Leg med virus og malware

T1 – Sikkerhed

# Opgavens fokusområder

Du har kendskab til begreberne firewall og hacking

Du har kendskab til multifaktor-autentifikation

Du har kendskab til begrebet malware og antivirus

# Kort fortalt

I denne opgave skal du sikkerhed og trusler, og du skal afprøve malware på virtuelle maskiner

# Praktiske oplysninger

I denne opgave er tilegnelse af viden (del 1) og test af viden (del 2) blandet sammen, så du skal besvare spørgsmål efter hvert materiale du har set eller læst.

# Opgave

## Del 1 – Tilegnelse og test af viden om Multifaktor autentificering

Læs Wikipedia om [Multi-factor authentication](https://en.wikipedia.org/wiki/Multi-factor_authentication) eller se videoen [Tom Scott: Why You Should Turn On Two Factor Authentication](https://www.youtube.com/watch?v=hGRii5f_uSc). Besvar herefter spørgsmålene i skemaet.

|  |  |
| --- | --- |
| Spørgsmål | Svar |
| Hvorfor anvendes multifactor autentificering? | For at sikre, at uvedkommende personer ikke kan få adgang til følsom information. |
| Hvad er de 4 forskellige autentifikationsfaktorer? | Noget du ved (password/pin/signatur) - Noget du er (fingertryk/ansigtsgenkendelse) - Noget du har (bankkonto/telefon/nøgle) - Hvor du er (fysisk lokation) |
| Hvor mange autentifikationsfaktorer skal kombineres for at opnå god sikkerhed? | 3-type autentifikationsfaktorer da det gør det meget mere besværligt for uvedkommende personer at få adgang til dine informationer. Dog kan du ikke være 100% sikker, da alt med tiden kan blive forfalsket, men det er endnu et skridt, der gør det mere besværligt. Minimum 2. |

## Del 2 – Tilegnelse og test af viden om firewall

Se videoen [What is a firewall](https://www.youtube.com/watch?v=kDEX1HXybrU) og besvar herefter spørgsmålene i skemaet.

|  |  |
| --- | --- |
| Spørgsmål | Svar |
| Hvad er firewallens opgave i et netværk? | Skabe en sikkerhedsbarriere mellem et privat netværk og det offentlige netværk. |
| Hvad er en access control list? | Det er en liste med adresser som fortæller en firewall om hvilke adresser er kan gå ind og ud af netværket. (Allow/Deny) |
| Hvad kan en firewalls regler være baseret på? | IP-adresser/Domain navne/Protokoller/Programmer/Ports/Søgeord-Nøgleord. |
| Hvilke typer firewalls findes der? | Host-baseret firewall - Software firewall installeret på computeren, beskytter kun den computer. (Windows Firewall, Avast m.m.)  Netværk-baseret firewall – Kombination af hardware og software, beskytter hele netværket. |

## Del 3 – Tilegnelse og test af viden om hacking

Se videoen [Hacking challenge at DEFCON](https://www.youtube.com/watch?v=fHhNWAKw0bY) og besvar herefter spørgsmålene i skemaet.

|  |  |
| --- | --- |
| Spørgsmål | Svar |
| Hvad er social engineering? | Person-hacking – Brug svagheder i et netværk (udgiv dig for at være en anden) for at få adgang til følsom information. |
| Hvordan beskytter man sig mod social engineering? | Sørg for at du kun giver adgang til nogen som allerede har en form for adgangskode. Sørg for at du ikke videregiver information som en person ikke behøver at blive oplyst om. |
| Hvad er phishing? | Det er hvor du ringer og prøver at efterligne en anden (kæreste, eller selve personen) og ved hjælp af social engineering, får adgang til følsom information. |
| Hvordan beskytter man sig mod phishing? | Hvis du bliver kontaktet af en som ikke har en adgangskode til f.eks. ens bank/telefonnetværk, så kan du ikke give/ændre den nuværende adgangskode. Send en mail til vedkommende at der er blevet ringet op omkring ændring af kode og opfordrer til at ringe igen med adgangskode for at ændre den. |

