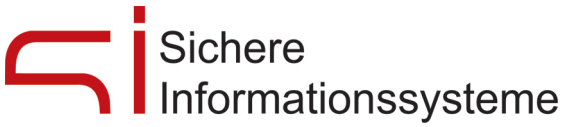


Netzwerk- und Kryptopraktikum (NKP4)

Challenge 06 – D A R K

Markus Zeilinger

SoSe 2023

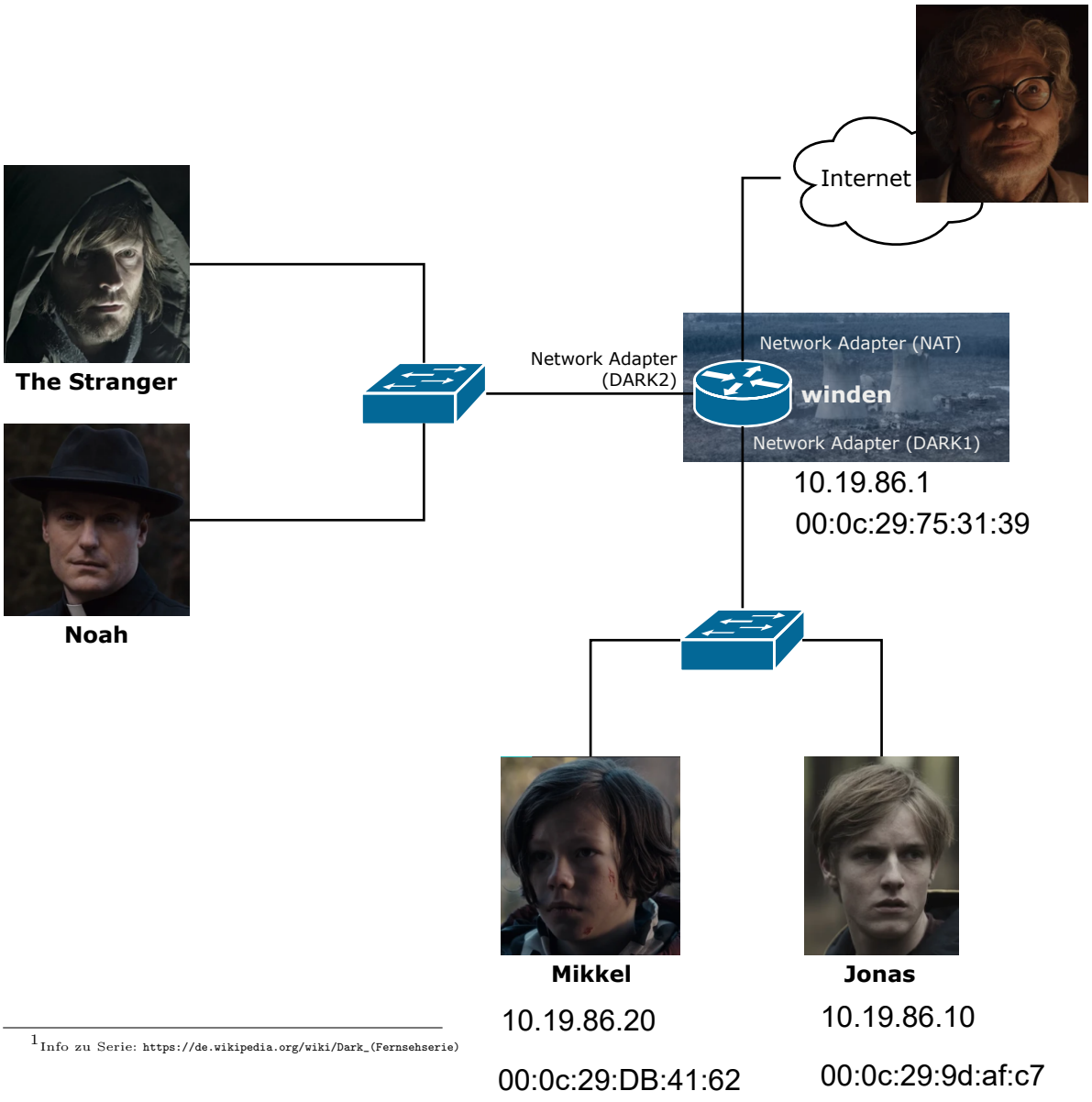
Ausgangslage

23. Juni 2020, die Apokalypse naht. Jonas Kahnwald[1] bleiben nur mehr wenige Tage, um die Katastrophe zu verhindern. Dazu muss er unbedingt wissen, was der geheimnisvolle Fremde (thestranger) vom Uhrmacher und Entwickler der Zeitreisemaschine H. G. Tannhaus erfahren hat.

Ziel

Jonas Ziel ist es also (und damit deines), dieses Geheimnis zu erfahren und damit hoffentlich die Katastrophe zu verhindern.

Netzplan



[1] Info zu Serie: https://de.wikipedia.org/wiki/Dark_(Fernsehserie)

Teilaufgabe 1 – Inbetriebnahme & Information Gathering

- Lade zunächst die für die Aufgabe notwendingen VMs via Moodle herunter, entpacke das Archiv und öffne die VMs in VMware Workstation (VMware Workstation 16.x oder höher, VMware Fusion 12.x oder höher).
- Konfiguriere die virtuelle Verkabelung der VMs korrekt (`winden`: Network Adapter (NAT), Network Adapter 2 (LAN Segment `DARK1`), Network Adapter 3 (LAN Segment `DARK2`), `mikkel` & `jonas` (LAN Segment `DARK1`), `thestranger` & `noah` (LAN Segment `DARK2`).
- Starte die VMs! Die VMs `jonas`, `mikkel`, `thestranger` und `noah` sind gelinkte Clone von VM `winden`, daher muss möglicherweise der Pfad dorthin neu ausgewählt werden. Wegen der Pfadänderung frägt VMware Workstation beim Start, ob die VM kopiert ("I copied it" oder verschoben ("I moved it") wurde (nachdem wir in keinem gemeinsamen Netzwerk arbeiten und die VM `winden` am Interface in Richtung Internet im NAT-Modus betrieben wird, kann für alle VMs "I moved it" gewählt werden).
