

Vol2 Issue 5 April/July .2012

SecurityKaizen

MAGAZINE

Mobile and Wireless Security

Interview with
Vivek Ramachandran
Founder of Security tube.net

Are We Ready For
Cyber war?

BLUEKAIZEN.ORG

How to hack
Mobile Applications?

CSCAMP November 2012

CALL FOR SPEAKERS..

SecurityKaizen
WWW.BLUEKAIZEN.ORG

Exhibition

CTF
Competition

Training

Sessions

Contents

Editor's Note

Couple of months ago, I bought my first smart phone "Samsung Galaxy Note with android platform".

New & News

In recent years we've witnessed the extraordinary lengths to which cyber criminals will go to breach target networks and steal valuable data for monetary or competitive gain.

True Story

Are we hacked?

By "We" I mean countries and individuals who use and depend on technologies that they didn't create, own or control.

Interview

With ... Vivek Ramachandran

A man that you have to respect....

Grey HAT

Sensitive services have been widely applied in mobile applications such as mobile banking and mobile trading.

Awareness

Wireless Security Awareness

Wireless security is actually a weak sauce and despite the fact of how Wi-Fi evolved in the past few years

Best Practice

I can imagine that some of the readers are saying, thanks god, I have not allowed Wi-Fi in my network so, I'm secure and I can flip the paper BUT, wait, unfortunately YOU ARE under Wireless threats even you've chosen not to install it and even if you believe that Encryption is enough for protecting your existing Wireless Network.

SK Magazine Team

SecurityKaizen
magazine

Chairman & Editor-In-Chief
Moataz Salah

Editors

Omar Sherin
Hassan Elhadary
Hemil Shah
Mohamed Bedewi
Hatem Ali
Joe Sullivan
Mohamed Enab
Vinoth Sivasubramanian

Website Development
Mariam Samy

Translation
Mai Alaa El-Dein

Marketing Coordinator
Mahitab Ahmed
Mohamed Saeed

Designed & Printed By
2DAY Adv.

Security Kaizen is issued
Every 3 months
Reproduction in Whole or
part without written permission
is strictly prohibited
ALL COPYRIGHTS ARE
PRESERVED TO
WWW.BLUEKAIZEN.ORG

改善

BLUE KAIZEN

Connecting Minds Improving Lives

For Advertisement In Security Kaizen Magazine and www.bluekaizen.org Website
Mail: info@bluekaizen.org Or Phone: 0100 267 5570

Editor's Note

Couple of months ago, I bought my first smart phone "Samsung Galaxy Note with android platform". I spent the first two weeks exploring the phone capabilities, installing and uninstalling many applications from the android market and I even explored the Internet for more .apk files.

Finally, I ended up with my stable environment having my main apps installed including configuring my Gmail, facebook and twitter accounts. But then I thought to myself why I don't also configure my admin access to bluekaizen.org on my new smart phone. Days later, I thought why not install the HSBC mobile app, that will make my banking transactions more fast and easy. After few weeks, you can say I rarely use my laptop now that I have most of my basic and advanced activities on my new galaxy note.

But suddenly it hits me, what if my smart phone was lost or stolen? Despite of the fact that I lost my 700\$, phone cost, I easily let the thief gain access to nearly all my digital identities!!

Imagine losing your mail access, your facebook and twitter accounts, especially if you run facebook pages or groups using this accounts; which may also affect your business reputation. Imagine losing access to your bank account, imagine losing confidential and important files, the phone's memory is 16Gbyte; of course I won't use it all for movies! That made me start to have a deeper look on different smart phone's threats and risks, not only physical theft, what about different malwares from tons of mobile applications that exist online, what about the privacy issues of those applications, what about the GPS and the

determination of location issues? If one is updating his location 24/7 on facebook or on Gtalk, I can wait for him to be outside his house and go steal it.

Threats are many and questions are endless that's why we decided to dedicate this issue to mobile and wireless security to put a spot on this emerging threats as we believe that different malwares and attacks will target different smart phones' platforms as number one target in the near future.

Second thing we want to announce in this issue is that Bluekaizen.org has decided, in an attempt to expand its team in order to reach more audience and to promote more its main purpose of existence: knowledge transfer and information sharing, to launch Bluekaizen Chapters.

Bluekaizen Chapters are small communities that share the goals and the dream of bluekaizen in different universities around the world. Today we have more than nine Bluekaizen chapters in different universities in Egypt (Cairo, Ain Shams, Alex, Helwan, AAST, MSA, AUC, Zagazig and Assuit)

Bluekaizen Chapters main activities will be including promoting the information security awareness in their community, build a database for people interested in information security, distribute the recent printed copy of security kaizen magazine, organize events and more.

Finally, we are glad to announce the launch of security kaizen labs 2012 that will be held next May in EBI in Nasr City where we will have the opportunity to meet all our beloved readers for the next time in few months after cscamp2011. Security Kaizen Labs is a two days event where all security training providers gather in one place to provide real Hands on, intensive training for the Security professionals and beginners, looking forward to seeing you all there.

BlackBerry®

Are we hacked?

STORY True

By "We" I mean countries and individuals who use and depend on technologies that they didn't create, own or control.

Traditionally, every country, group of people or individuals exercised full control and ownership over the information they created/own. Then came the Internet and the rules of the game changed forever. In June 2007 the government of France banned the use of the BlackBerry phones for all government officials and employees above a certain grade/level (See Figure 1). Around the same period other governments held undisclosed talks with the Canadian Company RIM (Research in Motion) owners of BlackBerry and many asked why?

In 2011 many countries across the world (Including Emirates, Saudi Arabia and India) raised the red flag for BlackBerry, threatening to ban the use of the technology and the devices within 60 days unless certain technical issues are remediated.

In order to understand why certain conscious governments and countries and privacy advocates are unhappy with how certain Cloud based communication companies like RIM for instance, handle information we need to understand the mechanics of the technology and how it works.

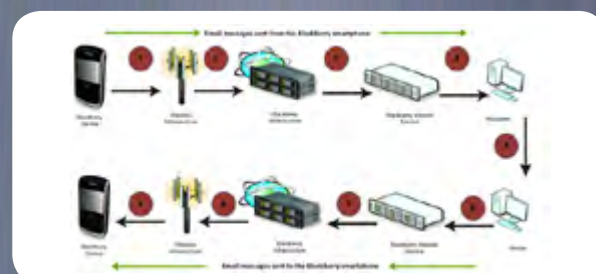
As per the figure (2) below, if you want to send an email to your friend (In the same city) once the email leaves your blackberry device, it travels through your GSM data network of your carrier (Vodafone, Mobinil or Etisalat) to the internet (Leaving Egypt) your email go straight into one of the strategically located



Figure 1 BlackBerry Banned in France

RIM/BlackBerry data centers around the world or what they call (BlackBerry Infrastructure). Depending on your carrier your email will most probably either end up in the UK, or Belgium!

