**M16 | Introducció**

Mètodes utilitzats per els ciberatacs

* Enginyeria social
  + es basen en descobrir info de la víctima a través de qualsevol vía manipulant-la, correus falsos, etc.
* Vulnerabilitats del sistema
  + atacs que es basen en forats de seguretat que presenten els sistemes operatius i/o programes en general.
* Software maliciós
  + Programes que al ser executats provoquen l’atac a la màquina de la víctima
  + Usualment combina amb l'enginyeria social.

Punt + feble de l’enginyeria social són les persones.

ENGINYERIA SOCIAL

* Informació personal bàsica que un hacker buscarà d’una víctima
  + Pet’s name
  + Dates significants
  + Nom del fill
  + Lloc de naixement
  + Vacacions favorites
  + …
* Altres accions que es pot fer
  + Enviar correus amb enllaços de software maliciós
  + Enviar correus amb webs que contenen components maliciosos
  + Enviar software maliciós dins d’un arxiu PDF/Excel/Word
  + Instal·lar Keylogger
  + …
* Vulnerabilitats del sistema
  + Qualsevol vulnerabilitat d’un S.O. és porta d’entrada per a un possible atac.
* Com protegir-nos?
  + Actualització constant dels S.O.
  + Instal·lació i actualitzazció dels antivirus i tallafocs
  + Monitorització i control de les xarxes ( Eines IDS, IPS, HIPS )
  + Utilització d’eines que utilitzin protocols segurs per a qualsevol operació a la xarxa
* Vulnerabilitat tipus Zero-day
  + El desenvolupador de software no sap que aquesta vulnerabilitat que existeix.

TIPUS DE HACKER

Black hat hacker

* grans coneixements de com entrar a un sistema informàtic aprofitant les seves vulnerabilitats.
* utilitza malware per explotar les vulnerabilitats
* utilitza keyloggers, link farming, ARP Spoofing, per aconseguir el seu objectiu

White hat hacker

* hacker ètic
  + hacktivisme
  + auditories de seguretat i Pentesting
* Utilitza les mateixes eines que un black hat hacker, però la seva finalitat és trobar les vulnerabilitats d’un sistema per així saber com protegir-lo
* Té el permís de l’empresa per fer els atacs, realment les empreses els contracten per a saber com protegir-se,.

Diferenciació de hackers en una empresa

* Red Team
  + Atacants → Seguretat ofensiva
  + Es dediquen a buscar vulnerabilitats del sistema, utilitzant les eines que utilitza un atacant
  + Emular el comportament d’un atacant
* Blue Team
  + Defensors → Seguretat defensiva
  + Tècnics que es dediquen a protegir els sistemes per a què no puguin ser atacats.
  + Necessiten eines de defensa ( Firewall, vigilància ( IDS, IPS ) etc )

**M16 N02 | Hacking ètic**

Hàcking ètic

* Conceptes prèvis
  + Hacker → Atacant
  + Víctima → empresa client
* Atacs a la infraestructura i els sistemes informàtics d’una empresa
* També poden incloure la plana web
* Finalitat
  + Trobar possibles vulnerabilitats ( configuracions incorrectes o errors de programació que si no es solucionen, es poden convertir en un forat de seguretat )
  + Veure les possibles conseqüències si s’ataquen les vulnerabilitats.
  + Buscar com solucionar la vulnerabilitat
  + Protegir-se dels possibles atacs

Introducció al hacking ètic

Test extern

* Es realitza des d’internet, sobre la infraestructura del client, de la seva xarxa pública
* Exemples:
  + Enrutador
  + Firewall
  + Servidor web
  + Servidor de correu
  + …
* Quan l’objectiu del hacking és una persona, es poden utilitzar eines i plataformes intel·ligents per trobar informació privada
* Plataformes + conegudes
  + Maltego
  + Have i been pwned?

Test intern

* Es realitza dins de la xarxa de l’empresa client
* Es simula el comportament d’un empleat que té accés a la xarxa de la empresa
* Es troben més forats de seguretat, ja que els administradors de xarxa acostumen a protegir d’atacs externs, el perímetre de la seva xarxa, i en canvi subestimen i obliden de protegir la xarxa interna de possibles atacs des de dins.
* Els estudis demostren que la majoria d’atacs que tenen èxit, provenen des de dins de la empresa

Modalitats de pentesting

* En funció de la informació que el client li traspassa a l’empresa auditora que fa el test d’intrusió.
* Black box pentest
  + Pentest de caixa negra
  + Acostumen a ser proves d’intrusió externes
  + El client no proporciona cap informació sobre la seva xarxa
  + L’auditor va a cegues, no sap com és la infraestructura, ni quins servidors…
* White box pentest
  + Pentest de caixa blanca
  + Proves d’intrusió internes
  + Client proporciona a l’auditor tota la info sobre la xarxa
* Grey box pentest
  + Pentest de caixa gris
  + Barreja dels anteriors
  + L’empresa client aporta algunes dades a l’empresa auditora

Altres serveis d ehacking ètic

* Test d’enginyeria social
  + Com conscienciats estan els treballadors de l'empresa amb la seguretat
  + Fer-los preguntes sobre usuaris i contrasenyes
  + Preguntar si tenen el mateix password a tot
  + Correus amb malware
  + …
* Wardriving
  + Entrar a la wifi de l’empresa client de manera no autoritzada per trobar vulnerabilitats i poder-les explicar
  + Sovint es fa des de les proximitats de l’empresa o des de un cotxe aparcat
  + Respecte a les Wifi, habitualment van encriptades amb WPA2 i els atacs estan basats en diccionaris
* Simulació d’equip robat
  + S’acorda amb la empresa client simular què podrien arribar a fer un lladre que robés un portàtil a algún treballador de l’empresa
  + Habitualment es limita a 24 hores i no es dona cap tipus d'informació personal ni password.
  + L’auditor ha d’entrar al sistema i robar tota la info que pugui
  + Pivoting → Intentar accedir a altres sistemes des del portàtil
* Auditoría de seguretat física
  + Buscar la manera d’entrar físicament a l’empresa, per exemple, burlant la seguretat de taxes RFID i NFC
  + Un cop dins de l’empresa, es pot posar algún dispositiu espía, per exemple un punt d’accés wifi fals i obert a tothom amb algun sniffer.
* Warshipping
  + Enviar un paquet amb algun dispositiu tipus RaspberryPI autònom, per a esniffar les telecomunicacions de la empresa.

FASES D’UN TEST D’INTRUSIÓ

1. Recopilació d’informació
2. Reconeixement
3. Anàlisi de vulnerabilitats
4. Explotació de vulnerabilitats
5. Informe d’auditoria

RECOPILACIÓ D’INFO

Informació Gathering:

* Es busca tot tipus d’info de la empresa i treballadors d’aquesta

Tècniques passives

* No contacte entre empresa/client
* Metodología OSINT

RECONEIXEMENT

* Scanning + enumeration
* Aconseguir màxima info possible sobre la xarxa de la empresa
* Tècniques actives
  + Es posen en contacte directament amb la infraestructura de la empresa.
* EINES HABITUALS
  + DNSLookUp
  + Nmap
  + Netcat
  + Netdiscover
  + pQf
  + Zenmap
  + Sparta
  + Shodan