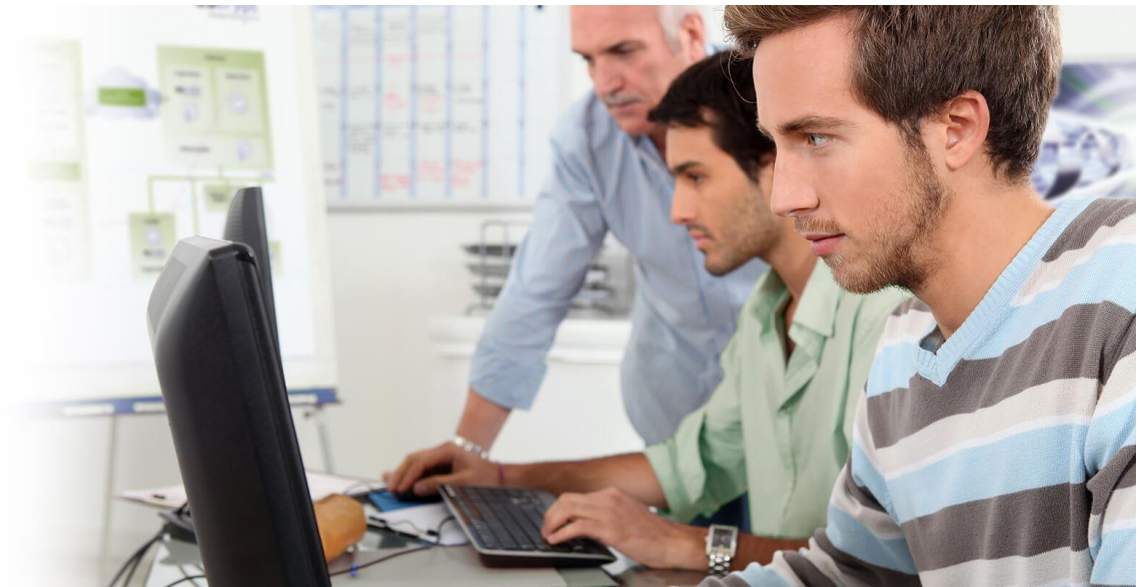
Penetration testing for Basic Infrastructure

日程 **2018年7月5日(木)～6日(金) 9:00~17:00**

Venue **UDX CONFERENCE 6F (秋葉原)**

Organizer **株式会社ナノオプト・メディア**



BASIC INFRASTRUCTURE HACKING

開催概要

このコースでは、豊富なハッキングツールやテクニックを習熟できます。
非常に基本的なものから始まりますが、数多くの演習を通じて様々なツールについて深く学び、ペンテスターやハッキングのプロにとっても有益な未知の側面を知ることができます。このコース全体を通じてツール同士の相関関係を検討し、各種ツールをただ列挙するだけではなくツール同士の相関関係から次のツールを最大限活用する方法を分析します。受講者の皆さんには、インフラストラクチャーのハッキングに関連するさまざまなコンポーネントをハッキングするためのツールとテクニックを使用できるだけではなく、ここでしか学べない秘密のテクニックを知ることによってツールの動作する概念をしっかり理解し今後活用できるレベルまで到達させます。

スケジュールとカバー分野

Basic Infrastructure Hacking - Day 1

- Module 1: ポートスキャニングの技術
- Module 2: オンラインパスワード攻撃の技術
- Module 3: データベースをハッキングする技術
- Module 4: Metasploit基礎
- Module 5: パスワードクラッキング
- Module 6: Unixのハッキング

Basic Infrastructure Hacking - Day 2

- Module 7: Unix上でのアプリケーションサーバーのハッキング
- Module 8: サードパーティーのCMS Softwareのハッキング
- Module 9: Windows Enumeration
- Module 10: クライアント側の攻撃
- Module 11: Windows上でのアプリケーションサーバーのハッキング
- Module 12: ポストエクスプロイテーション
- Module 13: Windowsドメインのハッキング

受講対象者

・システム管理者

・SOCアナリスト

・初級～中級くらいのペネトレーションテスター

・ネットワークエンジニア

・セキュリティスペシャリスト

・さらにスキルアップしたい方

受講のメリット

・受講後30日間はハックラボにいつでもアクセス可能。このコースで学んだ内容を復習する最適な環境です。

・コース受講中に、たくさんのスクリプトやツール、手引きが提供されます。

・ロゴ付き修了証明書の授与

受講者の声 (一部抜粋)

・攻撃側の手法を学べる機会があまりないので受講出来てうれしかったです。Metasploitは前から存在だけは知っていましたが、さわる取っ掛かりがなく長いこといじってみたいと思っていたので良い機会でした。

・とても勉強になりました。しっかりと自分の力になるよう復習したいと思います。また受けたいです。

・とても有益な情報が多く、実践的な内容であり、資料も詳しく書かれていて今後も役に立つと思います。

・思っていたよりも難しいところもあったので、ついていくのが大変でしたが、覚えなければいけない事がたくさんあると気づかされてとても良い経験をさせていただきました。ありがとうございました。

講師 ※当日は通訳が入ります

Will Huntは、約10年間IT セキュリティ業界に従事している情報セキュリティ専門家です。
ハイエンドのITセキュリティコンサルティングとトレーニングを提供するITセキュリティ専門企業である NotSoSecure (www.notsosecure.com)ではDirectorを務めています。それ以前にも、彼は、大手 IT セキュリティ企業のための技術および非技術的なトレーニングを開発し、提供するペンテスターでした。それ以前のWillは、経験豊富なデジタルフォレンジックコンサルタントとトレーナーとして活躍していました。
Willはブログstealthsploit.comを運営しており、さまざまなソフトウェアの脆弱性を特定し明らかにし続けています。

受講料

第1次早期割引：￥195,000（税抜）締め切り：2018年5月25日(金)

第2次早期割引：￥235,000（税抜）締め切り：2018年6月22日(金)

通常申込：￥275,000（税抜）

※2日間の昼食代を含みます

受講に必要なPC環境

このコースは管理者権限とルートアクセスがあるノートパソコンだけあれば参加できます。
このクラスでは、英国のデータセンターでホストされている最新のハックラボへのVPNアクセスを提供します。ラボに接続すると、関連するすべてのツールやVMが見れるようになり、ハックラボの各参加者に専用のKali VMを提供しています。したがって、VMを持ち込む必要はありません。
必要なのは、VPNクライアントをインストールして接続するための管理者権限だけです。

当日の持ち物

管理者権限とルートアクセスがあるノートパソコンを持参してください。
また、このクラスではネットワーク接続を利用します。
ネットワークに接続できるご用意をお願いします。（無線LAN接続になります）

アクセス

JR秋葉原駅電気街口から「アキバブリッジ」を通って徒歩3分。
秋葉原へは、都心を結ぶJR山手線の他、京浜東北線、
総武線及び東京メトロ日比谷線、銀座線（末広町駅）、
つくばエクスプレスが接続しています。

路線名	駅名	出口	所要時間
JR 線	秋葉原駅	電気街口	徒歩3分
東京メトロ 日比谷線	秋葉原駅	3番出口	徒歩4分
東京メトロ 銀座線	末広町駅	1番出口	徒歩3分
つくばエクスプレス	秋葉原駅	A1出口	徒歩3分

受講に関するお問い合わせ:
Cyber Security Expert Training 運営事務局　営業担当(ナノオプト・メディア内)
TEL：03-6258-0590　FAX：03-6258-0598　Email: contact@f2ff.jp