As per RIM official documentation, throughout the email's entire journey it is compressed and scrambled "not readable to humans" using RIM's Proprietary technologies and a copy of the email is stored for 7 days in the BlackBerry data centers replicated across selected countries around the world in case the recipient was not



reachable.

The problem (From individual's Privacy and National Security Perspective) lies in step 3 (The BlackBerry infrastructure), it simply means that the entire electronic communication (Emails, Contacts, attachments...etc.) of hundreds of thousands of Egyptian users and users from other countries (Mostly developing countries) including big private companies and top government officials are stored outside the country using a proprietary technology that only RIM and Data centers hosting countries have access to.

Just as an example, if a top government official is sending or approving the Ministry's budget by email, or two local companies negotiating a take over or a merging deal. Or two friends communicate personal pictures or audio clips.

All of the above critical pieces of information leaves the country and gets stored in a black box at another country or countries, what if this treasure grove of information and tons of Data is analyzed and mined for intelligence information, important things like top government decisions or even the general public opinion and mood.

This might not be happening, but it's certainly a possibility and a threat that should not be taken lightly, or else why would countries like India issue a 60 days ban asking for step 3 (BlackBerry Infrastructure) to be hosted inside the country or have the right to any time access what information is leaving the country.

From the personal privacy side, not many users in Egypt know that when they chat on blackberry messenger or what is known as the BBM "a popular feature for an entire generation of young female users in Egypt" their entire conversation, text, images and audio clips are stored somewhere in Europe. BBM is not one to one conversation that no body listens to; some one definitely can if he wants. See figure 3



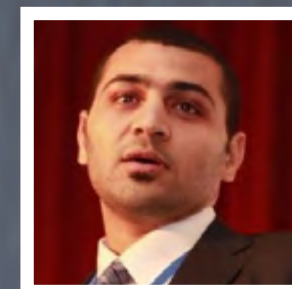
Once the BBM chatting message leaves your phone and carrier it leaves the country before being routed through the BlackBerry Infrastructure or cloud service to the recipient who might "ironically" be in the room next to you.

This is also true for IP based audio and voice conversation services, For example the main Skype data center in the Middle East is in Israel, nearly all the Middle East audio and video calls made on Skype are routed through Israel. Are we auditing those companies to know how they handle our information? Can someone guarantee that those millions of conversations taking place on a daily basis are not scanned for certain keywords for example?

The same idea or principle of personal, corporate or even government information being handled through third party cloud services owned, designed and operated outside of your legal jurisdiction or national authority is true for all of Google and android services, Apple's iCloud or even cloud based social networks like Facebook and twitter or image sharing platforms like Flickr or Pinterest.

So answering the title of the article, Yes we are all "Hacked".

Definitely we should use and encourage adopting technology, but it should be our technology. Till then, sent using Hotmail.



Omar Sherin

I am a certified CBCP, CRISC And ISO27001 LA and in my spare time an active blogger in CLIP.Wordpress.com

How to Hack Mobile Applications

Sensitive services have been widely applied in mobile applications such as mobile banking and mobile trading. Mobile banking applications, such as HSBC mobile banking Apps for Android, enable customers to make account management operations through their mobile application. Mobile trading apps, such as Amazon Mobile for iPhone, enable shopping online through a mobile application. In this article, we will walk through an approach to hack a mobile application in order to give highlight on exposed risks.

Our victim application

Let's assume that we have a mobile application which enables users to purchase products online. The mobile application connects to a web service hosted on a backend server using SOAP (Simple Object Access Protocol).

A simplified architecture diagram is shown in figure 1.



Figure 1: Architecture of victim mobile application



Our hacker will be a normal user having credentials to work with the mobile application. He will try to have unauthorized access to make money fraud.

Intercepting Traffic

Before we hack, we will need to understand how the application works in order to identify the attack surface and know the entry points for hacking. Thus, we need to understand the data flow which will allow us to understand how information is sent to and from the server. Moreover, we need to identify the contents and the sequence of the data sent and received while running the mobile application.

To achieve this, we need to intercept the traffic between the mobile application and the server. We will let the mobile application send traffic through our proxy. Web proxies, such as "Burp" [3], will be useful here as most mobile apps will use HTTP to communicate with their backend servers.

We have two options here:

- As shown in figure 2, we can configure the HTTP proxy settings in the mobile device to connect through our proxy. Note that if the traffic is sent over SSL, a warning will appear on the mobile app which can be ignored.
- Another way is to run the mobile app in an emulator and configure the emulator to connect to the internet through our proxy.

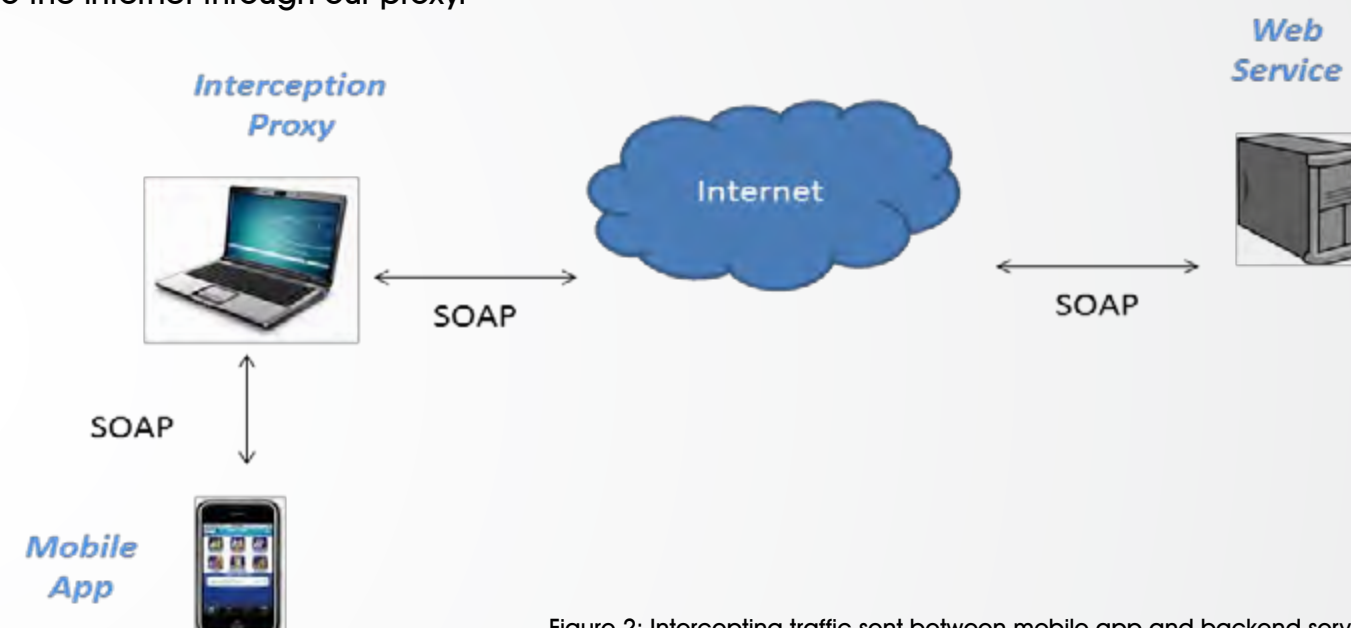


Figure 2: Intercepting traffic sent between mobile app and backend server

We will need to go through different screens on the mobile app and keep an eye on our proxy to watch how the traffic is sent between the mobile app and the backend server. It will help us identify the approach used by the application to communicate. Most mobile apps will use either REST (Representational State Transfer) which simply uses HTTP. Others might use SOAP which sends XML messages over HTTP. Thus, Burp will be so beneficial in intercepting and recreating traffic sent to backend services. For example, we can change the value of ProductID in the SOAP message intercepted as shown in figure 3.

