Arbeitsauftrag 3

**ICMP-Port-Sperrung erweitern:**



Um ICMP-Flooding zu simulieren habe ich als erstes „hping3“ heruntergeladen.

Der Rest hatte wegen Fehler mit der IP-Adresse nicht funktioniert.

**Diskussion**

**Whitelisting:**

* Bietet Schutz im Darkweb vor Botnetz-Angriffe.
* Durch Whitelisting werden nur bestimmte Hosts erlaubt und der unerwarteter Traffic sofort als schädlich erkannt.
* Erlaubt nur Traffic von bekannten und vertrauenswürdigen Quellen

**Blacklisting:**

* Blockiert bekannte und schädliche IP-Adressen während alles andere erlaubt ist.
* Domäne die mit Darkweb Aktivitäten zu tun haben können verwendet werden um diese Quellen zu sperren.

**Schwachstellen von Whitelisting:**

* Änderungen in der Infrastruktur können Traffic blockieren wenn die Whitelist nicht regelmäßig aktualisiert wird.
* Hoher Aufwand für die Aktualisierung der Whitelist.
* Angreifer können die IP-Adresseneines vertrauenswürdigen Hosts ändern um eine Whitelist zu umgehen.

**Schwachstellen von Blacklisting:**

* Angreifer können IP-Adressen oft wechseln um Blacklist zu umgehen.
* Blacklist schützen oft nur vor bekannten Angreifern oder Angriffsmustern.