]HackingTeam[

Training

Training Sessions Schedule Attempt for
General Intelligence Presidency of Saudi Arabia
Milan, February 2th 2011

Part 1:

IT Security Fundamentals

HT S.r.l.
Headquarters: Via della Moscova, 13 20121 Milano
Tel: +39.02.29060603 – Fax: +39.02.63118946
e-mail: info@hackingteam.it – web: http://www.hackingteam.it
P.IVA: 03924730967 – Capitale Sociale: € 223.572,00 i.v.
N° Reg. Imprese / CF 03924730967 – N° R.E.A. 1712545

Session 1

Session 1.1:

?? Welcome reception

Session 1.2:

?? Linux basics

?? Windows basics

Session 1.3:

?? Ip and networking basics

Session 2

Session 2.1:

?? Firewall, IDS and IPS basics

Session 2.2:

?? Information_gathering

Session 2.3:

?? Introduction to hacking

HT S.r.l.
Headquarters: Via della Moscova, 13 20121 Milano
Tel: +39.02.29060603 – Fax: +39.02.63118946
e-mail: info@hackingteam.it – web: http://www.hackingteam.it
P.IVA: 03924730967 – Capitale Sociale: € 223.572,00 i.v.
N° Reg. Imprese / CF 03924730967 – N° R.E.A. 1712545

Session 3

Session 3.1:

?? Password cracking

Session 3.2:

?? Wireless Hacking

Session 4

Session 4.1

?? Introduction to exploiting

HT S.r.l.
Headquarters: Via della Moscova, 13 20121 Milano
Tel: +39.02.29060603 – Fax: +39.02.63118946
e-mail: info@hackingteam.it – web: http://www.hackingteam.it
P.IVA: 03924730967 – Capitale Sociale: € 223.572,00 i.v.
N° Reg. Imprese / CF 03924730967 – N° R.E.A. 1712545

Part 2:

Remote Control System advanced training

HT S.r.l.
Headquarters: Via della Moscova, 13 20121 Milano
Tel: +39.02.29060603 – Fax: +39.02.63118946
e-mail: info@hackingteam.it – web: http://www.hackingteam.it
P.IVA: 03924730967 – Capitale Sociale: € 223.572,00 i.v.
N° Reg. Imprese / CF 03924730967 – N° R.E.A. 1712545

Session 1

Session 1.1:

?? Welcome reception & teaming up.

?? RCS installation.

?? User Creation on RCS : teams create a user for each member, an activity and a belonging for the team and two targets, one for desktop and one for mobile.

?? Lesson**:** A glance to RCS attack vectors [optional

Session 1.2:

?? Hands-on:

SCENARIO 1: "Go There!"

Alessandro Del Piero uses Skype cyphered calls in order to organize criminal missions with his gang. We know where he usually sits and which his laptop is, but furthermore we've noticed that sometimes he leaves his notebook to drink a coffee. It's not possible to guess if he leaves the pc switched on or not. It's necessary to install RCS on his pc and find out who he's calling every day and what's the matter of the conversations…

HT S.r.l.
Headquarters: Via della Moscova, 13 20121 Milano
Tel: +39.02.29060603 – Fax: +39.02.63118946
e-mail: info@hackingteam.it – web: http://www.hackingteam.it
P.IVA: 03924730967 – Capitale Sociale: € 223.572,00 i.v.
N° Reg. Imprese / CF 03924730967 – N° R.E.A. 1712545

HT S.r.l.
Headquarters: Via della Moscova, 13 20121 Milano
Tel: +39.02.29060603 – Fax: +39.02.63118946
e-mail: info@hackingteam.it – web: http://www.hackingteam.it
P.IVA: 03924730967 – Capitale Sociale: € 223.572,00 i.v.
N° Reg. Imprese / CF 03924730967 – N° R.E.A. 1712545

Session 2

Session 2.1:

?? Hands-on:

SCENARIO 2: "The docs sharing"

After monitoring the network traffic, we discovered that between [target1 mail] and [target2 mail] email addresses there's a huge sharing of documents containing bad activity-related infos. We must find out the name of at least one of these guys and have a look in his face...