Now, we can use "Burp" to attack the backend service with different types of attacks such as SQL injection and brute force attacks. However, we would like to do something stealthy that cannot be detected by application firewalls. Logic attacks will do it.

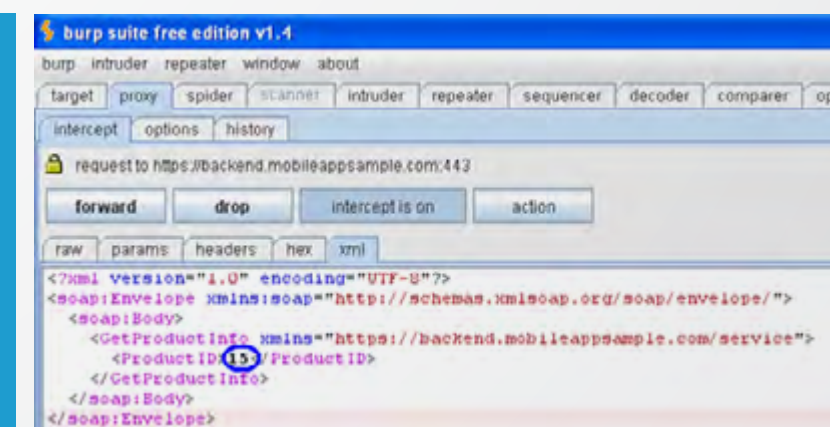


Figure 3: Burp proxy used to intercept SOAP messages

Exploiting a Logic Attack

Logic attacks are one of my favorite attacks. In such attack, we abuse the logic of the application to achieve our threat goals. It needs deep understanding of the logic of the application. One of the best papers published in this area is available on [1]. The author elaborated how to shop online for free using business logic flaws in several web applications. Our attack is inspired from this paper.

Figure 4 demonstrates how SOAP messages are sent and received through the victim mobile application in order to execute an order. It starts by sending Product info and ends by receiving the activation code for the purchased product.

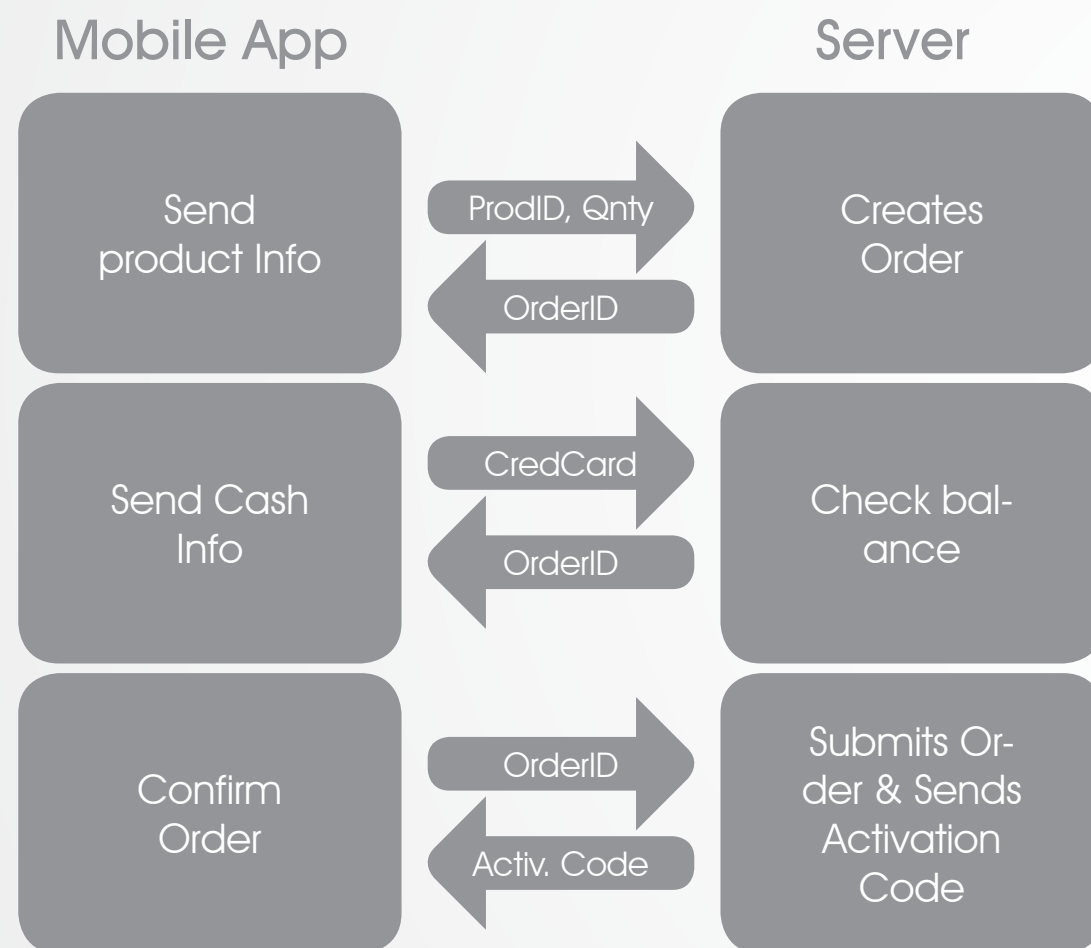


Figure 4: Normal order execution process

Now, let's try to purchase a product with lower price than its actual price. Assume that Product 1 has lower price than Product 2. Our target is to purchase Product 2 with the low price of Product 1. We will use "Burp" to send SOAP messages to the server with a sequence the server does not expect. Attack scenario will be as follows:

