T-02
OPERATIVSYSTEM

1) Hva er Multitasking?
Gir hver kjørende program tids-luker på CPU. Sørger for at det kan se ut til at flere programmer kjører «samtidig», Men i realiteten bytter veldig fort mellom hvert program.

2) Hva er forskjellen på User- vs Kernel-modus?
Vanlige applikasjoner og mange andre av tjenester OS-et tilbyr kjører i «user mode» altså (ring 3), mens OS-kjernen kjører i kjernemodus(ring 0). I user mode kan man ikke aksessere hardware(HW) og utstyrsdrivere direkte og har kun tilgang til minne som OS-et har tildelt samt at man har et begrenset instruksjonssett. I kjernemodus kjører man i såkalt protected mode og har tilgang til hele minnet samt at alle instruksjoner kan kjøres. I kjernemodus har man også ingen sikring fra hardware(HW)

3) Hva er forskjellen på prosess og tråd?
Når et program kjøres på en datamaskin kalles det en prosess. En prosess er allokerings-enhet og OS oppretter en prosess samt tideler den rettigheter og ressurser. En prosess kan innholde flere tråder som kan utføre instruksjoner delvis uavhengig av hverande. En tråd er en utførings-enhet og utfører instruksjoner.

4) Hva tilbyr som oftest et filsystem?
Et filsystem tilbyr som oftest en abstraksjon av hvordan eksternt, ikkeflyktig minne er organisert. De fleste filsystemene organiserer filer hierarkisk i kataloger.

5) Hva er en virtuell maskin(VM)?
En programmvare som simulerer hardware ved å «hijacke» alle systemkall og ellers kjøre instruksjoner som vanlig.

6) Nevn noen basic NTFS tillatelser

NTFS Permission	Folders	Files
Read	Open files and subfolders	Open files
List Folder Contents	List contents of folder, traverse folder to open subfolders	Not applicable
Read and Execute	Not applicable	Open files, execute programs
Write	Create subfolders and add files	Modify files
Modify	All the above + delete	All the above
Full Control	All the above + change permissions and take ownership, delete subfolders	All the above + change permissions and take ownership

7) Nevn minst ett viktig tiltak for å sikre OS mot angrep

- Laste ned patcher/opdateringer med en gang disse blir tilgjengelige
- Ingen brukere med høyere tilgangsnivå enn absolutt nødvendig
- Konservativ installasjonspolicy generelt

8) Hva er Rootkits?

Rootkits er en samling av software som brukes til å få tilgang til områder personen ikke er autorisert til. Rootkits kan manipulere data på root-nivå og dermed endre/fjerne filer. Siden rootkit kan endre filer så kan den også skjule seg for antivirus programmer.

- Ved å hooke NtQueryDirectoryFile kan man velge å fjerne oppføringer av enkelte filer (som man ønsker å skjule).
- Dette vil da medføre at FindNextFile ikke viser filen du ønsker å skjule.
- Anti-Virus applikasjoner som skanner filer ved å enumerere ut filer på harddisken vil da ikke finne filen du har skjult.
- På denne måten har ”rootkittet” klart å skjule seg selv på systemet.

9) Hva er stack-buffer overflow? Hvordan kan dette være en svakhet?

Stack-buffer overflow handler om at man kan sende in mer data enn stacken forventer og dermed overskriver retur-adressen. Dette kan være en svakhet ved at man kan gi en returadresse som viser til “farlig” kode. Dette skjer fordi språk som for eksempel “C” ikke sjekker grensene for arrays når de deklareres og de leser stort sett user-input inn I arrays.

10) Hva er et “0-day”-attack?

0-day attack er ett angrep/svakhet som ennå ikke er kjent/funnet. Dette gjør svakheten farlig fordi selskapet selv ikke vet om svakheten og brukerne er dermed ikke beskyttet mot denne svakheten.