

Usermanual for ITSecX

Erik Brändli

June 20, 2015

Version	Name	Datum	Status	Unterschrift
v 1.0.1us	Erik	18.06.2015	unstable	
v 1.0.1ps	Erik	18.06.2015	pretty-stable	
v 1.0.1s	Erik	19.06.2015	stable	
v 1.0.1	Hüseyin Bozkurt	21.06.2015	Freigeben	

1 Inhaltsverzeichnis

Contents

1	Inhaltsverzeichnis	2
2	Einleitung	3
2.1	Autoren und Mitwirkende	3
2.2	Autoren und Editoren	3
2.3	Einsatzgebiet	3
3	Vorbereitung des Produktes	4
3.1	Vorausgesetztes	4
3.2	Erstellen eines tcpdump-services	4
3.3	Erweiterungen	4
4	Installation des Produktes	4
5	Inbetriebnahme	4
6	Funktionen	5
6.1	Datei	5
6.1.1	IP Settings	5
6.1.2	Import → Settings	5
6.1.3	Export → Settings	5
6.1.4	Verbindung → verbinden	5
6.1.5	Verbindung → trennen	6
6.2	Tools	6
6.2.1	IP Settings	6
6.2.2	Import → Settings	6
6.3	Files	6
6.3.1	IP Settings	6
6.3.2	Import → Settings	6
6.4	Window	6
6.4.1	IP Settings	6
6.4.2	Import → Settings	6
7	Schritt-für-Schritt Beispiel	6
8	Rechtliche Hinweise	6

2 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 vorrangig aus einer Funktionsreferenz, Erläuterungen zu den wichtigsten Features und weitere ergänzende Informationen.

2.1 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

2.2 Autoren und Editoren

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

Vielen Dank!

2.3 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!

3 Vorbereitung des Produktes

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

3.1 Vorausgesetztes

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

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

3.2 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/>)

3.3 Erweiterungen

Um folgende Dinge müssen Sie sich kümmern:

-) Es sollte sich der Tcpdump bei Systemstart von alleine starten.
-) Sudo befehl muss ohne Passwort erfolgen

4 Installation des Produktes

Führen Sie den gelieferten Installer aus um die Software zu installieren.

AxNetworks ist eine wichtige externe Komponente, damit die Software auf dem Windowsgerät läuft. Nach erfolgreicher Installation ist das Produkt voll einsatzbereit.

5 Inbetriebnahme

6 Funktionen

In diesem Kapitel werden die Funktionen der Gui erklärt bezüglich ihrer Anwendung und Auswirkung

6.1 Datei

6.1.1 IP Settings

In "**IP Settings**" lässt sich festlegen zu welchem Device man sich verbinden möchte. Man findet zwei maskierte Eingabefelder wieder. Das Eingabefeld mit IP-Address nimmt die IP-Adresse(v4) vom Device entgegen und validiert ob diese IP korrekt ist. Das Feld nimmt eine bis zu 4 stellige Zahl zur Definierung des Kommunikations-Port am Device. Mit dem Knopf "**Apply Settings**" können Sie die Einstellungen übernehmen. "Discard Settings" verwirft die temporäre Konfiguration.

6.1.2 Import → Settings

Ermöglicht das Importieren von Konfigurationen bezüglich:

-) **Verbindung-Punkt (IP:Port)**
-) **Authentifizierung (Username, Passwort)**

Ein OpenFileDialog öffnet sich und bittet Sie darum eine Datei auszuwählen, eine **.conf** Datei (Die Sie mit unserer Software erstellten, siehe auch Kapitel ??) Desweiteren wird die Verbindung sofort getestet um zu überprüfen ob die übergebenen Daten korrekt sind, und das Device verfügbar ist. **Dies kann in gewissen Fällen länger dauern.**

6.1.3 Export → Settings

Ermöglicht das Exportieren von Konfigurationen bezüglich:

-) **Verbindung-Punkt (IP:Port)**
-) **Authentifizierung (Username, Passwort)**
-) Interface-Settings (Schriftfarbe, Hintergrundfarbe, ...)

Desweiteren wird empfohlen eine Setting erst dann zu exportieren wenn die Verbindung bereits getestet wurde. **Diese Datei enthält sensible Daten bitte schützen Sie sich selbst, indem Sie diese Datei schützen**

6.1.4 Verbindung → verbinden

Über diesen Menüpunkt verbindet man sich zum Device, dafür ist jedoch erforderlich, dass Sie Ihre Daten in die Felder "Username" & "Passwort" eintragen. Danach bestätigen Sie Ihre Eingabe mit dem Button "**Apply + Login**", durch das klicken auf den Button

probiert das Programm sich zu dem Device zu verbinden.

6.1.5 Verbindung → trennen

Mit der Funktion trennen lässt sich die Kommunizierschnittstelle zurücksetzen, folglich sind Sie vom Device getrennt.

6.2 Tools

6.2.1 IP Settings

6.2.2 Import → Settings

6.3 Files

6.3.1 IP Settings

6.3.2 Import → Settings

6.4 Window

6.4.1 IP Settings

6.4.2 Import → Settings

7 Schritt-für-Schritt Beispiel

8 Rechtliche Hinweise