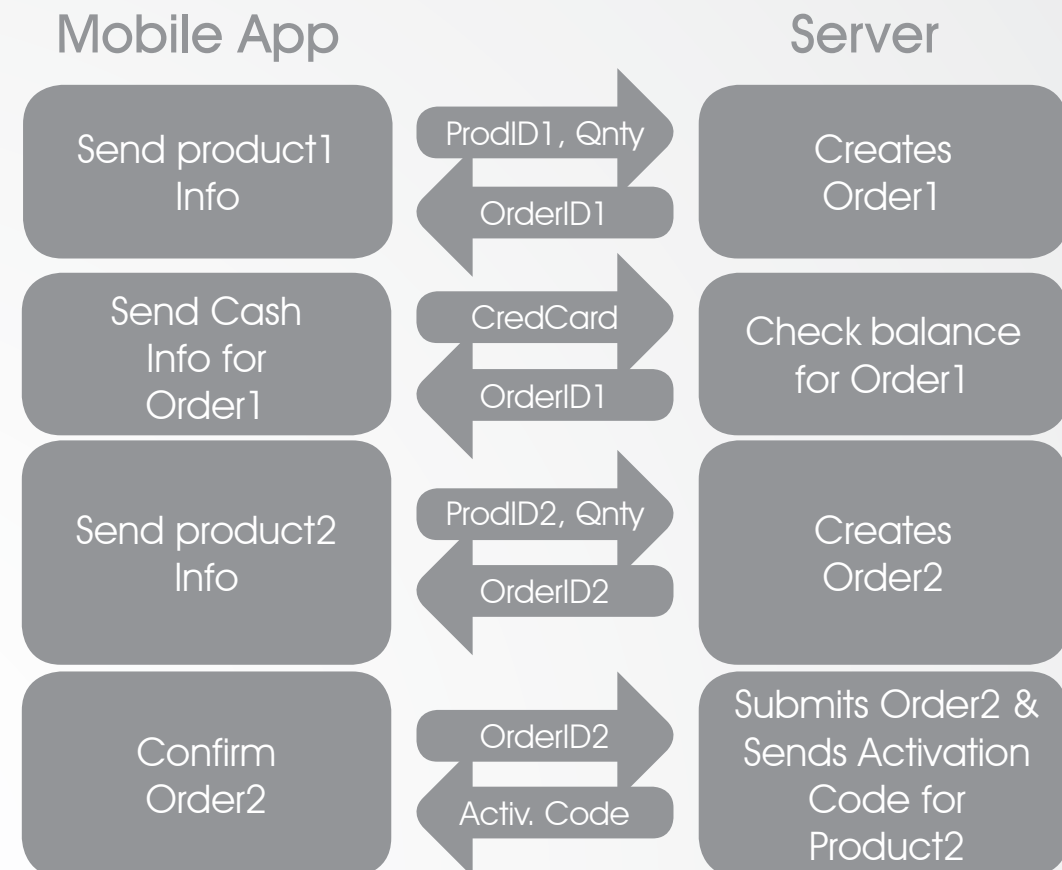


Figure 4: Attack scenario

Now, we have succeeded to get activation code for Product 2 although paid for the cheap Product 1. This is due to lack of proper validation on the server side. The server was expecting a Confirm Order SOAP message for Order 1. However, we sent it a Confirm Order SOAP message for Order 2. The server thought that we already paid and gave us activation code for Product 2.

Countermeasures:

Several countermeasures can be applied to overcome the attack discussed in the article.

- Backend service should deal with clients as if they are hackers. Traffic is not always sent from the trusted mobile app. The application should have performed robust server side authorization checks on the requests sent by our interception proxy.
- Logging security events is usually ignored by developers. If logging and alerting was on, the application administrator would have noticed that we tried to confirm on an order that has not been checked for cash balance.
- A secure connection should only be established on the mobile application after verifying the identity of the backend server. For example, if the application uses SSL and does not trust the certificate supplied by the server, it should block the connection. This would have made using the proxy more difficult.
- For further guidelines offered by OWASP, please refer to OWASP Top 10 Mobile controls [2].

References:

- [1] "How to Shop for Free Online", <http://www.informatics.indiana.edu/xw7/papers/caas-oakland-final.pdf>
- [2] "OWASP Top 10 Mobile controls", https://www.owasp.org/index.php/Projects/OWASP_Mobile_Security_Project_-_Top_Ten_Mobile_Controls
- [3] "Burp Suite", <http://portswigger.net/burp/>



Hassan El Hadary

GCIH, GWAPT I am a Senior Security Engineer at SecureMisr and a Community Instructor at SANS Institute.

Hacking Storage in iOS

Long was the time when Mobile phones were used only for making calls or sending SMS. With Smart phone and applications running on it, definition of mobile phones has been changed in last 5 years. To provide different services, companies have started writing mobile applications. These mobile applications came with ease of use for the user. Easier the application is to use, chances of having popular is more. Today, There is a mobile application for virtually everything - for banking, for shopping, to find a restaurant, to plan your travel trip, to review your business documents or last but not least social media. Only iOS platform have more than 750000

applications. To serve clients with minimal information or click, applications have started storing information on the device. As a result, One of the key check is to look for information in the iOS device while performing iOS application security review as the biggest threat is data stored in temporary files or default locations. In 9 out of 10 applications, we find some sensitive information stored in the local device. What happens if you leave your device to someone or you are connected to open Wifi at airport or you loose your device. All your information is in the attacker hand which can be stored password of your bank account or a PDF statement which you downloaded from your bank account or a credit card information which you used last night to do some shopping or your home address as you came back from your friend's home last night and you were lost. We have created a list of location where different sensitive information is usually stored. List is divided in different categories.



Hemil Shah, CISSP, CSSLP, ACP is the founder and Director of eSphere Security, a company that provides Professional services in the Security Arena

System Information

Detail	Location
Location	/var/stash/Applications
Etc	/private/etc
Var	/private/var
User	/var/mobile
Provisioning Profile	/var/mobileDevice/ProvisioningProfiles
Logs	/var/log, /var/logs /var/mobile/Library/Logs
Network Settings	/var/preferences/SystemConfiguration/com.apple.network.identification.plist
Wifi Settings	/var/preferences/SystemConfiguration/com.apple.wifi.plist /var/preferences/SystemConfiguration/preferences.plist
Apple ID, Owner information and Firmware Information	/root/Library/Lockdown/data_ark.plist
Keychain	/var/Keychains
KeyBoard Cache	/User/Library/Keyboard/dynamic-text.dat
Tmp	/private/var/tmp

Default Application Information

Address Book	/var/mobile/Library/AddressBook/AddressBook.sqlitedb /var/mobile/Library/AddressBook/AddressBookImages.sqlitedb
Last searched Google maps	/var/mobile/Library/Caches/MapTiles/MapTiles.sqlitedb
Google Map History Information	/var/mobile/Library/Maps/History.plist /var/mobile/Library/Maps/Directions.plist
Calendar	/var/mobile/Library/Calendar/Calendar.sqlitedb
Data under notes application	/var/mobile/Library/Notes/notes.sqlite
Configuration file for Applications	/var/mobile/Library/Preferences
Photos	/var/mobile/Media/DCIM/
Application Pictures when HOME button is pressed (Each application has its own directory - Default applications)	/User/Library/Caches/Snapshots

Default services Information

Call History (Odd number is for Outgoing calls, Even number is for Incoming calls)	/var/mobile/Library/Callhistory/call_history.db
SMS (Odd number is for Outgoing calls, Even number is for Incoming calls)	/var/mobile/Library/SMS/sms.db
Voicemail	/var/mobile/Library/Voicemail/voicemail.db
Voice mail recording	/var/mobile/Library/Voicemail/
System provided applications, ringtones and wallpapers	/var/stash
Call History	/var/wireless/Library/CallHistory
Call Log	/var/wireless/Library/logs
Call Preferences	/var/wireless/Library/Preferences

