Milano, 10 luglio 2014

Spett.le

**Università degli Studi di Milano - Dipartimento di Informatica**

**Segreteria degli Studenti**

**Via Comelico 39**

**Oggetto: Collaborazione HT s.r.l. / sig. Andrea di Pasquale**

La presente lettera per attestare che il Sig. ANDREA DI PASQUALE , nato a Catania il 2 febbraio 1989, ha collaborato e collabora tutt’ora con la scrivente azienda.

HT S.r.l. è una azienda informatica attiva nel campo della Sicurezza Informatica e più in particolare nella produzione, sviluppo e commercializzazione di software.

Il sig. Andrea di Pasquale ha svolto inizialmente un Tirocinio Formativo retribuito dal 16 maggio 2012 al 15 novembre 2012 con la mansione di Sviluppatore SW. Il percorso formativo, in affiancamento agli sviluppatori Senior della Società, prevedeva lo sviluppo di funzionalità di interesse per i prodotti dell’azienda in ambiente Wi-fi con cifratura forte e analisi di modalità di iniezione di codice all’interno di diversi formati di file.

Successivamente, in data 1 febbraio 2013, il Sig. Di Pasquale ha stipulato un contratto di apprendistato della durata di 36 mesi e scadenza al 31 gennaio 2016, con la qualifica di Apprendista Impiegato e la mansione di Sviluppatore Software.

Si allega alla presente lettera un resoconto delle tematiche e delle attività che hanno visto e che vedranno coinvolto il sig. Di Pasquale nel corso del presente rapporto di lavoro.

Restiamo a Vostra disposizione per ulteriori chiarimenti,

Distinti Saluti,

HT s.r.l.

Direttore Generale

Giancarlo Russo

**Allegato:**

**Attività svolte durante il periodo di collaborazione del sig. Andrea di Pasquale**

L’obiettivo delle attività svolte presso HT s.r.l. da parte di Andrea Di Pasquale è stato quello di partecipare allo sviluppo del prodotto, chiamato *Network Injector*, il cui scopo principale è l'alterazione dei contenuti all'interno di pagine Web durante il trasferimento di rete dai server ai browser dei client.

Nello specifico Andrea di Pasquale ha contribuito alle seguenti attività:

1. Sviluppo del prodotto su reti Wi-Fi (standard IEEE 802.11 a/b/g/n)
2. Integrazione, modifica e sviluppo di moduli di attacco, simulazione e di configurazione all'interno del prodotto quali:
   1. *Wireless Intruder*: cracking delle password su reti Wi-Fi con cifratura WEP64, WEP128, WPA, WPA2, WPS
   2. *Fake Access Point*: simulazione di reti Wi-Fi in caso di non presenza fisica di reti Wi-Fi utilizzabili
   3. *Physical Unlock*: rimozione temporanea e ripristino delle password su sistemi operativi desktop tramite collegamenti Firewire/Thunderbolt per mezzo di SBP2 DMA
   4. *System Management*: configurazione del prodotto per l'accesso in remoto al sistema tramite reti Ethernet, Wi-Fi e 3G
3. Sviluppo delle GUI relative al prodotto, chiamate *Appliance Control Center* e *Tactical Control Center* affinché tutte le funzionalità offerte dal prodotto siano user-friendly per i clienti
4. Sviluppo del pacchetto di installazione e di aggiornamento del prodotto tramite la pacchettizzazione *Deb* fornita dai sistemi *Debian-like*

Lo sviluppo del prodotto *Network Injector* ha richiesto inoltre l'utilizzo e la modifica di diversi software esterni:

1. Personalizzazione della ISO di *Linux Ubuntu* in versione OEM per ospitare il prodotto
2. Modifica del tool *cryptsetup* per la cifratura/decifratura automatica del sistema *Linux Ubuntu* tramite *dm-crypt*
3. Integrazione e modifica dei moduli/driver relativi a periferiche Ethernet, Wi-Fi e 3G su kernel *Linux* 3.5
4. Modifica del tool *iw* della suite *iw-tools* per il corretto supporto alle reti Wi-Fi su standard IEEE 802.11n
5. Integrazione e modifica della suite *aircrack-ng* per l'analisi, la simulazione e l'attacco di reti Wi-Fi IEEE 802.11. Nello specifico sono state richieste le seguenti modifiche:
   1. Aggiunto supporto per reti Wi-Fi di ultima generazione su standard IEEE 802.11n a 2.4/5 Ghz
   2. Migliorata la procedura di riautenticazione dei client connessi con cifratura WPA/WPA2 identificando i falsi positivi
   3. Corretti alcuni problemi sul simulatore di Access Point
   4. Corretta la decifratura CCMP/AES dei frame con cifratura WPA/WPA2 in presenza di QOS
6. Integrazione del tool *reaver* per l'attacco di Access Point con tecnologia WPS
7. Integrazione e modifica del tool *inception* per ripristinare le condizioni originali del sistema una volta concluso l'attacco

Durante lo sviluppo del prodotto sono state utilizzate le seguenti tecnologie su sistema operativo *Linux*:

* *Python*
* *C*
* *Bash*
* *GTK+ 3*