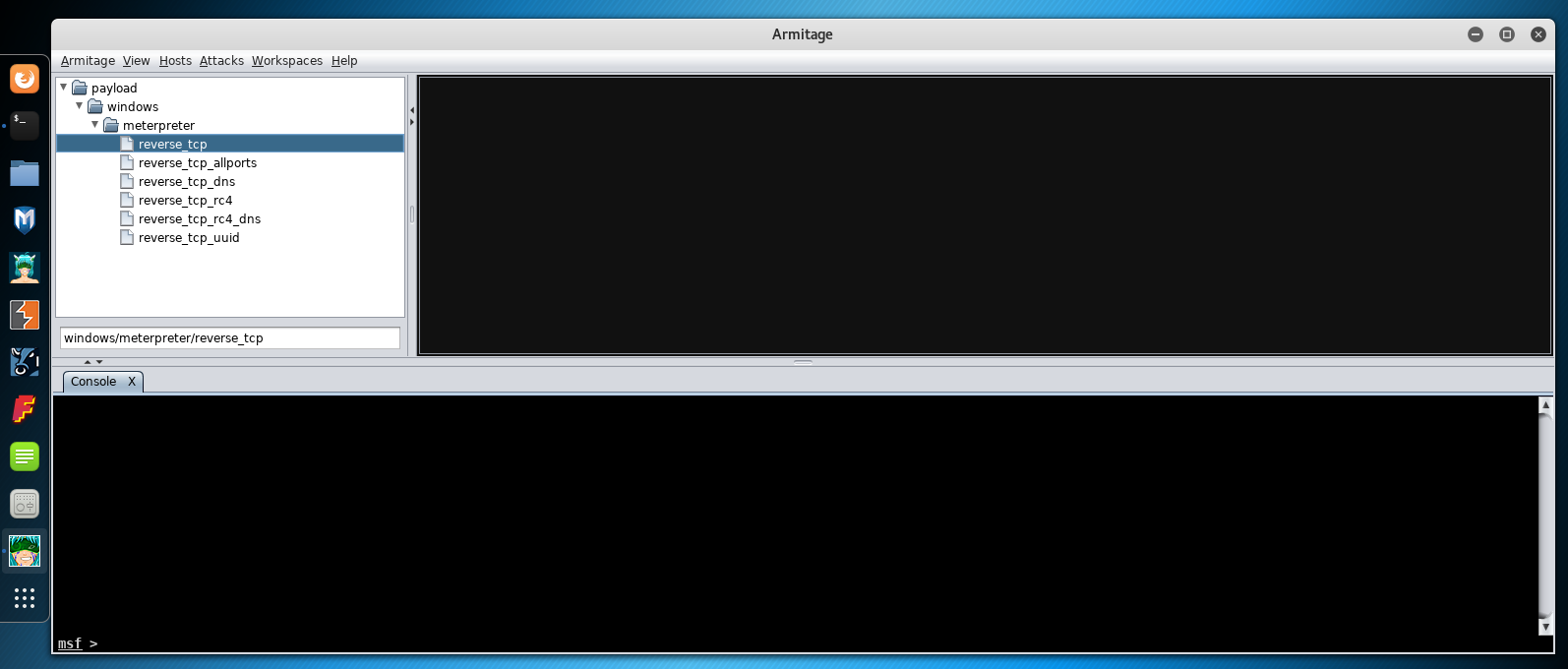
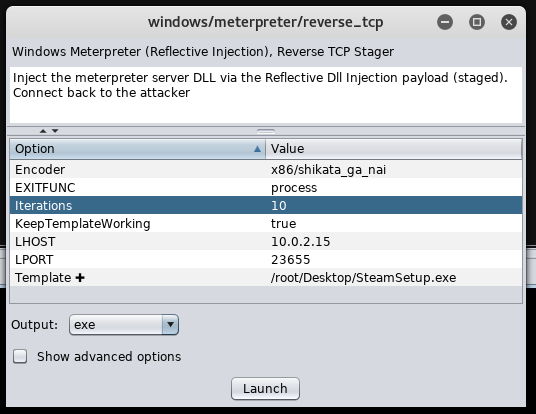
|  |  |
| --- | --- |
| **Angriffsbeschreibung** | |
| **Name:** Exploit Infiltration | **Hauptverantwortlicher**: Daniel Haering |
| **Ziel des Angriffs**: Datenklau und Kontrolle des gekaperten Systems | **Gefährdete Personengruppen**: Alle |
| **Beispiel eines Angriffsszenarios** | |
| Akteure : Odysseus(Dark Web Predator/Hacker) , Priamos(Opfer) **Fallbeschreibung**:  Beginnen wir mit der Vorstellung unseres Predatoren 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 userer Geschichte sind es die Soldaten, die wenn sie erst einmal in der Stadt sind ihre eigenen Ziele vefolgen. | |
| *2.) Das Vorgehen* | |
| Zu Beginn startet der Predator einmal das Metasploit Framework und zur Vereinfachung auch die grafische Oberfläche Armitage | |