User Installed Application information

Installed Applications	/User/Applications
Application Directory (Binary, supporting files)	/User/Applications/<app GUID>/<appname.app>
Applications documents i.e. images, PDF, text files	/User/Applications/<app GUID>/Documents
Application cookies	/User/Applications/<app GUID>/Library/Cookies/Cookies.binarycookies
Application Preferences (plist files)	/User/Applications/<app GUID>/Library/Preferences
Application temporary storage	/User/Applications/<app GUID>/tmp
Application crash report	/User/Library/Logs/CrashReporter
Application Screens when pressed HOME button	/User/Applications/<app GUID>/Library/Caches/Snapshots

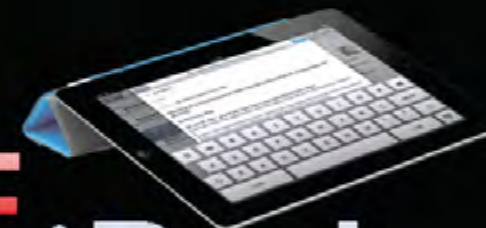
User Installed Application information

Browser Cookie	/User/Applications/<app GUID>/Library/Preferences
Browser favorites (Book marks)	/var/mobile/Library/Safari/Bookmarks.db
Browser History	/var/mobile/Library/Safari/History.plist
Browser Settings	/var/mobile/Library/Preferences/com.apple.mobilesafari.plist
Browser Cache	/User/Library/Caches/com.apple.WebAppCache/ApplicationCache.db



SecureNinja

Forging IT Security Experts



FREE The new iPad

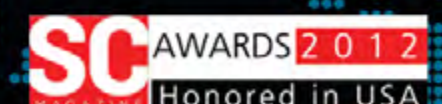
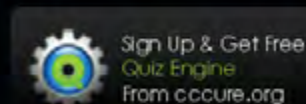
Get The new iPad with select SecureNinja Boot Camps

Offers ends on May 31, 2012 – Call 703-535-8600 and mention code: **KaizenNinja312** to secure your special rate.

* Terms and conditions apply

www.secureninja.com

Expert IT Security Training & Services



London | Istanbul | Dubai | Washington, DC | Singapore | San Diego | Tokyo | Bucharest

© 2003-2012 Secure Ninja. All rights reserved.

Wireless Security Awareness

By Mohamed Bedewi
CEO of Dark-Hack Network

Wireless security is actually a weak sauce and despite the fact of how Wi-Fi evolved in the past few years, it still considered a new technology which we know only a little about.

Important facts for you to consider

1) WEP Encryption is very easy to crack and it only takes a few minutes to bypass, in my personal Opinion if I will had to use this one I will use it as a **Honey-Pot !**

2) MAC Address Filtering is a good idea but it will only tackle the attacker for a few minutes before he spoofs your MAC address, inject you out of the network and simply be you.

3) Disabling SSID Broadcasting seems smart but it's actually not because it can give you a big headache when configuring your network and causes an increase in network traffic.

4) MITM Attacks are easily achievable in the above scenario and before you know you'll find the attacker emulated the access point and sniffed every host on your network.

Tackle The Attacker Procedures:

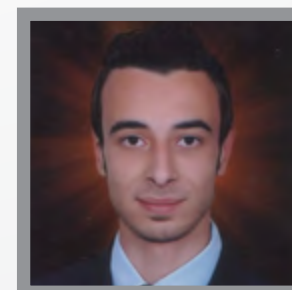
- 1)** Use a Wi-Fi honey-pot to tackle the attacker till you collect some useful information about him/her and his/her attacking techniques to report or punish him/her.
- 2)** Consider WPA2 Enterprise encryption with a complex password chars "Numbers, Letters and Special Characters" and this way you'll make it harder on the attacker.
- 3)** MAC Address filtering can be used to make it a little hard on the attacker but not too much actually and you already know the reason.
- 4)** Depending on your network size make sure to monitor your network activity using any professional software and if you noticed any unusual activity get a packet analyzer software.

Wi-Fi is the next communication evolution with no doubt but till now we didn't find any workarounds for its security design flaws, it's too new and needs more time to evolve even more that's why starting from now you should put an extra eye on your wireless access points.

Some Definitions Explained:

We're working hard to make our articles friendly for both experts and beginners that's why the following approach is only for beginners:

- 1) WEP Encryption:** short for Wired Equivalent Privacy and was designed to provide the same level of security as that of a wired LAN but it simply failed.
- 2) Honey-Pot:** Fake vulnerable system deployed by network administrator to attract attackers and analyze their attacking mechanisms to achieve better security for the real system.
- 3) MAC Address Filtering:** allows network administrator to permit specific devices to connect to the network while denying all other devices, this filtration is based on devices MAC Address.
- 4) SSID:** short for Service Set Identifier and is a token that identifies a 802.11 Wi-Fi network which without no-one will be able to connect to the network.
- 5) MITM:** short for Man in the Middle and it happens when an attacker inserts himself between two Communicating parties, both believe they're talking to each other when they're not.
- 6) WPA2 Enterprise:** short for Wi-Fi Protected Access 2 and it provides government grade security by implementing the (NIST) AES encryption algorithm and 802.1 x-based authentications.



Mohamed Bedewi
Owner of Dark-Hack Network

A holistic approach to PCI-DSS Compliance

New & News 2012



In recent years we've witnessed the extraordinary lengths to which cyber criminals will go to breach target networks and steal valuable data for monetary or competitive gain. This phenomenon is particularly apparent in the world of electronic commerce, where account details of credit card users are sold for a premium on the black market.

Fortunately, the principal stakeholders in the card payment ecosystem have defined a standard that has proven to be highly effective (albeit not infallible) at protecting data from such breaches. Over the past five years, the PCI-DSS framework has evolved from being mere guidelines without enforceable sanctions to a 'must-have' certification that you are required to obtain if you are involved in manipulating, storing or transmitting cardholder data.

Despite its seemingly narrow focus on cardholder data protection, PCI-DSS spans most IT disciplines and skills. This includes networks, databases, web

applications, file systems and encryption along with core security-related processes such as vulnerability and configuration management. As a result, the cost of implementing compliance has become alarmingly high, bringing into question the applicability of the standard in terms of risks versus reward.

Earlier this year, the Ponemon Institute conducted a study on the actual costs of compliance among 160 enterprises, including 46 international ones. The results of this study showed that for mid-size organizations, the total cost of compliance with regulations such as PCI-DSS, SoX, HIPAA and others, averages \$3.5 million. However, the cost of non-compliance was measured at \$9.4 million, nearly triple the cost of compliance. While these figures illustrate a sizeable benefit for investment in compliance, the cost burden remains high. So, what strategies can be employed to reduce the complexities and costs of a PCI implementation? What are the

principal concerns to consider in terms of PCI implementation?

