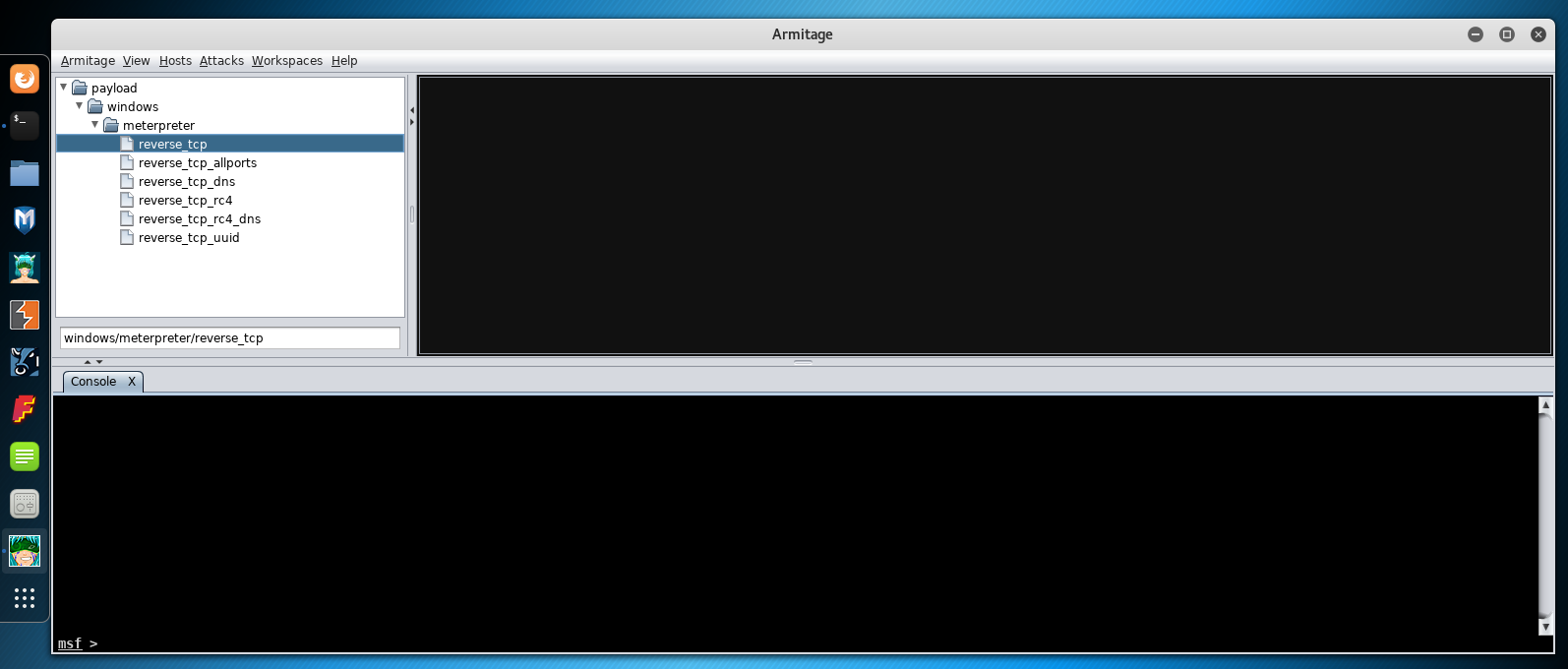
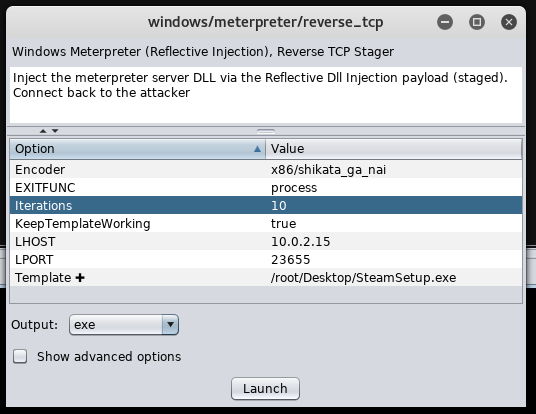
|  |  |
| --- | --- |
| **Angriffsbeschreibung** | |
| **Name:** Exploit Infiltration | **Hauptverantwortlicher**: Daniel Haering |
| **Ziel des Angriffs**: Datenklau und Kontrolle des gekaperten Systems | **Gefährdete Personengruppen**: Alle |
| **Beispiel eines Angriffsszenarios** | |
| Akteure: Odysseus (Dark Web Predator/Hacker), Priamos(Opfer) **Fallbeschreibung**:  Beginnen wir mit der Vorstellung unseres Predators und seinen Waffen. | |
| *1. Tool: Metasploit:* | |
| Beginnen wir mit seiner größten Waffe.  Unser Predator braucht gar nicht viel Wissen über das Hacken besitzen. Denn er besitzt das Betriebssystem Kali Linux mit vorinstalliertem Metasploit. Metasploit ist hauptsächlich eine Datenbank für bekannte Exploits und nützliche Payloads, die gewöhnlich in Assembler geschrieben wurden.  Dabei ergeben sich 2 Fragen:   1. Was ist ein Exploit? 2. Was ist eine Payload? | |
| * 1. *Ein Gleichnis* | |
| Als Hilfestellung versuchen wir es mit einem Gleichnis, weil dieses beim Hacken so häufig verwendet wird. Nennen wir unseren Hacker mal Odysseus und unser armes Opfer Priamos und das System des Priamos Troja. Unsere Schwachstelle ist der „Segen der Götter“. Odysseus entwickelt nun eine List (siehe Exploit). Hierbei baut er das Trojanische Pferd (schon wieder Exploit) um mit seinen Soldaten (siehe Payload) in die Stadt (System) zu kommen.  Vorsicht: Der Computer Trojaner ist ähnlich, aber nicht das Gleiche. Der Vergleich funktioniert hier aber auch. | |
| * 1. *Exploit* | |
| Damit das ganze nicht zu einfach ist hat Exploit 2 Bedeutungen. Es ist zum Einem das Schadprogramm das eine Schwachstelle nutzt um einzubrechen und dann eigenen Code auszuführen. Zum anderen ist es aber auch Teil des Exploits, nämlich nur der Schlüssel um einzubrechen (Trojanisches Pferd) | |
| * 1. *Payload* | |
| Dahingegen ist die Payload der Code der Ausgeführt werden soll, wenn die Sicherheitslücke durchbrochen wurde. Somit das eigentliche Ziel des Angreifers. In unserer Geschichte sind es die Soldaten, die wenn sie erst einmal in der Stadt sind ihre eigenen Ziele verfolgen. | |
| *2.) Das Vorgehen* | |
| Zu Beginn startet der Predator einmal das Metasploit Framework und zur Vereinfachung auch die grafische Oberfläche Armitage | |



