Facts - Termine

Dauer: **15.02. – 13.03.2013**

Anmeldeschluss: **13.2.2013**

Registrierung: ab **30.1.2013** möglich unter supportnwt@fhstp.ac.at
(Website ist ab Registrierungsstart verfügbar).

Preisverleihung:
Im Rahmen der Tage der offenen Tür am **16.3.2013, um 11 Uhr** an der FH St. Pölten.

Inhalt:
Challenges in unterschiedlichen Schwierigkeitsstufen zu Themen aus dem Bereich der IT Security. Die Aufgaben sind sowohl praktischer als auch theoretischer Natur.

Sieger/In: meisten Punkte (pro Institution) und pro Kategorie

Gewinn: Apple iPad, Sachpreise

Teilnehmen kann jede/r Schüler/in oder Teams (wird empfohlen) aus den berufsbildenden höheren Schulen, sowie aus der AHS (Oberstufe); der Bewerb ist in zwei Kategorien mit unterschiedlichen Schwierigkeitsgraden unterteilt und ermöglicht sowohl Schulen mit fortgeschrittenem technischem Background (zB HTL) als auch allen anderen Schulen (zB AHS, HAK) sich mit gleichwertigen GegnerInnen zu messen. Die Wahl der Kategorie steht natürlich jedem Team individuell frei. Die Teilnahme ist **kostenlos**!

Spielregeln: Die Spielregeln werden gemeinsam mit dem Szenario veröffentlicht.

Ansprechpartner:

- DI Christoph Lang-Muhr, BSc
- Daniel Haslinger, BSc
- Erreichbar unter: supportnwt@fhstp.ac.at

Voraussetzungen

- Zunächst natürlich ein möglichst **motiviertes Team** :-) Die Einbettung der Challenge in den Unterricht ist keine Voraussetzung aber erfahrungsgemäß förderlich.
  Es ist möglich, pro Schule auch mehrere Teams zu registrieren.

- Spaß an Technik und Herausforderungen.
  Ob Hacking, investigative Recherche oder logische Kombinationsgabe: geplant ist jedenfalls ein möglichst breites Spektrum an Aufgabenstellungen.

- Zugang zum Internet mit **freiem Port 1194 / udp & tcp**.
  Dies ist notwendig, um die Zielsysteme zu erreichen. Bitten Sie Ihren Administrator ggf. um Freischaltung dieses Ports.

Ablauf

- Dauer: 4 Wochen, freie Zeiteinteilung
- Der Zielserver steht rund um die Uhr zur Verfügung
- Technische und theoretische Aufträge werden in einem virtuellen Szenario erledigt
- Punktevergabe erfolgt nach Schwierigkeitsgrad
- Punktestand aller Teams kann während der Challenge auf einem interaktiven Ladder verfolgt werden (genannt werden nur die selbstgewählten Teamnamen)
- Die ersten 3 Plätze werden am Ende der Challenge inklusive Name der Schule veröffentlicht

Mögliche Themen

Bereits vor Beginn der Challenge erhalten die TeilnehmerInnen eine Liste an Themengebieten, auf welche sie sich vorbereiten können.

Beispiele:

- Forensik
- Steganographie
- Cross Side Scripting (XSS)
- SQL-Injection
- Kryptographie
- Command Injection
- Malwareanalyse
- . . .