TK2100

T-02

**OPERATIVSYSTEM**

Notater repetisjon:

* SHA-0 og SHA -1 regnes som usikre
* Kombinerer aes og rsa , genererer random symmetrisk privat nøkkel ,K5 krypterer meldingen effektivt , og krypterer K5 med bobs offentlige nøkkel
* Sender både k5(m) og kb(k5) til bob
* RSA er en treig algoritme og trenger å bruke minst mulig data for å kryptere /dekryptere

Notater i dag:

* Antivirus gir en beskyttelse mot virus og datamaskinen er sårbar mot virus uansett hvor forsiktig man er og det lages mange virus hver dag. Det er andre komponenter i tillegg til antivirus som beskytter mot datavirus.
* Backup er viktig for å ikke miste data , det må ikke være virus, men det kan også være at hardisken er ute av drift, virus kan infisere skylagringen så backup av filene til ekstern lagring anbefales , som f.eks harddisker ,usb osv.
* To-faktor autentisering forhindrer angrep på online kontoer, den høyeste sikkerheten er fysisk kodebrikke, authentical app
* Man må være bevisshet om at det finnes mange trusler og kan forventes å bli angrep som f eks: ikke trykk på en link ,svar på en epost eller sett inn en ukjent usb stikk, ikke oppgi passordet ditt hvis noen ringer (ikke svar ) ikke last ned piratkopierte filer (de inneholder ofte malware)
* Beskytt personlig og sensitiv informasjon som f.eks ikke del sensitive bilder på nettet eller info om bankkontoen din (hold dette alltid anonymt for deg selg). Dekk til webcamera , man kan bli presset for penger etter at private bilder er stjålet eller lekket ut. Mange på internett ønsker ikke deg noe godt.
* User mode og kernel mode er en viktig del av sikkerheten på operativsystemet.
* User mode kan ikke aksessere Hardware , utstyrsdrivere direkte et virus kontakter usermode hvis pc infiseres.
* Hvis angriper får tilgang til kernel mode , har angiperen tilgang til minne og harwaren til pc
* Minnet er der filer og prosesser lever
* Under graving av sikkerheten handler om å få tilgang til minneområdet
* OS og applikasjoner befinner seg i minnet eller i filsystemet, OS viktigste oppgave er å beskytte dette i datamaskinen.
* Procexp64.exe sjekker hvilke brukere og hvilke applikasjoner de har kjørt eller kjører på datamaskinen.
* Administrator har fullkontroll på filene dine. Du har alle rettigheter
* Ring 0 (kernel mode)
* Usermode prossesser har separate minneområder
* Session 0 isolation har ikke direkte minnetilgang til filene.
* Autentisering utføres med passord eller smartkort.
* I Windows : Hvis du er logget in som admin er du likevel ikke det.
* Kjører du maskinen med full privilegier vil det gi en påvirkning på sikkerheten.
* Protected mode separer de sårbare applikasjonen som gjør at man ikke infiserer maskinen.
* Windows all innkommende trafikk (Windows XP SP2 og Vista)
* Windows Defender (er en spyware ikke antivirus) er uaktuelt når det kommer til antivirus programmer.
* Bitlocker krypterer maskinen og er en form for AES kryptering
* Kan kryptere usb med Bitlocker.
* Word pdf kan krypteres ved inntasting av passord. ZIP filer er anbefalt for å sikre filene og man ser bare filnavnene.
* Rootkits filtrerer kernel kall for å skjule seg selv.
* Remote hacking utnytter svakheter i os services som lytter på nettverket.
* Viktigste tiltak mot sårbarheter er å PATCHE.
* Hendelseslogging
* Bootsekvensen – lasting av OS går via BIOS/UEFI som så laster en sekundære bootloader
* Kode med bakdører for å finne passordet på maskinen
* Buffer owerflow er et angrep som vil overskrive hva som måtte befinne seg i minne 10976 plasser over starten av arrayet

1. **Hva er Multitasking?**

Multitasking er når maskinen utfører flere oppgaver samtidig . Det kan være f.eks at maskinen kjører flere programmer. Dette har de fleste operativsystemer i dag som Windows og OSX som tillater brukeren/brukere kan kjøre flere applikasjoner samtidig.

1. **Hva er forskjellen på User- vs Kernel-modus?**

Får å oppnå best mulig sikkerhet og beskyttelse gir de fleste CPU-ene anledning til å kjøre instruksjoner enten i user eller kernel mode.

User mode (ring 3 ) kan ikke aksessere HW , utstyrsdrivere direkte og må bruke en API. Den har kun adgang til minnet som OS-en har tildelt og har et begrenset innstruksjonsett. Vanlige applikasjoner og mange OS-tjenester , undersystemer kjører i denne modusen.

Selve OS- kjernen kjører i kjernemodus (kernel- mode) (ring 0) . Modusen har tilgang til hele minnet og alle instrukser kan kjøres. Kernel mode har ingen sikring fra HW (HardWare)

User mode og kernel mode er en viktig del av sikkerheten på operativsystemet. User mode kan ikke aksessere Hardware , utstyrsdrivere direkte.

