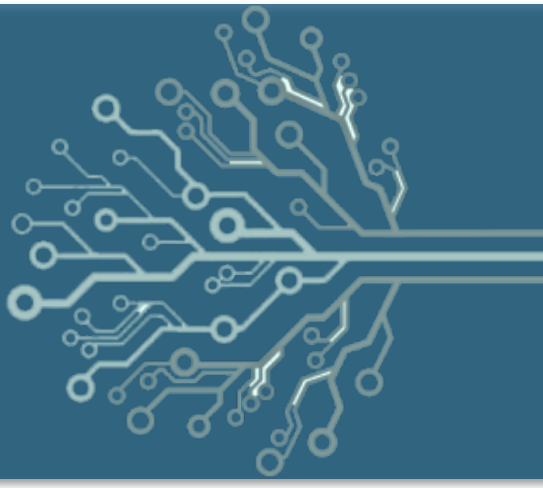
WHITE - GREY - BLACK HAT
Viene definito “white hat”, un hacker, un esperto di programmazione e sicurezza informatica, in grado di introdursi nei sistemi di reti con l’obiettivo di aiutare i proprietari di quel sistema a scoprire eventuali falle nell’accesso, valutarne l’affidabilità, e risolvere potenziali problemi di sicurezza, rispettando dunque l'etica degli hacker. Si può definire dunque a tutti gli effetti un “hacker buono”.
Il white hat si contrappone a chi si introduce illegalmente nei sistemi informatici con l’obiettivo di appropriarsi illecitamente di informazioni o provocare un danno, che viene definito “black hat”.
Una figura intermedia tra white hat e black hat è invece il “grey hat”, che ha l’inclinazione a violare le leggi e l’etica, ma non ha l’intento doloso tipico del “black hat”.

WIRELESS
Sistema di comunicazioni senza fili.

Z

Zero Day

Con questo termine (o 0-day) si indica una minaccia informatica che sfrutta vulnerabilità di applicazioni software non ancora divulgate o per le quali non è ancora stata distribuita una patch. Gli attacchi zero-day sono considerati una minaccia molto grave, in quanto sfruttano falle di sicurezza per le quali non è al momento disponibile nessuna soluzione.



PRESIDENZA DEL CONSIGLIO DEI MINISTRI

SISTEMA DI INFORMAZIONE
PER LA SICUREZZA DELLA REPUBBLICA

WWW.SICUREZZANAZIONALE.GOV.IT