Projecte ASIX 2k22

Escola Del Treball

2HISX 2021-2022

Aaron Andal & Cristian Condolo

CryptoSEC: "*Careful where you step in*"

Index

15. ACK Flood
16. ARP Spoofing
17. Ping Floor
18. TCP Session Hijacking
19. Atacs DoS
20. FTP Bounce

- **Bibliografía**: README

Atacs Informatics / Ciberatacs

Introducció

Els **ciberdelinqüents** es troben alertes de noves formes de atacar-nos al usuaris, agafant ventatge del nostre `desconeixement o vulnerabilitats` en les nostres defenses.

Cada vegada son més les empreses que tomen medides de prevenció, protecció y reacció devant d'incidents relacionats amb **la cibersegüertat**. Com la ciberdelinqüència actua en benefici propi els `metodes y tecniques` utilizades **van mutan y evolucionan**,donant a lloc a **noves formes de ciberdelinqüència**.

Les empreses sempre es troben expostes a atacs informatics constanment, per aixo, es important coneixer els **exemples de atacs informatics** que poden passar.

- Enginyeria social
- Keylogger
- Seqüencia TCP
- Malware o Software maliciós
- Virus
- Cuc informatic
- Troià
- Spyware
- Adware
- Ransomware
- Rootkit
- LOKI
- Escaneig de ports
- Man in The Middle
- ACK Flood
- ARP Spoofing
- Ping Floor
- TCP Session Hijacking
- Atacs DoS
- FTP Bounce

Exemples

1. `Enginyeria social` Que consisteix?

Aqui l'atacant aconsegueix peruadir a l'usuari perque li permeti accedir a les seves passwords o equips informatics, i robar informació o instal · lar sofware maliciós.

Com prevenir-ho?

Se precavit i lletgir el missatge determinat. A més, altres pautes per evitar ser victima de phishing: - Detectar errors gramaticals en el missatge - Revisa que l'enllaç coincideix amb l'adreça a la que apunta - Comprovar el remitent del missatge - No descarregar cap fitxer adjunt i analitzar-ho previament amb un antivirus. - No contestar mai al missatge

La millor defensa per a atacs Baiting es evitar connectar dispositius desconeguts d'emmagatzematge extern o amb connexió USB al nostre equip. Mantenir el nostre sistema actualitzat y les eines de protecció, com l'antivirus, activades i actualizades.

L'opció mes segura es evitar que tercers tinguin visió de la nostra activitat. També se recomana utilitzar gestor de contrasenyes i la verificació de dos pasos. Hem de cerciorar-nos que de no hi ha tercers persones observant el nostre dispositiu, especiament a l'hora d'ingressar dades personals.

En el cas del Dumpster Diving, l'unica medida de protecció que hem de seguir la eliminació segura d'informació perque no rebusquin en la nostra papelera.

Per al spam es recomana mai utilitzar el compte de correo electronic principal per registrar-nos a ofertes o promocions per Internet.

2. `Keylogger` Una eina la qual aconsegueix registrar les pulsacions que produeixen dins del teclat de l'usuari, aconseguint passwords y altres dades delicades.

3. `Seqüencia TCP` Aquest pot afectar a una empresa al generar duplicats de paquets perque l'intrus pot robar la sesió de una connexió TCP, provocant serios inconvenients al sistema.

4. `Malware o Software maliciós` Potser un del exemples d'atacs informatics més habituals, que consisteix en un programari maliciós que infecta un equip informatic de manera il · licita, i pot ser de diversos tipus com: virus,troians, spyware, entre d'altres.

5. `Virus` Són programes informatics que tenen la capacitat de replicar-se de manera oculta, despres d'instal · lar-se sense permis de l'usuaris, i que poden generar greus afectacions de funcionament a l'equip informatic infectat.

6. `Cuc` Un cuc informatic, es igual que un virus, es replica automaticament, pero, es diferencia d'aquest perque no requereix d'un programa per allotjar-se a l'ordinador de la victima, i ataca principalment a la xarxa i a l'ample de banda.

7. `Troià` Es un codi maliciós conegut com troià o caball de troia, es presenta principalment com un programa legitim, però en ser instal · lat, concedeix accés remot a l'atacant sobre l'equip informatic de la victima, podent manejar-ho gairebé el seu gust.

8. `Spyware` Es tracta d'un programa dedicat a la recopilació i la transmissió d'informació de l'usuari a un altre lloc, sense el seu consentient.

9. `Adware` Es un tipus de programari maliciós, destinat a l'enviament constant de publicitat a l'usuari, sense la seva autorització, i que pot estar inclòs en llocs web o fitxers que s'instal · len a l'ordinador.

10. `Ransomware` Aquesr malware impedeix l'acces a una part del sistema, i demana un rescat per això, de manera extorsiva.

11. `Rootkit` Es un grup d'eines que permeten als atacants ingressar al sistema de maner oculta, a més de fer indetectables els arxius que usen per fer-ho.

12. `LOKI` Es fa sevir per transmetre dades de manera oculta, aprofitant el trànsit habitual d'un xarxa, sense que el seu usuari aconsegueixi adonar-se'n.

13. `Escaneig de ports` Permet a l'intrus detectar quins ports estan disponibles per ingressar a la xarxa.

14. `Man in The Middle` Es fan servir per interceptar de manera il · licita una comunicacio que ha establert entre dos sistemes, amb la finalitat de furtar dades o informació valuosa.

15. `ACK Flood` S'usa per a l'enviament de paquets de tipus TCP o ACK a l'usuari atacat, fent servir una adreça IP falsa, cosa que pot alterar l'operativitat del sistema.

16. `ARP Spoofing` Consisteix en el col · lapse o modificació del trànsit d'una xarxa d'Ethernet, arribant fins i tot a aturar el trànsit completament.

17. `Ping Floor` Es un atac informatic que s'encarrega d'enviar una gran quantitat de paquets de tipus ping a l'usuari, congestionant el sistema de manera severa.

18. `TCP Session Hijacking` Un altre exemple notable d'atacs informàtics a una empresa passa quan hi ha un hackeig de la sessió TCP que s'ha establert entre dos sistemes. Aquest atac es dóna al moment d'autenticar i inici de sessió.

19. `Atacs DoS` Es representa quan un l'intrús aconsegueix evitar que l'usuari s'autentiqui o aconsegueix accedir normalment al sistema o a un lloc web, per exemple. Aquest tipus d'amenaça pot passar sovint en una empresa.

20. `FTP Bounce` L'atac FTP Bounce pot passar quan un instrús aconsegueix tenir accés a un servidor FTP, i des d'alla, procedeix a enviar firxers maliciosos a altres usuaris que es troben connectats a la mateixa xarxa.

D'aquesta manera, els atacs informatics estan a l'ordre del dia en una quantitat força elevada. Per això, les empreses han d'implementar mesures de seguretat informatica de manera urgent per prevenir abans que lamentar.

Realitzar una inversió important en matèria tecnològica i capacitat del personal repercutirà de manera positiva en les operacions i la productivitat d'una empresa, aconseguint prevenir de manera efectiva els atacs informàtics.

Bibliografía

- https://www.incibe.es/protege-tu-empresa/blog/las-7-fases-ciberataque-las-conoces
- https://www.osi.es/sites/default/files/docs/guia-ciberataques/osi-guia-ciberataques.pdf
- https://uss.com.ar/corporativo/ejemplos-de-ataques-informaticos-empresa/
- https://ciberseguridad.blog/25-tipos-de-ataques-informaticos-y-como-prevenirlos/