PCI-DSS is multi-disciplinary and to fully comply with the standard, it is essential to take a global consolidated approach to address all 12 requirements as a whole before focusing on solving individual elements. The core IT disciplines to be considered are: Networking – Fixed and Wireless; Data and Databases; IT Assets/ End-Points; and Web Applications.

Fixed Network

The PCI core requirement covers controlled network segregation, inbound/outbound traffic flows and DMZ implementation. Specific functions include: real-time perimeter anti-virus, IPSec/VPN tunneling support, IDS/IPS, use of strong cryptography (SSL/IPSec), default 'deny-all' settings, support of digital certificates and two-factor user authentication, event monitoring, federated device management and reporting, and network vulnerability analysis support. These services cannot be provided by a legacy firewall, even a so-called next-generation firewall. The only way to cost effectively provide all these services and avoid the deployment of multiple devices is through the use of a Unified Threat Management (UTM) device. A UTM-based solution can help organizations cover the fixed network requirements of PCI while achieving greater overall PCI effectiveness and simultaneously minimize implementation and operational costs.

Wireless Network

In many ways, the wireless network is subject to the same constraints as the fixed network but it must also meet the following key functions:

- 1) Support for both 'thick' and 'thin' access point (AP) solutions that can work in a seamless management framework
- 2) Detection of rogue APs against a defined hardware inventory
- 3) Support and logging of wireless IDS/IPS
- 4) Support for WPA or WPA2 Enterprise

mode with 802.1X authentication and AES encryption. In practice, the best approach in larger deployments is to minimize the deployment of thick APs, which have wireless control, IPS and other security features built into the physical devices, and favor the deployment of thin access points, which are much easier to manage and maintain. Thin APs tunnel wireless traffic to wireless controllers, allowing significant economies of scale and a simplified security management capability through a 'single pane of glass' management console for increased visibility and policy enforcement.

IT Assets / Endpoints

IT assets include servers, desktops, laptops, operating systems, mobile devices and network equipment. The objective is to ensure that all assets that constitute the PCI cardholder data environment are subject to core security management processes. Here, in order to have the most effective approach in meeting the PCI DSS requirements at minimal cost and complexity, it is important to consider the management of deployed endpoint security technologies and controls. The top 5 elements on the checklist are:

- 1) Support for asset vulnerability management to ensure that all operating systems are patched to the latest version and to assess configuration specific vulnerabilities
- 2) Configuration management capability against globally accepted best practices for operating system platform deployment (e.g. NIST, FDCC)
- 3) Endpoint policy control to blacklist/whitelist software, processes, devices, drivers, access lists etc....
- 4) Automated remediation of configuration and audit issues for cost-effective operation
- 5) Deployment of client/mobile device anti-virus, preferably administered centrally

Data & Databases

It is impossible to comply with PCI DSS without implementing a database security solution to protect against data loss or fraud. Whether due to an error or a deliberate intent to harm, data loss can have serious consequences. In order to meet PCI-DSS compliance, a database security solution must include:

- 1) Database-specific vulnerability assessment and penetration testing
- 2) Configuration management for assessment against global best practices and/or the organization's own data security standards
- 3) Access control assessment both at the database and application levels
- 4) Real-time monitoring of database users and their activity on both database and critical cardholder data.

In order to simplify the creation and enforcement of data security policies that will help meet PCI-DSS compliance, it is important to look for a centrally-managed database security solution that provides all of the above features on one device.

Enhanced solutions include features such as automatic database and sensitive data discovery. Other desirable functions include pre-built policies that cover standard industry and government requirements which when combined with a comprehensive set of graphical reports deliver out-of-the-box readiness and immediate value for PCI-DSS compliance.

Web Applications

Since web applications are exposed to the outside world by definition, the PCI-DSS standard addresses them in detail in requirement 6.6. There are two methods that a company can apply in order to be in compliance with PCI DSS: a) Conduct yearly code reviews or b) Deploy a Web application firewall. While code reviews/testing is important, a significant cost saving can be made through the

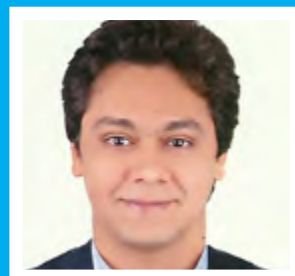
implementation of a Web application firewall.

The key functions that should be included in such a solution include:

- 1) Support of OWASP Web security guidance, cross-site scripting (XSS) and cross-site request forgery (CSRF) vulnerability protection
- 2) Support for DoS and buffer overflow attacks at both the HTML and HTTP level
- 3) Access control and web application user authentication
- 4) Monitoring and management of error events
- 5) Incorporation of a web application vulnerability scanning capability for regular internal scans.

Conclusion

The multi-disciplinary nature of PCI-DSS requires the deployment of a variety of different security technologies. Consequently, organizations often deploy a combination of security technologies from different vendors in order to fully address the requirements of the standard. Unfortunately, using a large number of solutions from a variety of vendors often results in a wide array of disparate products and services introduced into the PCI solution. The result is spiraling complexity (in terms of support, maintenance, resource training, etc.) and increased total cost of ownership. Minimizing the number of vendors to work with, to a single one if possible, is the only way to dramatically reduce both operating and capital expenses while removing complexity from implementation and management. A common platform provided by a single vendor will also enable you to enhance your security posture, coverage and visibility for a lower overall risk of PCI project failure. In summary, a consolidated approach allows you to increase performance, improve security and reduce cost



Hatem Ali

Country
Manager, Egypt, Libya
and East Africa at
Fortinet



Every day, Fortinet protects the networks of many of the largest and most successful organizations in the world.

We deliver complete content protection to block hidden threats.

Our consolidated network security technologies combine application control with identity-based policy enforcement.

Learn how you can increase security, improve performance and lower costs.

Visit us at www.fortinet.com to find out how you can protect your network today.



Healthcare
Government & Defense
Education
MULTI-THREAT SECURITY
Service Providers
Financial Services
Retail
Utilities

Security Kaizen Labs 2012

Registration Now Open

Date : 9,10 May 2012
Place: EBI, Egyptian Banking institute Nasr City, Behind Tiba Mall



It's time
 To learn how hackers do it
<http://www.bluekaizen.org/sklabs.html>



Security Kaizen Labs 2012

SKLab 2012 Agenda, Cairo, Egypt
<http://www.bluekaizen.org/sklabs.html>

Room 1 - Beginners
Room 2 - Professional
Room 3 - Vendors

Day 1 - Wednesday - 9 May, 2012

10:00 am - 11:00 am	Opening Session		
11:00 pm - 11:30 pm	Coffee Break		
R o o m s	Beginners	Professional	Vendors
11:30 pm - 1:00 pm	Introduction to Application Security	Use Honeypots to Know Your Enemies	Managing vulnerabilities in the enterprises
C o m p a n y	SANS EGYPT	Egyptian CERT	metasploit®
1:00 pm - 1:30 pm	Break		
1:30 pm - 3:00 pm	Hacking Wireless Networks	SQL Server 2012 (DENALI) Security & Compliance	Managing the unmanageable devices in network
C o m p a n y	nen	FBI	NETCLARITY
3:00 pm - 4:00 pm	Lunch Break		
4:00 pm - 6:00 pm	Web Hacking & Security workshop	Defending your application against cross-site scripting & SQL Injection	Cisco Identity Service Engine ISE
C o m p a n y	COMPUtek	eVision	CISCO