Session 2.2:

?? Hands-on:

SCENARIO 3: "Follow the smartphone"

We have to monitor constantly the location of the sims with numbers [target 1 number] and [target 2 number]. We must have a listening at the incoming

HT S.r.l.
Headquarters: Via della Moscova, 13 20121 Milano
Tel: +39.02.29060603 – Fax: +39.02.63118946
e-mail: info@hackingteam.it – web: http://www.hackingteam.it
P.IVA: 03924730967 – Capitale Sociale: € 223.572,00 i.v.
N° Reg. Imprese / CF 03924730967 – N° R.E.A. 1712545

and outcoming calls...

Session 3

?? Hands-on:

SCENARIO 4: "The on-line gamer"

Lionel Messi is a dangerous criminal and we must have access to his laptop and search the hard drive looking for some files of interest. We know that he usually have a drink in the HT Internet Cafè, and uses the protected wi-fi network to surf the web and to play on-line poker..."

HT S.r.l.
Headquarters: Via della Moscova, 13 20121 Milano
Tel: +39.02.29060603 – Fax: +39.02.63118946
e-mail: info@hackingteam.it – web: http://www.hackingteam.it
P.IVA: 03924730967 – Capitale Sociale: € 223.572,00 i.v.
N° Reg. Imprese / CF 03924730967 – N° R.E.A. 1712545

HOWTOs

U3 Thumb

1. Build your U3 .iso file from the RCS Console and save it on the Desktop
2. Install the application Universal Customizer - rename your .iso file with this name "U3CUSTOM.iso"
3. Overwrite your .iso file on the existing one to this path:

   C:\<installation path>\Universal_Customizer\BIN

4. Run the Universal Customizer application: "Universal_Customizer.exe" - follow the automatic steps

HOWTO: Injection Proxy Appliance in wi-fi scenarios

1. Check that Ipa is up and running and it's reachable by rcs server.
2. Get access to the IPA and edit the file /rcsipa/ect/rcsredirect.conf
3. Uncomment the variable "wifi-key" and assign the key of the network you want to monitor.
4. Check that the sniffing and the response interfaces are properly assigned in the file and that are up and running.
5. Check that the monitor interface is in monitor mode:

   > iwconfig [interface] mode monitor

1. Let the response interface join to the wireless network:

   > iwconfig [interface] essid [network] key [key]

1. Get access to rcs console and configure the ipa with the sniffing rules.

HOWTO: Remote Mobile Infection on Windows Mobile

1. Get access to the console, select a mobile backdoor and create a .CAB file in the Build section (it's also possible to trop it with another .CAB file).
2. Get access to the server where the Frontend of RCS is hosted

HT S.r.l.
Headquarters: Via della Moscova, 13 20121 Milano
Tel: +39.02.29060603 – Fax: +39.02.63118946
e-mail: info@hackingteam.it – web: http://www.hackingteam.it
P.IVA: 03924730967 – Capitale Sociale: € 223.572,00 i.v.
N° Reg. Imprese / CF 03924730967 – N° R.E.A. 1712545

3. Copy the .CAB in the location:
   C:\RCSASP\EXPREPO
1. Click on the WAP button and edit the Wap Push settings
2. Insert the target number
3. Insert the web URL pointing to the .CAB copied in the EXPREPO
4. Send the sms.

Target's info:

Target 1
Name: Alessandro Del Piero Mail: rcstarget1@yahoo.it Phone: +393666648647
Target 2
Name: Lionel Messi Mail: rcstarget2@hotmail.com Phone: +393349115122

HT S.r.l.
Headquarters: Via della Moscova, 13 20121 Milano
Tel: +39.02.29060603 – Fax: +39.02.63118946
e-mail: info@hackingteam.it – web: http://www.hackingteam.it
P.IVA: 03924730967 – Capitale Sociale: € 223.572,00 i.v.
N° Reg. Imprese / CF 03924730967 – N° R.E.A. 1712545

Notes:

HT S.r.l.
Headquarters: Via della Moscova, 13 20121 Milano
Tel: +39.02.29060603 – Fax: +39.02.63118946
e-mail: info@hackingteam.it – web: http://www.hackingteam.it
P.IVA: 03924730967 – Capitale Sociale: € 223.572,00 i.v.
N° Reg. Imprese / CF 03924730967 – N° R.E.A. 1712545