Usermanual for ITSecX

Erik Brändli

June 18, 2015

1 Einleitung

EditierenITSecX ist die Abkürzung für "IT - Security - Extreme". ITSecX lässt sich mit dem von uns zur Verfügung gestellten Devices verbinden.
Die interne Syntax ist C # . Das Hauptziel des Projektes ist es zu zeigen, wie einfach man Daten Abfangen und auswerten kann und Amateur Pen-Testern die Möglichkeit zu geben, schnell dynamisch an Ziele gelangen. Es ist auch möglich aus der zur Verfügung gestellten Software weit mehr rauszuholen (gegen Aufpreis).
Dieses Handbuch besteht vorranging aus einer Funktionsreferenz, Erläuterungen zu den wichtigsten Features und weitere ergänzende Informationen.

1.1 Autoren und Mitwirkende

Das Projektteam bestand aus 5 Mitgliedern von denen aktuell noch 2 vorhanden sind.

-) Erik Brändli
-) Hüseyin Bozkurt
~~-) Markus Schulmeister~~
~~-) Arian Sayah~~
~~-) Raied El'beidak~~

Projektabnehmer:

-) Michael Borko
-) Werner Kristufek
-) Erich Trenner
-) Elisabeth Wildling

1.2 Autoren und Editoren

Folgende Personen verdienenen Anerkennung dafür, dass Sie wesentlichen Inhalt zum Handbuch beigetragen haben und/oder weiterhin beitragen werden: Hüsyein Bozkurt und Erik Brändli.

Vielen Dank!

1.3 Einsatzgebiet

Als Einsatzgebiet sind Schulen mit IT-Ausbildung gedacht, da man dort den Schülern lehren, kann wie einfach es ist ein Netzwerk auszutricksen bzw. um zu veranschaulichen, dass Netzwerksicherheit ein wichtiger Part in unserer Welt ist.

Denn die meisten Schüler denken, dass ihre Daten sicher sind, und dass niemand mitlesen kann!

2 Vorbereitung des Produktes

Sollten Sie bereits unser modifiziertes "Arch Linux" besitzen können Sie dieses Kapitel überspringen.

2.1 Vorausgesetztes

Um das Produkt zu verwenden erwerben Sie am besten unser "Arch Linux" von unserer Seite, oder Sie insatllieren sich zu Ihrer Arch Linux version folgende Pakete dazu:

-) Openssh
-) openbsd-netcat
-) nmap
-) tcpdump
-) dsiff

2.2 Erstellen eines tcpdump-services

Falls Sie nicht unser modifiziertes "Arch Linux" verwenden müssen Sie sich einen Service schreiben welches einen tcpdump startet auf einem von Ihnen ausgewählten Interface startet. Dieser Dump muss in eine Datei geschrieben werden, wie dies funktioniert finden sie auf der Seite von tcpdump.(http://www.tcpdump.org/)

2.3