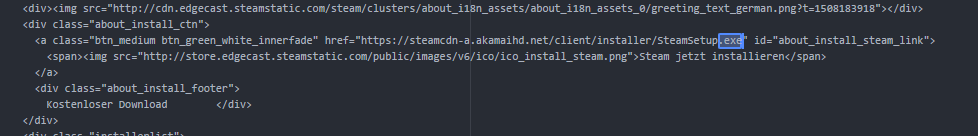
|  |
| --- |
| Hier gibt der Hacker nun Windows/meterpreter/reverse\_tcp ein. Dabei handelt es sich um eine Payload die eine direkte tcp Verbindung zum Opfer ermöglicht und kompletten Zugriff auf das Zielsystem. |
| *3. Widerherstellen der Datei mit Recuva* |



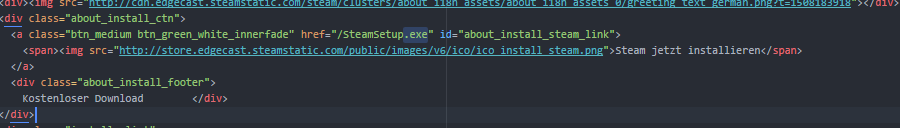
|  |
| --- |
| Nun stellt der Predator die Optionen wie oben dargestellt ein. Wichtig ist hier vor allem, dass man sich den Port merkt auf dem man lauschen will. Anschließend klickt er auf launch und kann seine Falle platzieren.  Um diese einzuschleusen gibt es unterschiedliche Möglichkeiten. Unser Predator hat sich für das Vortäuschen einer bekannten Seite entschieden |



