PENETRATION TEST
Processo operativo di valutazione della sicurezza di un sistema o di una rete che simula l'attacco di un utente malintenzionato. L'analisi comprende più fasi ed ha come obiettivo evidenziare le debolezze della piattaforma fornendo il maggior numero di informazioni sulle vulnerabilità che ne hanno permesso l'accesso non autorizzato. L'analisi è condotta dal punto di vista di un potenziale attaccante e consiste nello sfruttamento delle vulnerabilità rilevate al fine di ottenere più informazioni possibili per accedere indebitamente al sistema.

WEB SERVICE
Componente applicativo, un sistema software in grado di mettersi al servizio di un' applicazione comunicando su di una medesima rete tramite il protocollo HTTP; consente quindi alle applicazioni che vi si collegano di usufruire delle funzioni che mette a disposizione.

INTERFACCE MACHINE-TO-MACHINE
Tecnologie e servizi che permettono il trasferimento automatico delle informazioni da macchina a macchina con limitata o nessuna interazione umana. Le comunicazioni M2M possono realizzarsi anche attraverso protocollo IP (Internet Protocol) e per questo motivo sono considerate la base dell' Internet of Things (IoT).

INTERNET OF THINGS
Insieme di tecnologie che permettono di collegare a Internet qualunque tipo di apparato.
E' un neologismo utilizzato in telecominicazioni, un termine di nuovo conio, che nasce dall'esigenza di dare un nome agli oggetti reali connessi ad internet.

CLOUD COMPUTING
Il cloud computing è un insieme di servizi che vengono erogati in hosting in Rete.
Cloud computing privato: infrastruttura informatica appartenente ad una specifica azienda e dedicata alle esigenze di quella sola organizzazione. L'infrastruttura fisica, può essere ubicata direttamente nei locali dell'azienda o data in gestione ad un terzo.
Cloud computing pubblico: erogazione di servizi che si basano su una infrastruttura informatica appartenete al fornitore del servizio; in questo caso è previsto il trasferimento di tutti i dati aziendali dai propri server a quelli del provider.

SISTEMA PCI-DSS
Standard PCI-DSS (Payment Card Industry Data Security Standard) elaborato con lo scopo di uniformare le modalità di gestione della sicurezza dei dati delle carte di credito da parte del consorzio PCI creato da American Express, Discover Financial Services, JCB, MasterCard Worldwide e Visa International. Lo standard deve essere rispettato da tutte le entità (esercenti, service provider, banche) coinvolte in una transazione mediante carta di credito che comporti la trasmissione, l'utilizzo o la memorizzazione del Primary Account Number (PAN) della carta. Tutti i settori commerciali ne sono interessati.

PHISHING
Truffa informatica effettuata inviando un'e-mail con il logo contraffatto di un istituto di credito o di una società di commercio elettronico, in cui si invita il destinatario a fornire dati riservati (numero di carta di credito, password di accesso al servizio di home banking, ecc.), motivando tale richiesta con ragioni di ordine tecnico.

ANTIVIRUS
Applicazione in grado di verificare la presenza di virus nei file memorizzati sui vari supporti (floppy, disco fisso, zip, etc), in memoria, e nel settore di boot. In caso venga trovato un virus conosciuto è normalmente possibile procedere all'eliminazione e/o alla pulizia del file. Gli antivirus hanno anche una funzione preventiva, cioè rimangono sempre attivi per impedire l'accesso dei virus al sistema. Devono essere periodicamente aggiornati per avere una protezione efficace.

PERSONAL FIREWALL
Programma installato su un comune personal computer che controlla le comunicazioni in entrata e in uscita dal PC stesso, permettendo o vietando alcuni tipi di comunicazione in base a regole o policy di sicurezza preimpostate dall'utente in fase di configurazione.

MALWARE
Letteralmente Malicious Software. Insieme di programmi che espongono il PC a rischi sia in fatto di privacy che di funzionamento del sistema operativo, si trasmettono via internet attraverso la posta elettronica o la semplice navigazione sfruttando le porte aperte del computer analogamente o congiuntamente ai worms. In questa categoria rientrano i virus, dialers, tracking coockies, ecc.

WORM
Tipo di disco ottico che consente di registrare i dati anche in diverse sessioni, ma ogni file rimane definitivamente archiviato e non modificabile.

RANSOMWARE
Sono un tipo di malware che bloccano i documenti contenuti sui sistemi infettati fino a quando il legittimo proprietario non paga un riscatto, in genere in bitcoin. Al pagamento della somma, i criminali in genere sbloccano la protezione dai documenti e rimuovono il criptovirus.
Inizialmente diffusi in Russia, gli attacchi con ransomware sono ora perpetrati in tutto il Mondo.