Day 2 - Thursday - 10 May, 2012

R o o m s	Beginners	Professional	Vendors
10:00 am - 12:00 pm	Digital Forensics Investigation	Malicious PDF file analysis	Web Application Firewall (FortiWEB)
C o m p a n y	RAM Academy	Egyptian CERT	FORTINET
12:00 pm - 1:00 pm	Coffee Break		
1:00 pm - 2:30 pm	Session 2	Exploiting and Defending Advanced Application Attacks	EnCase® Forensic
C o m p a n y	COMING SOON	SANS EGYPT	Guidance SOFTWARE
2:30 pm - 3:30 pm	Lunch Break		
3:30 pm - 5:00 pm	Introduction to Open Source Intelligence	A study of an Antivirus Engine	Mcafee Endpoint Encryption
C o m p a n y	Egyptian CERT	Synapse	McAfee SECURE
5:00 pm - 6:00 pm	Closing session		

facebook® Security

At Facebook Security, we are constantly iterating on our systems and working on innovative ways for you to keep your account secure. Starting this month, people who access Facebook using the Android application will be able to take advantage of our new native Code Generator.

Code Generator is our latest addition to our Login Approvals feature, aimed at making it easier to confirm logins made on new devices. Before, if you had any difficulties receiving SMS or had poor cellular service, it was often tough to use Login Approvals easily. Now, using Code Generator, users will be able to receive Login Approval codes through your Facebook Application, without waiting on an SMS, and it will work regardless of whether you have cellular or Internet access.

If you have an Android device, go to <http://on.fb.me/LoginApprovals> and follow the instructions there to set up Code Generator. Once you have finished, you can simply navigate to Code Generator within the Facebook for Android app to receive the security code needed to complete a login from a new device. For your security, this code will refresh every 30 seconds.

We are working hard to expand this functionality to other devices, and you can still use Login Approvals via SMS even if you don't have an Android device. You can learn more about Login Approvals here - <https://www.facebook.com/help/?faq=148233965247823#What-is-Login-Approvals?>

Special thanks to Jake Brill and Mergen Nachin on their contributions to this project.

Note: If you are having difficulties finding the Code Generator app on your device follow these steps: 1. Open the Facebook for Android App 2. Tap [insert menu icon] 3. Find the Apps section 4. Click Code Generator

Joe Sullivan

I am the chief security officer of facebook.com, i manage a few of the teams at facebook focused on making sure that people who use facebook have a safe and positive experience



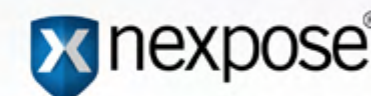
Fixed Solutions



Ask experts!



DSphinx



www.fixed-solutions.com



@fixedsolutions












fb.me/fixedsolutions














Cyber WAR










Today it becomes clearly obvious that the nextwar won't be a war of guns and bullets, but a war of malwares, viruses, Trojans and more. That was so clear in the famous stuxnet case in Iran and it will be clearer after reading this article.

Our friend from Italy Paolo Passeri, owner of hackmageddon.com made an amazing research on Cyber War that started to rise in the Middle East since the beginning of this year. It all started when the Saudi hacker 0xOmar published thousands of credit card owned by Israeli citizens. After that, the Israeli deputy foreign minister Danny Alton announced that the hacker 0xOmar doesn't own all this number of credit cards and this kind of terrorists must be treated firmly.

That made 0xOmar published more credit cards and more Israeli hackers replied to him with more attacks on different Saudi websites and then it became a real war, Israel from one side and different Arab countries from the other side. Paolo collected all this data from different sources on the internet, gathered it in one timeline and presented it to us to be published in Security Kaizen Magazine fifth issue. Paolo did a great work and his efforts were remarkable.

Date	Attacker	Target	Description
Everything starts here...			
Jan 2	0xOmar		Everything begins here. 0xOmar, a Saudi hacker from a crew called Group-xp claims to have stolen information of 400,000 Israeli Credit Cards, after hacking several websites. Leaked information include name, address, city, zip code, Social Security Numbers, mobile phone number, home phone number, credit card number (including exp year, month and CVV). Three Israeli banks, Isracard, Leumi Card and Visa CAL, acknowledge that they had been affected by the attack and blocked the compromised cards but refute 0xOmar's figure of 400,000 compromised cards, stating a figure far closer to 15,000. ¹
Jan 5	0xOmar		In a new post on pastebin, 0xOmar denies he only owns 15,000 credit cards and shares the information of other 11,000 credit cards, claiming he owns 60,000 more after hacking 80 servers. ²
Jan 6	Amir Phadida	0xOmar	Amir Phadida, an Israeli student claims to have been able to track the real identity of the Saudi Hacker '0xOmar', after an intense eight-hour search. According to him, '0xOmar' is in real life a 19-year-old computer science student from Mexico named Omar Habib. ³
Jan 6	0xOmar		The same day, on a new pastebin post, 0xOmar marks the revelations as a failure and challenges the whole world to find him in two weeks. ⁴
A quick escalation...			
Jan 7		0xOmar	Israeli Deputy Foreign Minister Danny Ayalon declares that breaches of Israel's cyberspace are a breach of sovereignty similar to terrorism and should be treated as such. ⁵
Jan 7			Hamas spokesman Sami Abu Zuhri hails the anonymous Arab hackers who managed to penetrate credit cards of Israelis and expose their details as a creative work and a new means of resistance against the occupation. ⁶
Jan 8			Another front of war: As part of the so called #OpFreePalestine, @AnonymousSTL attacks some Israeli domains and leaks some information. Victims include: topilinks.co.il, Bar-Ilan University Geography and Environment Department (home.geoenvironment.ac.il), Israel Institute of Technology Cancer and Vascular Biology Research Center (technioncancer.co.il), NBN (Nefesh B'Nefesh, nbn.org.il), ILAN (ilan-israel.co.il), SNIP (snip.co.il). ⁸
Jan 9	?		A hacker temporarily takes over the website of Israel's deputy foreign minister, Danny Ayalon (http://www.dannyayalon.com) ⁸ after his declarations of the 7 th of June. ⁹
Jan 10	0xOmar		An Israeli hacker called 0xOmar (a clear reference to the Saudi Hacker) publishes details of 200 Saudi credit cards online and threatens to post more in revenge for acts by Arab hackers. ¹⁰ He declares to own more 300,000 credit cards. ¹¹
Jan 11			An hacker called @FuryOfAnon publishes a list of IPs which allegedly belong to some Israeli organizations that utilize SCADA systems and even revealed that they could be accessed using the "100" default password for Siemens systems. ¹²
Jan 12	0xOmar		As a further retaliation for the Israeli Hacker 0xOmar claiming to publish Saudi Credit Cards, 0xOmar publishes 200 credit cards and threatens to publish 200 more every day... ¹³ Moreover in his pastebin messages he invites the hackers of all the world to unite against Israel. ¹⁴
Jan 12	0xOmar Pro3ct10n		The reaction is nearly immediate: 0xOmar and Pro3ct10n publish details of more than 1,000 Saudi individuals and threatens to post next week, details of 5,000 Credit Cards (they claim to own 5,000,000). ¹⁵
Jan 13			The Israeli Defense Ministry establishes a special cyber warfare administration that will coordinate the efforts of security agencies and the Israeli defense industry in developing advanced systems to deal with cyber warfare. ¹⁶
Hannibal enters the Scene			
Jan 13	Hannibal Lecter		An Israeli Hacker who calls himself Hannibal Lecter, and defines himself "a Jew who lived somewhere in the world" claims to own 30,000,000 emails belonging to Arabs and starts to post them on pastebin (1,500 everyday for 55 years!). ¹⁷
Jan 15	Hannibal Lecter		As promised, Hannibal Lecter keeps on dumping 1,500 emails per day until Jan 15 when he also dumps 20,000 Facebook accounts belonging to Arab people. He also claims to own "10 million bank accounts of Arabs from Iran And Saudi". The leak contains emails and cleartext passwords. ¹⁸