## Del 4 – Tilegnelse og test af viden om malware

Se videoen [Different Types of Malware Explained | How does Anti-malware Detects them?](https://www.youtube.com/watch?v=JZOLa7_LShk) og udfyld herefter tabellen med forklaring på de enkelte begreber. Brug Internet til at finde et eksempel på navn på hver af disse typer.

|  |  |  |
| --- | --- | --- |
| Type | Forklaring | Eksempel på navn |
| Virus | Kan kopiere sig selv og sende til andre computere. Kan spredes ved at vedhæfte sig selv med andre filer. Kan kun udføre instrukser hvis brugeren kører programmet. Virussen kan slette og korrupte systemfiler. | Nimda, ILOVEYOU, Stuxnet. |
| Orm | Skal ikke have brugeren til at køre programmet for at udføre instrukser. Kan sprede af sig selv ved at udnytte netværket eller system sårbarheder. Designet til at overbelaste et webservice ved at bruge båndbredde. | Morris Worm, Nimda, SQL Slammer, Conflicker, Welchia. |
| Trojaner | Kommer ind i brugerens computer forklædt som en normal fil eller program. Kan give fjernadgang eller stjæle fortrolig information til hackeren. Kan også downloade kraftige malware og virke som spyware. | Nimda, Tinba, Shlayer. |
| Rootkit | Bruges for at få fjernadgang til en computer uden at blive opdaget. Køre filer på computer, ændrer indstillinger, ændre software og sikkerhedssoftware, stjæle fortroligt data og installere farligt malware via fjernadgang. | Knark, Zero Access, Adore, Fudmodule Da IOS, Spicy Hot Pot. |
| Ransomware | Krypterer brugerens data og kræver løsepenge for at få adgang til data igen ved hjælp af en dekrypteringsnøgle. Skal betales i form af Bitcoin som ikke let kan spores. | CryptoLocker, Bad Rabbit, NotPetya, WannaCry. |
| Bot | Bruges til at udføre en serie af instrukser automatisk. Bruges til at udføre DDOS angreb for at få adgang til servere. | MaXiTE, Bagle, Torpig, Storm, Sality. |
| Spyware | Optager browser historie, søgnings historie, bank login detaljer, kreditkort detaljer og keylogger som optager brugerens indtastninger. Sendes over internettet til udvikleren. | Advanced Keylogger, CoolWebSearch, FinSpy, Gator, GO Keyboard, HawkEye, HuntBar. |

## Del 5 – Test af kompetencer

1. Gå på opdagelse i [The Malware Museum](https://archive.org/details/malwaremuseum) og afprøv mindst 10 forskellige klassiske virus. Virus kører i en virtuel maskine, så du skal ikke være nervøs for at der sker noget med din egen PC.
2. Prøv at hente filen [eicar.com](https://secure.eicar.org/eicar.com) – hvad sker der når du downloader denne?

Kan ikke hente noget: ”X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H\*”

1. Undersøg Windows Defender, som er den indbyggede antivirus i Windows. Har den identificeret nogle farer?

Nej

1. Gennemfør en [fuld scanning af din PC](https://tweak.dk/computer/windows-defender-offline) med Windows Defender. Identificerer denne nogle farer?

Nej

## Kriterie for færdiggørelse

Opgaveløsningen er færdig når du…

* Har læst eller set materialet i del 1 og besvaret de tilhørende spørgsmål
* Har set materialet i del 2 og besvaret de tilhørende spørgsmål
* Har set materialet i del 3 og besvaret de tilhørende spørgsmål
* Har set materialet i del 4 og forklaret de enkelte typer af malware
* Har løst opgaverne i del 5

… eller når dagsplanen angiver en ny aktivitet.