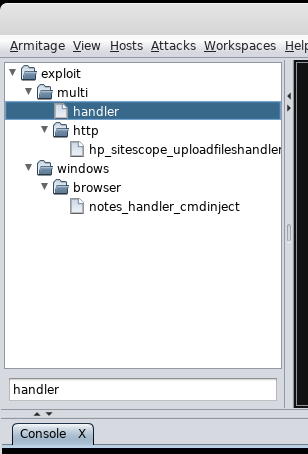
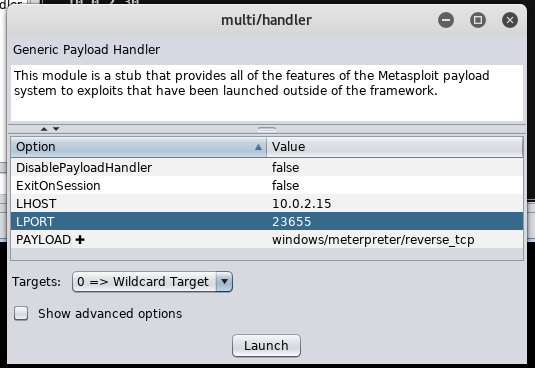
|  |
| --- |
| Dies ist die ganz normale Steam Download Seite. Hier lässt sich der Hacker den Quelltext anzeigen und kopiert diesen in eine lokale Datei. Anschließend muss er nur den Link zum Download ändern |
| *Vorher* |



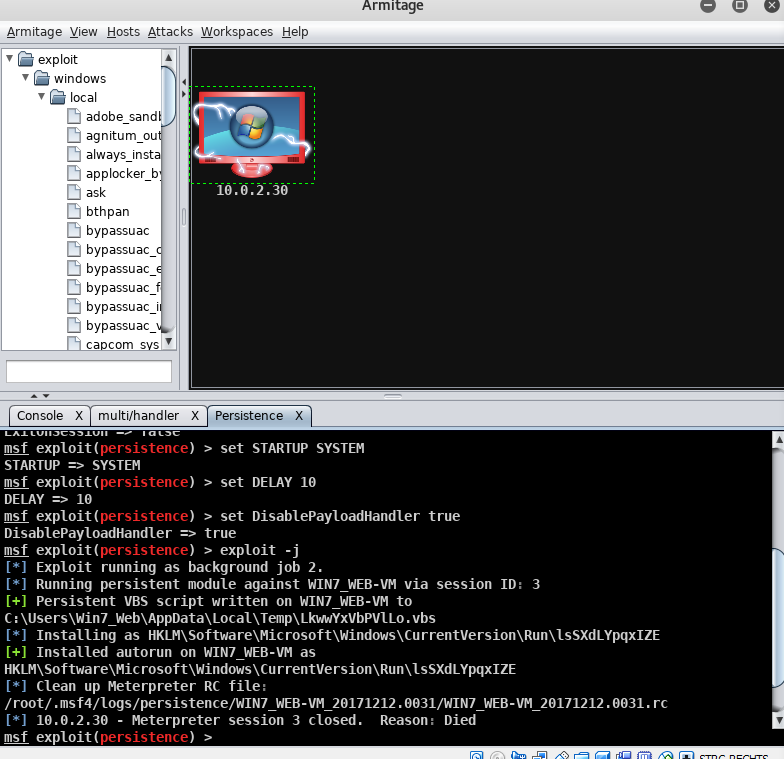
|  |
| --- |
| *Nachher* |



|  |
| --- |
| Nun kann der Hacker die Seite mit der infizierten Datei hochladen. Hierfür eignet sich die Domain von Steam mit einem kleinen unauffälligen Tippfehler. Der Link zu dieser Seite kann dann einfach in passendem Kontext in einem Forum gepostet werden und die ahnungslosen Nutzer Laden sich die präparierte Datei herunter.  Der Köder ist nun ausgesetzt. Unser Hacker muss nun aber noch ein Netz auswerfen in das die Fische gehen können. Hierfür muss ein Multihandler mit folgenden Optionen erstellt werden. Hier ist nun auch wieder der Port relevant |