- Angreifer-System `jonas`: Zugangsdaten (`toor` + `toor123`), es können und müssen Packages nachinstalliert werden. Du kannst statt der vorhandenen VM `jonas` auch ein anderes System (z. B. Kali VM) verwenden. Acht dabei darauf, dass diese andere VM dann in Bezug auf Netzwerk so konfiguriert wird/ist wie die VM `jonas`!
- Sammle im nächsten Schritt mit geeigneten Tools möglichst viele Informationen über das gegenständliche Netzwerk und die Systeme darin!

Teilaufgabe 2 – Eavesdropping

Du hast einen konkreten Anhaltspunkt für dein Vorgehen und zwar, dass es Kommunikation im geswitchten Netzwerk, in dem sich `jonas` befindet, gibt. Versuche mit einer geeigneten Angriffstechnik an diese Kommunikation zu gelangen!

Teilaufgabe 3 – Sic Mundus Creatus Est

Ab hier hängt dein weiteres Vorgehen von deinen Erkenntnissen in Teilaufgabe 2 ab. Wähle auf Basis der aufgezeichneten Kommunikation eine geeignete Angriffstechnik, um an das gesuchte Geheimnis zu gelangen!

Warnhinweis

In gegenständlicher Aufgabe werden offensive Angriffs-Tools eingesetzt. Achte darauf, dass du diese Tools auch wirklich nur im Kontext der Aufgabe und gegen die in der Aufgabe verwendeten VMs einsetzt! Es ist nicht Teil der Aufgabe andere Systeme, insb. Systeme außerhalb des virtualisierten Netzwerks anzugreifen!