Hvis pc blir infisert av et virus vil den først kontakte usermode.

Hvis angriper får tilgang til kernel mode , har angriperen tilgang til hele minne og hardwaren til pc uten beskyttelse fra prosessoren og (operativsystemet) og angriper har mulighet til å utføre systemkall direkte.

1. **Hva er forskjellen på prosess og tråd? Tråder er flyt av prosseser**

En prosess er en program som kjører på maskinen. Prosess er altså en samling av ressurser som er nødvendige for å utføre en oppgave som er beskrevet med en programkode eller kodet. Eksempler på ressurser er Minne/Ram evt diskplass. Tråder er en flyt av utførelse inni en prosess, som kjører enten parallelt eller samtidig. Trådene er lette prosesser og det er mye raskere å opprette nye tråder enn nye prosesser. Det er oftest raskere kommunikasjon mellom trådene sammenliknet med prosessene.

Er samling av ressurser for å utføre en handling som er representert i en programkode eller er kodet. Tråder er en flyt av prosesser som ligger inni en prosess .Det er raskere å opprette nye tråder enn nye prosesser

User mode kan ikke aksessere HW direkte eller andre utstyrskomponenter og må bruke en API for å gjøre det . Den har tilgang på minne som er utdelt av OS og har en begrenset instruksjonssett. Vanlige app , noen os-tjenester og undersystemer kjører i denne modusen.

1. **Hva tilbyr som oftest et filsystem?**

OS og alle applikasjoners kjøretilstand befinner seg i minnet eller filsystemet.

Filsystemer tilbyr ofte adgangsrettigheter og fil-tillatelser . I adgangsrettigheter er det tre nivåer : Bruker , (user) , Gruppe(group) og andre (Other)

Der det er tre adgangsrettigheter for hvert nivå:

Lese (read), skrive(write) og utføre(execute). Disse kan endres av eier eller bruker ved bruk av kommandoen chmod : chmod o+r filen.min

1. **Hva er en virtuell maskin(VM)?**

En virtuell maskin (VM) er programvare som kjører på en datamaskin som hovedsakelig fungerer som en reel fysisk datamaskin . Noen virtuelle datamaskiner etterligne drift av reelle fysiske datamaskiner , mens andre gir en abstrakt grensesnitt til den fysiske datamaskinen for å gjøre programmering for flere PC- typer enklere.

1. **Nevn noen basic NTFS tillatelser**

Read, List Folder Contents, Read and execute, Write, modify, Full Controll. Er eksempler på NTFS tillatelser

1. **Nevn minst ett viktig tiltak for å sikre OS mot angrep**

* Antivirus gir en beskyttelse mot virus og datamaskinen er sårbar mot virus uansett hvor forsiktig man er og det lages mange virus hver dag. Det er andre komponenter i tillegg til antivirus som beskytter mot datavirus.
* Backup er viktig for å ikke miste data , det må ikke være virus, men det kan også være at hardisken er ute av drift, viruset kan infisere skylagringen så backup av filene til ekstern lagring anbefales , som f.eks harddisker ,usb osv.
* To-faktor autentisering forhindrer angrep på online kontoer, den høyeste sikkerheten er fysisk kodebrikke, authentical app (avgjør rollen/identiteten til personen som gjøres ved eks smartkort eller smarttelefon.
* Enhver person bør være bevist på at det finnes mange trusler og kan forventes å bli angrep som f.eks.: ikke trykke på en link ,svar på en epost eller sett inn en ukjent usb stikk, ikke oppgi passordet ditt hvis noen ringer (ikke svar ) ikke last ned piratkopierte filer (de inneholder ofte malware)
* Beskytt personlig og sensitiv informasjon som f.eks ikke del sensitive bilder på nettet eller info om bankkontoen din (hold dette alltid anonymt for deg selg). Dekk til webcamera , man kan bli presset for penger etter at private bilder er stjålet eller lekket ut. Mange på internett ønsker ikke deg noe godt (Vær oppmerksom på hva du legger ut på nettet).

1. **Hva er Rootkits?**

Rootkits filtrerer kernel kall for å skjule seg selv.

En rootkit er en type skadelig programvare designet for å gi angriperen eller hackeren tilgang og kontroll over maskinenheten. Noen rootkits kan infisere maskinens HardWare i tillegg til at den påvirker programvaren og OS-et . Rootkits er dyktige til å skjule drivere og prosesser (tilstedeværelse) mens de forblir skjulte er de aktive. Når rootkits bryter seg inn i datamaskinen på en uautorisert måte gir den nettkriminelle anledning til å stjele personlig info fra maskinen. Rootkits er oppsummert en programvare som brukes av angriperen/svindleren for å få kontroll over en datamaskin eller et nettverk på administrasjonsnivå som lar dem stjele eller endre på filene i maskinen din utilsiktet.