|  |
| --- |
| Wenn nun ein Fisch ins Netz gegangen ist kann man dies direkt in der Armitage Oberfläche sehen und über einfache Klicks Screenshots, Keylogger erstellen oder gar eine versteckte Konsole öffnen. Auch der Datei Upload und Download kann hier direkt verwendet werden. Einfach mit rechtsklick auf den Rechner und die Optionen genießen |



|  |
| --- |
| **Schutzmaßnahmen** |

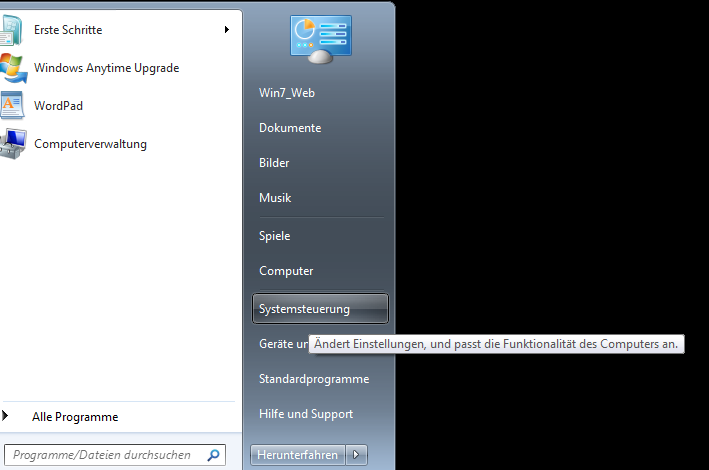
|  |
| --- |
| 1. **Updates** |
| Updates stehen für die meisten Menschen synonym mit Verbesserungen, Aufwertungen. Sie beinhalten aber auch den Punkt Fehler zu korrigieren oder Lücken zu schließen, meist als Patch bezeichnet.Diese wird häufig außeracht gelassen und kann von einem Hacker ausgenutzt werden um einen Metasploit bzw. Exploit Angriff auszuführen, da dieser Angriff sich gezielt Schwachstellen sucht um diese für seine Zwecke zu nutzen.Deswegen ist es Sinnvoll sobald ein Update erschienen ist, dieses auch auszuführen. Der Hacker kann schließlich auch sehen, dass ein Update für dieses Programm rausgekommen ist und so wird ihm sogar die Arbeit abgenommen die Schwachstelle selbst herauszufinden. Ohne Update kann er diese Schwachstelle noch immer ausnutzen. |

|  |
| --- |
| 1. **Nutzer mit eingeschränkten Rechten** |
| Die größte Schwachstelle ist der Mensch. Um zu verhindern das ein Metasploit Angriff erfolgen kann, ist eine der Besten Möglichkeiten die Zugriffsrechte des Nutzers einzuschränken. Den Nutzer kann man kontrollieren, den Angreifer nicht. |

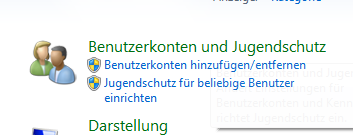
|  |
| --- |
| Windows Account mit eingeschränkten Rechten |
| Ein Beispiel für einen Nutzer mit eingeschränkten Rechten ist ein Standardnutzer bei Windows. Dies bedeutet er hat keine Administrator Rechte und kann gewisse Änderungen, die ein Angriff gerne ausführen würde, nicht ausführen. Dies verhindert nicht den Angriff, sondern sorgt für eine Schadensbegrenzung bzw. verhindert den allgemeinen Zugriff oder den Zugriff auf sensible Daten. |
| Voraussetzung: Admin muss Passwortgeschützt sein und Standardnutzer darf dieses nicht kennen. |
| *1. Klick auf das Windows Symbol* |



