Usermanual for ITSecX

Erik Brändli

June 21, 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

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 vorranging 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 verdienenen Anerkennung dafür, dass Sie wesentlichen Inhalt zum Handbuch beigetragen haben und/oder weiterhin beitragen werden: Hüsyein 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 insatllieren 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 installlieren.
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 Kommunikationis-Port am Device. Mit dem Knopf "**Apply Settings**" können Sie die Einstellungen übernehmen. "Discard Settings" verwirft die temporäre Konfiguration.
Bild

6.1.2 Import → Settings

Ermöglicht das Importieren von Konfigurationen bezüglich:
-) **Verbindung-Punkt (IP:Port)**
-) **Authentifizierung (Username, Passwort)**
Ein OpenFile Dialog öffnet sich und bittet Sie darum eine Datei auszuwählen, eine **.conf** Datei (Die Sie mit unserer Software erstellten, siehe auch Kapitel 6.1.3) Desweitern 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, . . .)
Desweitern 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 Menupunkt 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.
Bild

6.1.5 Verbindung → trennen

Mit der Funktion trennen lässt sich die Kommunizierschnittstelle zurücksetzen, folglich sind Sie vom Device getrennt. um sich erneut zu verbinden müssen Sie alle Settings neu eingeben, oder Sie laden eine Konfiguration über Import → Settings (6.1.2)

6.2 Tools

Hier befinden sich jene Tools die das Device ausführen kann, Konfigurationen für diese Tools werden automatisch geladen bzw. in einem Fenster für Sie bereit gestellt, dass sie nur mehr auswählen müssen wer & was.

6.2.1 Scanner → nmap

nmap ("Network Mapper") ist ein Tool womit Sie einen fremden Computer:
-) prüfen können ob dieser Ein-/Aus-geschalten ist
-) schauen weleche Ports offen hat
-) evtl. erkennen welches Betriebsystem auf diesem Computer läuft.
-) wie weit dieser Computer entfernt ist Hier bei ist nicht die Rede von wie viele Meter ist dieser Computer weg, sondern wieviele netzwerktechnische zwischen Punkte es gibt.
Bild

6.2.2 Sniffing → tcpdump → start/stop

tcpdump legt die Netwerkpakete in einem Logfile(**.pcap**) ab.
Mit der Funktion **start** wird der "Dump" in eine Datei geschrieben.
! Sollte es bereits gestartet sein, wird dieser neugestartet.
Mit der Funktion **stop** wird der "Dump" angehalten.
Bild

6.2.3 Direct Command

Über diese Funktion ist es möglich einen Befehl am Device auszuführen, denn evtl. möchten Sie selbst etwas auslesen oder umstellen.
Bild

6.3 Files

Mit den Funktionen in diesem Menü können Sie mit den Logs und Datein arbeiten, also diese Anzeigen und herunterladen.

6.3.1 View File

Hier können Sie in dem Sie die auf der linken seite eine Datei auswählen diese anzeigen. **Bild**

6.3.2 View tcpdump

Wenn Sie diese Aktion ausführen wird der aktuelle tcpdump im Hauptfenster ausgegeben. **Da diese Daten erst konvertiert werden müssen kann dies eine gewisse Zeit in anspruch nehmen!** **Bild**

6.3.3 View tcpdump → Download

Sollten Sie diese Funktion auswählen kommt ein "speichern unter" Dialog diesen müssen Sie bestätigen, dann wird der aktuelle tcpdump an dieser Stelle gespeichtert. **Bild**

6.4 Window

In diesem Menüpunkt können Sie den angezeigten Ausgabetext optisch bearbeiten.
Bild

6.4.1 Set Fontcolor

Hier können Sie die Textfarbe wählen.

6.4.2 Set bgcolor

Hier können Sie die Hintergrundfarbe wählen

6.4.3 Clear

Mit dieser Funktion leeren Sie die Ausgabe im Hauptfenster

7 Schritt-für-Schritt Beispiel

8 Rechtliche Hinweise