1. 講座名	Practical ECU hacking
2. 講座概要	本講座では、IPネットワークを経由したECUシステムへの侵入 及び 暗号アルゴリズム解析 を、ハンズオン形式で体験する 具体的には、 1：IPネットワークを経由したECUシステムへの侵入 ポートスキャン、実行中のサービスを調査、サービスの脆弱性を利用した攻撃、別ユーザーの権限奪取までを体験する 2：UDS Security Access暗号アルゴリズム解析 暗号処理の実行時間測定とソースコード解析、Keyを推測、Security Access成功までを体験する これにより、攻撃者の視点、思考や攻撃の仕組みを理解し、ECUのセキュリティ確保に役立てて頂くことを目的とする
3. 想定する受講者	自動車業界のエンジニアで実践的なセキュリティ技術を学びたいと考えている方
4. 習得する技術	NMAPを使ったポートスキャン、実行中のサービスに対する脆弱性調査手法とECUへの攻撃手法、暗号アルゴリズム解析手法
5. 受講の前提条件	・簡単な英会話スキル(本講座は弊社Vulnerability Researcherが英語で行います/日本人スタッフも同席しサポートします) ・情報セキュリティ及びUDS Security Accessの基礎的な用語を理解している ・講師の指示に従ってLinux(NMAP, SSH)のコマンド入力が出来る ・講師の指示に従ってPythonでコードを書ける ・C++のコードを読める(ソースコードを解析して頂くため)
6. 日数（時間数）	1日(6.5時間)
7. 最大受講人数	8人(4グループ)
8. セミナー講師	White Motion 講師
9. 受講者の制限	無し
10. 実習機材	1グループ(2名)につき、下記機材1セットを貸し出します ・PC ・ターゲット基板(Raspberry Pi)
11. 到達目標	演習で行う一連の攻撃プロセスを理解する
12. 講座計画	[午前] 1：IPネットワークを経由したECUシステムへの侵入(2時間) - Linuxのターミナル上でNMAPを使用し、ターゲット基板に対して、ポートスキャンを行う - オープンポートから実行中のサービスを調査 - サービスの脆弱性を利用し、Webサーバー 及び SSHコマンドにより ターゲットのシステムへ侵入、別ユーザーの権限を奪取するまでを体験する [午後] 2：UDS Security Accessの暗号アルゴリズム解析 ①サイド・チャネル・アタック(1時間) - Pythonでエクスプロイトコードを作成し、PC内に仮想的に構築したECUに対して、Security Accessコマンドを送信 - 暗号処理の実行時間からKeyを推測し、Security Access成功までを体験する ②単純な暗号アルゴリズムの解析(1.5時間) ③複雑な暗号アルゴリズムの解析(2時間) - 講座用に準備したソースコードより、暗号アルゴリズムを解析 - Pythonでエクスプロイトコードを作成し、Security Access成功までを体験する
13. 開催時期	2019年12月13日(金)