PATCHING/PATCH
E' un file che ha il "compito" di risolvere i problemi, ovvero gli errori di programmazione, che impediscono il corretto funzionamento di un programma o di un sistema operativo. Generalmente vengono rilasciate dagli stessi produttori, allo scopo di rimediare ai bugs rilevati fino a quel momento, nell'attesa di rilasciare la nuova versione del software medesimo.

BUG
Termine che viene utilizzato per definire un errore che, presente all'interno di un programma, ne impedisce il corretto funzionamento. Un bug, inoltre, può rendere poco sicuro o instabile un programma o un sistema operativo.

APT (ADVANCED PERSISTENT THREAT)
Attacchi che, partendo da un attacco mirato, arrivano a installare una serie di malware all'interno delle reti del bersaglio, al fine di riuscire a mantenere attivi dei canali che servono a far uscire informazioni di valore dalle reti del soggetto preso di mira.

DNS
Sistema d'identificazione utilizzato in Internet basato sull'associazione e traduzione di nomi facilmente memorizzabili in indirizzi IP. Ad esempio per raggiungere il sito www.pc-facile.com, inserendo il suo IP: 64.41.127.187 nella barra degli indirizzi del browser, si ottiene lo stesso risultato che si ha digitando il nome.
Il DNS viene memorizzato su un database che si chiama WHOIS e che contiene tutti i nomi e gli IP assegnati in modo che non ci siano duplicati.

UTM
Gestione unificata delle minacce. Garantisce una serie di protezioni di alto livello per l'intera rete aziendale, fornendo al contempo, ai responsabili della sicurezza un pannello di gestione da cui ricavare in tempo reale un quadro d'insieme sulla presenza di eventuali minacce in rete, nonché sull'attività, eventualmente pericolosa o vietata, svolta dal personale collegato in internet.

TYPOSQUATTING
Registrazione di domini-civetta, il cui nome varia di una lettera (o al massimo due) rispetto al nome di un sito web molto conosciuto e con un grande volume di traffico. Una volta giunto nel sito del typosquatter, l'utente ignaro può anche essere portato a credere che il dominio sia quello originale, utilizzando loghi simili, simile struttura e simili contenuti rispetto al sito originale.

DRIVE-BY-DOWNLOAD
Involontario download di software da Internet; può cerificarsi in maniera anonima e silente, oppure, a volte, avviene mentre lo stesso utente sta installando qualcosa, mentre si visita un sito web, mentre si visualizza un messaggio e-mail oppure cliccando su un ingannevole finestra pop-up, credendo magari di chiuderla.

BOTNET

Computer compromessi da worm, trojan, backdoor e altri software che conferiscono il controllo del PC a un server centrale. Il gestore del botnet - chiamato "bot herder" - può impartire ordini ai computer infetti, facendo loro compiere qualunque azione. Tipico dei botnet è un attacco DDOS.

CATENA DI CUSTODIA

Documento per la predisposizione di elementi probatori. In esso è riportata tutta la cronologia, dal momento del sequestro del materiale, delle fasi di indagini e le conclusioni che sono state elaborate su di esso dai soggetti che a vario titolo ne hanno avuto legittimamente accesso.

SPYWARE

Tecnologia che mira a raccogliere informazioni su di una persona senza che questa ne sia a conoscaneza. Di solito si tratta di un software che viene installato sul PC ad insaputa della persona, ad esempio nascosto in alcuni programmi shareware come Kazaa.

RSS

In precedenza noto come Rich Site Summary o Really Simple Syndication, è un metodo per descrivere contenuti che possono essere forniti a chi pubblica informazioni su Internet. È parte del progetto XML e aderisce alle specifiche dell'organizzazione W3C. Un documento RSS non è altro che un elenco di elementi ciascuno identificato da un link e caratterizzato da una breve descrizione ed eventuali altre informazioni.

SOCIAL BUZZ

Social Buzz , ovvero mormorio, ronzio social, è una tecnologia in grado di misurare il successo delle notizie e dei fenomeni Facebook, Twitter, Google Plus ecc… più discussi.

DoS

Acronimo per Denial Of Service. Si tratta di un attacco che una macchina porta ad un' altra facendole consumare le risorse a disposizione in modo che non ne restino per gli utenti regolari. In generale si fa in modo che la macchina obiettivo venga sommersa da richieste fasulle che la costringono ad allocare memoria temporaneamente. Se queste richieste giungono in numero sufficente da esaurire le risorse, quelle che provengono dall'utenza non potranno essere soddisfatte.

DDOS

A differenza del DoS, in questo caso l'attacco viene portato da piu' macchine (chiamate in genere zombie) in contemporanea contro un singolo bersaglio. Il risultato, in questo caso, è il consumo della banda a disposizione della macchina/vittima in modo tale che le richieste di utenti leciti non possano essere soddisfatte.