Man skriver over

Forskjellige måter av rootkits: Firmware Hypervisor , kernel bibliotek ,applikasjon

Teknikker brukt av rootkits skjuling av drivere/prosesser , skjuling av registry oppføringer og skjuling av fysiske filer på disk.

1. **Hva er stack-buffer overflow? Hvordan kan dette være en svakhet?**

Stack – buffer r- overflow er en type angrep maskinen kan bli utsatt for. Den kan gi sikkerhetsbrudd og ustabilitet i systemet.

Med ulike skadelige muligheter og metoder for utnytting , utviklere stadig søker måter å beskytte datasystemer fra disse overskridelsene . Selv beskyttende alternativer finnes, kommer hver med sine avveininger eller gi begrensede muligheter til beskyttelse.

Mitt svar:

**Et program prøver å ta opp mer lagringsplass blir dataen lagret i en buffer og når dataen i bufferet er fullt «overflow» vil dataen lagres i nabo bufferet noe som medfører at dataen i bufferet kan bli ødelagt eller skadet . Dette vil forårsake en data korrupsjon som kan gi angripere tilgang til programmet . De kan gjøre uautoriserte endringer i systemet i programmet som kan gi dem tilgang til sensitiv informasjon gjennom data korrupsjon av minnet . De kan endre informasjonen de får tilgang til eller utnytte dem C og C++ er de to eneste programmeringsspråkene som ikke er sikret mot denne typen angrep og hvis det blir overflow i programmet som kjører disse kan det medføre en programmeringsfeil. De andre programmeringsspråkene har beskyttelse mot denne typen angrep som gjør at de ikke blir utsatt . Microsoft patcher jevnlig programmene sine for å forhindre stack buffer overflow (sikkerhetsbrudd) .**

**En buffer overflow angrep oppstår når et program bevisst forsøker å ta opp mer lagringsplass enn buffer kan håndtere , forårsaker noen ekstra data til "overflow ".**

**«Buffer er et sett med data» som har et begrenset antall plass. (hvis fult) blir dataen overført til nabo buffer som gjør at den ikke forsvinner**

**Kilde : datamaskin.biz**

En buffer er minnebruken ved et program som midlertidig lagringsplass for å håndtere et overskudd av data. Buffere kommer i forskjellige størrelser og er i stand til å lagre sett mengder data . En buffer overflow angrep oppstår når et program bevisst forsøker å ta opp mer lagringsplass enn buffer kan håndtere , forårsaker noen ekstra data til "overflow ". Dette kan føre til at data korrupsjon, som igjen gjør at en angriper å kapre kontroll over programmet . Buffer overflow kan oppstå som et resultat av en programmeringsfeil , men bufferoverløpangrep blir i økende grad brukt som en måte å undergrave systemets sikkerhet og angrep dataintegritet . Effekter av Buffer Overflow

Når bufferen er fylt opp med data fra et program , tenderer det overskytende data til å renne over . Denne ekstra data kan ikke åpenbart bare forsvinne , det vil som regel fortsette å fylle naboland buffere , noe som kan føre til at data i disse buffere for å bli ødelagt.

Program prøver å ta opp mer lagringsplass og når den bufferer vil ekstra data bli lagt til i en overflow det

En buffer overflow angrep oppstår når et program bevisst forsøker å ta opp mer lagringsplass enn buffer kan håndtere , forårsaker noen ekstra data til "overflow ". Dette kan føre til data korrupsjon, som igjen gjør at en angriper å kapre kontroll over programmet . Buffer overflow kan oppstå som et resultat av en programmeringsfeil , men bufferoverløpangrep blir i økende grad brukt som en måte å undergrave systemets sikkerhet og angrep dataintegritet

De fleste maskiner er sårbar stack buffer overflowen

Buffer håndterer et sett med data og når maskinen tar opp mer data lagres de i en overflow dette kan gi

bufferoverløpene kan tillate nettkriminelle å foreta uautoriserte endringer i systemet . Anslått å utgjøre nesten 50 prosent av PC- sårbarheter utnyttes i de siste 10 årene , kan bufferoverløpene føre til datamaskiner som utfører utilsiktede kommandoer , noe som gir brukerrettigheter til hackere og avslørende sensitive data , gjennom hele korrupsjon av minnet nær buffer .

C og C + + er fortsatt de mest sårbare språk til buffer overskridelser , som de ikke har noen beskyttelse mot overskriving noen del av minnet. Disse språkene kan heller ikke gi noen form for sjekk for å sikre at når du skriver til buffer at det ikke overkjørt sine grenser . Imidlertid , fordi C og C + + forbli vanlige programmeringsspråk , gjenstår problemet. Selskaper som Microsoft , patcher utgivelsen sikkerhet jevne mellomrom for sine programmer for å forhindre slike sikkerhetsbrudd .

1. **Hva er et “0-day”-attack?**

Det finnes ikke kjente hack for å ta over maskinen lokalt uten å bruke interaksjon dette kalles for 0-day attack.

Enkleste måten å knekke sikkerheten på er å angripe det svakeste leddet som er brukeren.

1