- **sessió 4**

14.- Virtualització.

BERNAL MACIAS, ALBERT - ORTUÑO SERON, BLAI

- Quins son els avantatges de fer servir virtualització? (breu, les més importants per a tu)
  La virtualització ens permet fer servir els recursos *hardware* que tenim de forma eficient, distribuint la capacitat de les nostres màquines (físiques) entre molts usuaris i entorns. Així que, sens dubte, la avantatge principal és el consum i l'eficiència de l'ús de recursos, però també hi ha avantatges en qüestions de monitorització, seguiment i versatilitat.
- Defineix el funcionament d'un hypervisor.
  Els *hypervisors* es composen de peces intel·ligents de *software* que possibiliten l'abstracció de recursos *hardware* i, d'aquesta manera, la creació de servidors virtuals integrats per màquines virtuals que accedeixen als recursos físics subjacents del servidor real i comparteixen aquests recursos entre si. Un sistema en el qual un hipervisor executa una o més màquines virtuals s'anomena sistema *host*, i cada màquina virtual que s'executa en el hypervisor s'anomena sistema *guest*.
  El *hypervisor* proporciona als *guests* una plataforma virtual que gestiona l'execució dels seus sistemes operatius, de manera que vàries instàncies de diferents sistemes operatius poden compartir aquests recursos de *hardware* virtualitzats.
- Al treball parlen de diferents eines de virtualització. Indica una característica d'una (o diverses) eines que t'hagi sorprès. Indica quina és i què és el que t'ha fet reflexionar.
  M'ha sorprès l'exitosa col·laboració de la tecnologia de virtualització de VMware i la plataforma de cloud de Amazon. Així mateix, m'ha sorprès que Xen sigui l'únic hypervisor de Type I que existeix, i també l'origen de KVM, com a recurs inherent de Linux.

15.- Monitorització.

ORELLANA CELIS, NICOLAS IGNACI - RODRIGUEZ GONZALEZ, ISIS

- Indica 3 coses que es poden monitoritzar (escull quines 3) i indica quins problemes implica no monitoritzar-les

3 coses que es poden monitoritzar: disponibilitat de servidors (si no detectem immediatament quan ens cau un servidor, patirem d'una caiguda del nostre servei, la qual cosa pot ser molt greu depenent de la naturalesa del servei que oferim), rendiment web (el fet de no parar compte en el rendiment de les nostres webs ens pot fer passar de banda problemes com un anormalment alt temps de càrrega o la fallada de certs elements de la web) i monitorització de seguretat (aquest tipus de monitorització serveix per evitar qualsevol tipus d'intrusió de seguretat que posi en perill el nostre sistema, ja sigui amb atacs externs o interns).

- Com funciona un software de monitorització?

De forma general, un software de monitorització s'encarrega de fer un seguiment de l'estat del nostre sistema informàtic, tant de la infraestructura com de la resta de subsistemes, amb la finalitat d'assegurar la fiabilitat i estabilitat dels serveis que ofereixen en conjunt. Aquest tipus de software es basa en la recollida de mètriques, processament i visualització de les dades, junt amb la generació d'alertes quan detectem quelcom que pot ser un signe de risc o mal funcionament d'algun component del nostre sistema.

- Reflexió. Penseu que la informació que s'extreu de softwares de monitorització com Nagios o Ganglia poen ser utilitzarts pel CIO o el CEO per prendre decisions? Raona la resposta.

Jo en principi diria que no. És a dir, la informació que ofereix la monitorització és, sens dubte, molt valuosa, però ho és per a enginyers i personal tècnic que estan per sota d'aquests càrrecs de la directiva empresarial. Tot i així, potser la monitorització d'usuaris reals (RUM) pot donar alguna informació útil a nivell de canvis estratègics que podrien ser interessant per l'empresa.

16.- Eines d’orquestació.

GIL VÁZQUEZ, ÁLVARO ANTONIO - PIRAU, CALIN CONSTANTI

- Quina és la funció de les eines d’orquestració? Quina utilitat tenen en un CPD?

Les eines d’orquestació ens permeten configurar, gestionar i coordinar automàticament una gran quantitat de serveis i aplicacions diferents en els nostres sistemes informàtics.

En un CPD, per exemple, ens poden fer estalviar molt de temps per exemple fent el deploy del nostre software a la nostra xarxa a una gran quantitat de màquines, o inicialitzant algun/s serveis de forma massiva, per exemple.