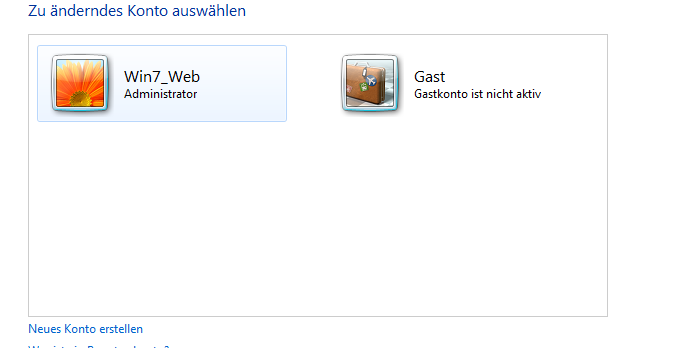
|  |
| --- |
| *2. Klick auf Systemsteuerung* |



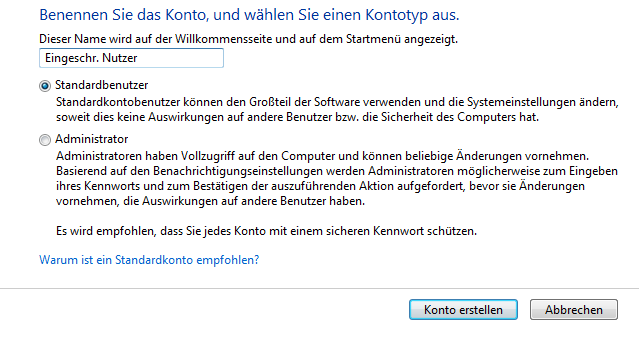
|  |
| --- |
| *3. Unter Benutzerkonten und Jugendschutz: Benutzerkonten hinzufügen/entfernen* |



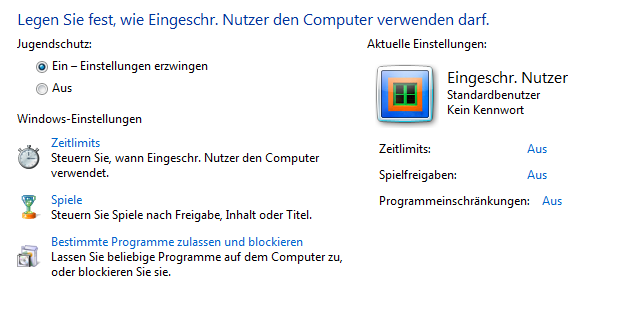
|  |
| --- |
| *4. Untem im Fenster auf neues Konto erstellen Klicken* |

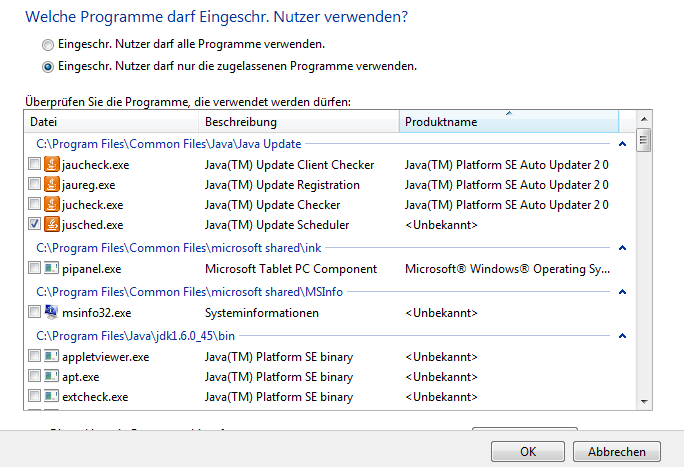


|  |
| --- |
| *5. Nutzer bennen und die Standardeinstellung Standardbenutzer ausgewählt lassen* |

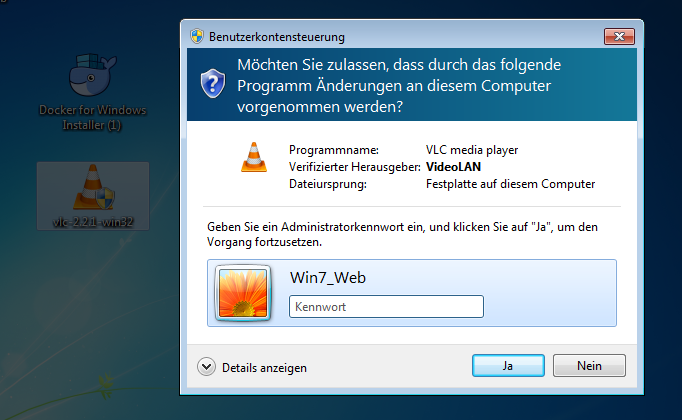


|  |
| --- |
| *6. Einstellungen Überprüfen und auf Konto erstellen klicken* |
|  |
| *7. Weitere Einstellungen: PW und einschränkungen* |