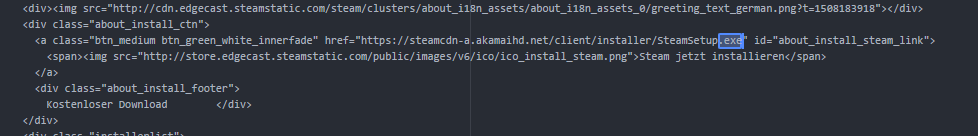
|  |
| --- |
| Hier gibt der Hacker nun windows/meterpreter/reverse\_tcp ein. Dabei handelt es sich um eine Payload die eine direkte tcp Verbindung zum Opfer ermöglicht und kompletten Zugriff auf das Zielsystem.  Sobald das Programm gestartet wird öffnet sich eine tcp Verbindung zu der zu der angegebenen IP und dem entsprechenden Port. Hier herüber wird eine Shell an den Angreifer gesendet. Der Angreifer braucht dann nur einen Handler starten, der diese Shell entgegen nimmt. Da der Angreifer die Shell nur annehmen muss und er diese nicht sendet ist es eine revverse\_tcp Verbindung. Wenn der Angreifer die Shell sendet nennt man dies forward\_tcp |
| *3. Widerherstellen der Datei mit Recuva* |



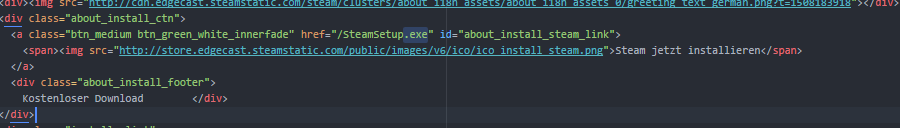
|  |
| --- |
| Nun stellt der Predator die Optionen wie oben dargestellt ein. Wichtig ist hier vor allem, dass man sich den Port merkt auf dem man lauschen will. Anschließend klickt er auf launch und kann seine Falle platzieren.  Um diese einzuschleusen gibt es unterschiedliche Möglichkeiten. Unser Predator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



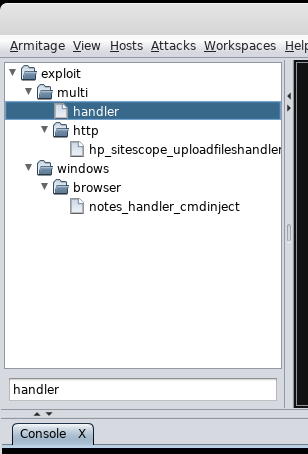
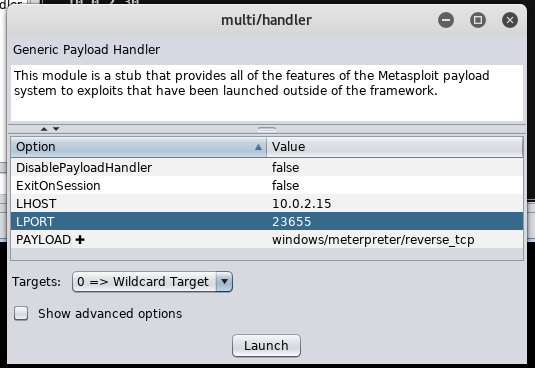
|  |
| --- |
| Dies ist die ganz normale Steam Download Seite. Hier lässt sich der Hacker den Quelltext anzeigen und kopiert diesen in eine lokale Datei. Anschließend muss er nur den Link zum Download ändern |
| *Vorher* |