- De les eines presentades, quina t’ha sorprès? Per quina funcionalitat?

M’ha sorprès bastant el comportament de Chef Workstation. El fet de definir l’estat desitjat del nostre sistema enlloc d’especificar la forma d’assolir aquest estat m’ha semblat una idea molt còmode a nivell de programador.

- Reflexió, les eines d’orquestració semblen tenir molt futur, però van evolucionant. Reflexiona sobre quines coses es poden anar automatitzant i formar part de les coses que fan els orquestradors.

No sé gaire on estan els “límits” actuals dels softwares d’orquestració, però imagino que els software d’orquestració podran ajudar a executar tests de les nostres webs i servidors de forma automàtica, potser corregint, fins i tot, diferents vulnerabilitats sense intervenció humana. O potser aquest tipus de software podria cercar errors *subtils* en codi d’una aplicació que s’ha actualitzat (per exemple, codi JavaScript o CSS d’una web) i informar al programador (o corregir ell mateix l’error), així com trobar rutines que es poden optimitzar / paral·lelitzar.

17.- Seguretat.

FRANCÉS FALIP, JAVIER - SÁNCHEZ MULERO, DAVID

- Quines són les ciberamenaces més comuns pels CPDs?
  Feblesa de les contrasenyes dels administradors / personal amb alt nivell d'accès (atac de diccionari o enginyeria social), mala configuració de les llistes d'accés per restringir el tràfic (ACL), falta de restricció de privilegis i rols dels usuaris del sistema. També cal desactivar els serveis innecessaris i gestionar / monitoritzar els recursos utilitzats a cada procés per evitar atacs de denegació de servei (DDoS).
- Descriu breument els equips de seguretat. Què fan?
  Els equips de seguretat estan present a tota empresa amb una mida considerable o que treballi amb dades que puguin necessitar un nivell de seguretat. Han de fer revisions periòdiques a les distintes bases de dades de vulnerabilitats i efectuar proves de penetració a la nostra xarxa corporativa i sistemes rellevants per tal de minimitzar-ne els riscos associats a l'explotació indeguda d'aquests. També han de protegir i con-figurar els sistemes de hardware i software de l'empresa per assegurar que no es pugui fer un mal ús dels recursos.
- Quines eines té un Blue team?
  Les principals eines són les SIEM, que utilitzen ML i Big Data. Són eines que recopilen informació en temps real de tota la infraestructura hardware i de les aplicacions en forma de *logs*, i transformen aquests *logs* en informació més accessible, com events. Els sistems SIEM no permeten així generar informació sobre atacs (com i quan va succeir) i events passats.

18.- Introducció a la seguretat informàtica en CPD
FREDERIC W. UHLMANN

- Quins són els pilars de la seguretat? Afegiríeu alguna cosa?
  Confidencialitat, Integritat i Disponibilitat.

- De les vulnerabilitats més comuns descrites, escull la que penses que és més complicada de protegir (i indica perquè).
  De les vulnerabilitats descrites, la que em sembla més complicada de protegir és la de *Cross-site request forgery*, ja que l'atac, des del *punt de vista* de la web les comandes rebudes són enviades per part d'un usuari legítim, de manera que és molt difícil detectar que s'està produint un atac. Hi ha una forma component d'enginyeria social aquí (per prendre el control d'aquest usuari en el qual la xarxa confia) i per tant és un atac molt difícil protegir.

- L'autor reflexiona sobre les implicacions en seguretat avui dia i posa com a exemple el cas d'hospitals i ramsomware. Pensa (o cerca) un cas i indica'l aquí.
  Em ve al cap un altre gran atac de ransomware que es va produir al 2017 (amb el ransomware WannaCry), que fa infectar a més de 200.000 ordinadors a 150 països (afectant a empreses com FedEx, Telefónica, Deutsche Bahn, a les aerolínies LATAM, a molts bancs a nivell mundial i, fins i tot, a parts del servei nacional de salut de Gran Bretanya).
  En principi, el WannaCry infecta a un *primer* ordinador quan un usuari obre un correu electrònic de *physhing*. Un cop instal·lat, WannaCry utilitza l'exploit conegut com a EternalBlue per a estendre's a través de les xarxes locals i *hosts* remots que no hagin rebut l'actualització de seguretat contra l'exploit i, d'aquesta forma, infectar qualsevol sistema exposat.