|  |
| --- |
| Der Nutzer kann nun keine Programm Instalieren oder ausführen die Adminrechte benötigen oder vom Admin eingeschränkt wurden |



|  |
| --- |
| 1. **Docker Container** |
| Sollte die Möglichkeit der eingeschränkten Rechte bei Nutzer nicht gegeben sein, kann man die Zugriffsmöglichkeiten des Angreifers einschränken, indem man Anwendungen auf einem abgetrennten System laufen lässt. In diesem Fall Container. Hierbei wird eine abgekapselte Umgebung (abdocken -> Docker), welche Individuell gestaltet werden kann, erstellt. In folgenden wird Docker für Windows 10 genutzt und eine einfache Ausgabe erzeugt. Diese Ausgabe kann auch weiter vertieft werden, so dass Steam oder eine andere Anwendung ausgeführt werden kann. |
| Docker Container einrichten |
| Benötigtes Betriebssystem: Windows 10 Professional und EnterpriseBenötigte Update Version: 14393.222 oder Höher |
| *1. Update Version überprüfen durch ausführen von winver* In das Windowssuchfeld winver eingeben und die Applikation starten, sofern die Version 14393.222 oder Höher vorhanden ist kann Docker Installiert warden, ansonsten muss Windows erst geupdatet warden. |
|  |
|  |
| *2. Docker Installer herunterladen und Installieren* Auf https://store.docker.com/editions/community/docker-ce-desktop-windows kann Docker für Windows 10 heruntergeladen warden. |
|  |
| Installer ausführen |
| In der Shell den Befehl " & $Env:ProgramFiles\Docker\Docker\DockerCli.exe -SwitchDaemon ” ohne Anfürungszeichen ausführen und zum Windows Container wechseln, da Docker Standardmäßig Linux-Container ausführt. |
| *3. Container Image des nano servers installieren* Weiterhin in der Shell “ docker pull Microsoft/nanoserver “ um ein Basisimage zu erhalten. |
| “ docker images “ in der Shell ausgeführt liefert eine Liste der intallierten Images |
| *4. Nano Server starten und simples Skript ausführen* |
| Mithillfe des Befehls “ docker run -it Microsoft/nanoserver cmd ” wird ein Container bzw. die Commandozeile eines Containers gestartet.  Der Befehl “ powershell.exe Add-Content C:\helloworld.ps1 ‘Write-Host “Hello World” ‘ ” erstellt ein neues Skript. In diesem Fall ein für Informatiker bekanntes “Hello World” Skript.  Vogang kann mit “ exit “ beendet werden sobald dieser abgeschlossen wurde. |
| Der Befehl “ docker ps -a ” liefert eine ID, die mithilfe des Befehls “ docker commit <ID> helloworld ” ein “Hello World” Image erzeugt. |
| Mithilfe des Befehls “ docker run --rm helloworld powershell c:\helloworld.ps1 ” wird das Skript ausgeführt und es erfolgt eine Hello World ausgabe. |

|  |
| --- |
| 1. **Erkennung** |
| Sofern ein Angriff erfolgt ist, sollte eine Erkennung und Beseitigung erfolgen. Diese Erkennung gestaltet sich sehr schwierig. Ausnahme ist ein Radikales verhalten des Angreifers, sowie eine konstant Überwachte Umgebung und dem Wissen über Exploit Angriffe. Eine Beseitigung läuft im normallfall auf ein Neuaufsetzen des betroffenen Systems hinaus. |
| Erkennung mithilfe von squil und Wireshark |
| Mithilfe von dem Linux-System Security Onion und den dort enthaltenen Programmen, squil und Wireshark, besteht die Möglichkeit einen erfolgreichen Angriff zu erkennen. Dabei sind jedoch Kenntnisse über den Angriff, dessen Verhalten und dem Standardverhalten des eigenen Systems von Nöten. |
|  |
| *1. squil starten -> select all und Wireshark starten* |
|  |
| *2. agent status -> Type: pcap, snort und ossec -> Status up* |
|  |
| *3. Angriff ausführen* |
|  |
| *4. squil erkennt exploit versuche* |
|  |
| *5. Filter Wireshark nach Payload des Angriffs oder Filter nach “ frame contains “Meterpreter” ”* |
|  |
| *6. Rechtsklick Packet und Follow TCP Stream auswählen* |
|  |
| *7. Handshake hat stattgefunden, was auf einen exploit Angriff schließen lassen kann.* |
|  |