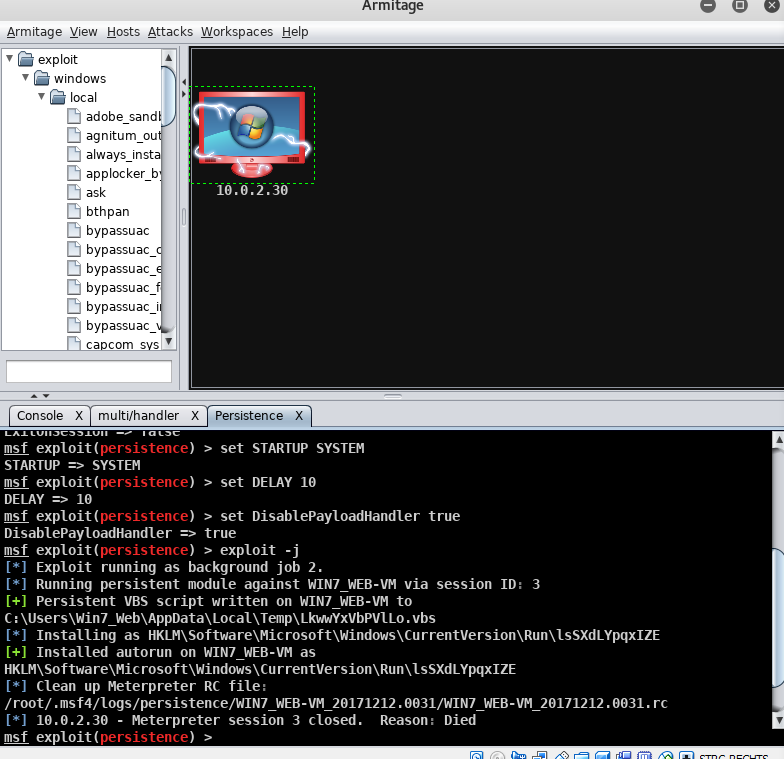
|  |
| --- |
| *Nachher* |



|  |
| --- |
| 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. Dieser nimmt dann die vom Exploit gesendete Shell entgegen und kann darüber dem infizierten System befehle geben. |



|  |
| --- |
| 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 |
| Um sich gegen so einen physischen Angriff zu schützen, kann man seinen USB-Stick sicher überschreiben. Zum Beispiel mit dem Programm: Abylon Shredder. Mit diesem wird der Speicherplatz überschrieben und der Angreifer kann somit Dateien nicht widerherstellen. |
| *5. Sicheres Löschen der Datei* |

Ein Bild, das Screenshot enthält.

Mit sehr hoher Zuverlässigkeit generierte Beschreibung

|  |
| --- |
| *6. Das Programm recuva erkennt die Datei noch……* |

Ein Bild, das Screenshot enthält.

Mit sehr hoher Zuverlässigkeit generierte Beschreibung

|  |
| --- |
| *6. Die Datei kann jedoch nicht mehr so widerhergestellt werden, wie sie ursprünglich war* |

Ein Bild, das Screenshot enthält.

Mit sehr hoher Zuverlässigkeit generierte Beschreibung

|  |
| --- |
| Ein Encodieren der Zeichen ist auf keinen Fall möglich. |
| **Kommentare**:  Das Programm Abylon Shredder besitzt 5 verschiedene Sicherheitslevel:  0: normales Löschen – Verknüpfungen entfernen  1: 2x überschreiben mit binären Nullen  2: 3x überschreiben mit Nullen und Zufallszahlen  3: 7x überschreiben nach DoDII-Methode  4: 13x überschreiben DoDII und Zufallszahlen  5: 35x überschreiben (Peter Gutman Methode)  Diese Möglichkeit schützt nicht davor, wenn man vertrauliche Daten in Dateinamen schreibt. |

Zusätzlich:

Eingehen auf Verfahren der Speicherung von Daten?!(Technik genauer beschreiben?!)Warum ist es dann sicher etc.