|  |
| --- |
| Schutz |
| Updates sind für jeden Nutzer relevant. Sie tragen dazu bei Lücken in Systemen zu schließen und erschweren Hackern den Zugriff auf ein System.  1. Weiterhin ist es wichtig, wenn man sich im Internet aufhält Links und Downloads aus dubiosen Quellen zu vermeiden und sich nur auf gesicherten und Vertrauenswürdigen Seiten aufzuhalten. 2. Sofern die Möglichkeit besteht können auch drastischere Maßnahmen getätigt werden, wie kein Internet auf diesem System. Ein Beispiel sind Krankenhäuser, in den Operationssälen ist es unter Umständen nicht notwendig aufs Internet zugreifen zu können, so dass dem Personal gar nicht erst die Möglichkeit gegeben wird sich auf Shopping Seiten Schuhe oder ähnliches anzusehen. 3. Nutzer mit eingeschränkten Rechten sind Hilfreich, wenn man einem Nutzer einschränken muss ohne dabei auf Internet zu verzichten. Dies triff meist auf Kinder bei privaten Nutzern und Angestellte in Firmen zu. Nutzern mit eingeschränkten Rechten fehlen die Adminrechte, welche von einem Installer benötigt werden. So kann verhindert werden, dass Steam oder andere Anwendungen auf diesem Rechner Installiert werden, was den oben erklärten Exploit-Angriff unmöglich macht. 4. Da die Einschränkung der Nutzer Wirksam ist, kann dies auch auf die Anwendungen erweitert werden. Mithilfe von Docker können Applikationen auf einem abgetrennten System ausgeführt werden. Dies Schränkt die Zugriffsmöglichkeiten des Angriffs ein und liefert, insbesondere für Betriebe, eine weitere Sicherheitsschicht. 5. Einen Metasploit-Angriff zu erkennen ist sehr schwierig, doch sobald er gefunden wurde bleibt meist nur noch ein Neuaufsetzen des Systems, da der Angreifer Zugriff besaß kann er endlose weitere Viren auf das System eingeschleust haben. |
| Fazit und Kommentare: Opimaler Schutz wird nur gewährleistet auf einem Vollständig abgekapselten System. Kein Internet und keine USB-Anschlüsse. Dies kann von Betrieben genutzt werden um wichtige Daten zu schützen.  Gutter Schutz wiid durch arbeiten mit abgekapselten System wie Docker geliefert, da dies den Angreifer einschränkt.  Nutzer mit eingeschränkten Rechten bieten mäßigen Schutz. Häufig ist dies nur für Private Nutzer mit Kindern Sinnvoll, da Programmierer und ähnliche Berufe auf vollständige Rechte angewiesen sind.  Einfachen Schutz bietet das vorsichtige Vorgehen von einem Selbst. Sowie regelmäßiges Updaten von Programmen.  Nur durch die Kombination von mehreren Schutzmaßnahem kann ein sehr guter Schutz erzielt werden. Leider sind Menschen nicht Perfekt und Fehler bei Programmen oder dem Verhalten von Menschen können jederzeit auftreten. Jedoch besteht die Möglichkeit dieses Risiko einzuschränken und entsprechende Level der Sicherheit zu schaffen, um entsprechenden Schutz zu gewährleisten.  Private Nutzer sollten darauf achten ihre Programme akutell zu halten und dubiose Internetseiten bzw. Downloads zu vermeiden.  Betriebe können dies erweitern indem Sie weitere Sicherheitsebenen einbauen. Nutzer einschränken und auf abgekappselten Systemen arbeiten. |