Now is the time for DDoS!			
Jan 15		Several Web Sites	In support for #OpFreePalestine, DevizSec hacks and defaces several websites all over the world. ¹⁹
Jan 16	0xOmar Nightmare		0xOmar and Nightmare attack the Tel-Aviv Stock Exchange (tase.co.il) and the Israel Airline (elal.co.il) websites, taking them down with a DDoS attack. ²⁰
Jan 16	0xOmar Nightmare		0xOmar and Nightmare keep on their DDoS attack against Israel's banks, which temporarily block overseas access to their websites over the cyber-attack. Banking system official declares that situation calls for drastic measures and First International Bank of Israel (FIBI) and Israel's Discount Bank are the first to apply the limitation as a precautionary measure. ²¹
Jan 17	IDF-Team		In retaliation for the last attack, a team of Israeli hackers, called IDF-TEAM (maybe Acronym for Israel Defense Force) attacks and brings down Saudi (tadawul.com.sa), UAE stock exchange (adx.ae) websites. ²² In any case Saudi sources deny infiltrations. ²³
There is no (cyber)war without (cyber)propaganda			
Jan 17			Hamas spokesman Sami Abu Zuhri describes the recent cyber attacks on Israeli websites as a new form of resistance against Israeli occupation. "This is a new field of resistance against the occupation and we urge Arab youth to develop their methods in electronic warfare in the face of [Israel's] crimes." ²⁴
Jan 17	ZionOps	0xOmar	A group of hackers going by the name ZionOps claims they have hacked 0xOmar's forum. ²⁵
Other forces enter the war, other innocents cyber-victims			
Jan 17			Unfortunately it looks like the Cyber War between Hannibal and 0xOmar is becoming the excuse for questionable actions targeting unrelated sites. In support (?) of Israel, AlienZ hacks powersoccer.ca and dumps 13,994 accounts. ²⁶
Jan 17	Prx3R0 L3ht	Arab Credit Cards	A couple of Israel Hackers dubbed Prx3R0 and L3ht threatens Arab hackers with a message on pastebin and as a demonstration publish some Arab Credit Card information on pastebin. ²⁷
Jan 17	Ano972		Anonymous 972 warns 0xOmar that every action against Israel will have a consequence, and as a demonstration dump personal information of 100 Saudi individuals. ²⁸
Jan 17	Hannibal Lecter		Hannibal posts what he states is the log-in information of over 10,000 email and Facebook accounts of Arabs and Muslims all around the world. ²⁹
Jan 18			Top Persian Gulf Kuwaiti imam Tareq Mohammed Al-Suaidan calls for Hacker Jihad and endorses 'cyber Jihad against Zionist enemy' with a tweet from his account followed by more than 240,000 followers. ³⁰
Jan 18	Nuclear Group		A new hacking group appears inside the Cyberwar between Pro-Israeli and Pro-Palestinian Hackers. Nuclear Group claims to have been able to hack into one of the biggest banks in Saudi Arabia, and publishes 4,800 Arabs Credit Cards. ³¹
Jan 18	Hannibal Lecter		In a two separate posts on pastebin, Hannibal Lecter shows an alleged threatening e-mail sent to him by Deputy PM of Iran Mohammad Reza Rahimi ³² and also claims to have disclosed the identity of 0xOmar. ³³
Other Attacks in support of Palestine and against Israel			
Jan 18	C'Seven Booter		In support of #OpFreePalestine C'Seven Booter hacks several Indian (??) websites and dumps the leaked admin information on pastebin. Targets of the attack include www.kgsbank.co.in, www.indiatvnews.com, www.sail.co.in, www.tfkolkata.bsnl.co.in, punjab.bsnl.co.in. ³⁴
Jan 19	Pak Cyber Combat Squad (PCCS)	Several Web Sites	PCSS joins #OpFreePalestine and starts a massive defacement campaign against several web sites leaving a message for the end of occupation by Israel. ³⁵
Cyber War or Cyber Guerrilla			
Jan 19	Gaza-Hacker		Israel Anti-Drug Authority (IADA) is victim of an SQL Injection hatack and is defaced by Gaza-Hacker. ³⁶
Jan 19			AlienZ attacks the Union of Arab Banks (uabonline.org) and dumps on pastebin (threatening Arab Hackers) nearly 500 Arab accounts with usernames and cleartext passwords. ³⁷
Jan 19	HAX ROOT CTR Robot Pirate Pakos Hacker	The Hackers Army	The official website of THA (The Hackers Army), one of the groups most active for #OpFreePalestine, gets hacked by HAX ROOT, CTR Robot Pirate and Pakos Hacker in support for the Israel Cause. ³⁸

Jan 19	FCA		The wave of attacks against Israel related institutions lands on France. A group going by the name FCA attacks, hacks and dumps 13,000 Accounts from CRIF, Council of Jewish Institutions of France. ³⁹
Jan 20			AlienZ hacks and destroys the database of Lebanonli.com, a directory service for finding Lebanese, Arab, Arab-American business. ⁴⁰
Jan 20	Ano972	codecity.ir	Anonymous 972 attacks an Iran based site for developers and dumps some accounts. This is done in retaliation for the fact that 0xOmar is an Iranian Hacker. ⁴¹
More forces enter the scene			
Jan 20	White Bishop		An Israeli hacker who goes by the name "WhiteBishop" dumps 2000 Saudi Credit Cards a retaliation to 0xOmar breach. ⁴²
Jan 20	Watchful Eye Hacker		An Israeli religious news site (hayessnet.com) is defaced by a new entry hacker named "Watchful Eye Hacker". ⁴³
Jan 20	TheJ0k3r5		An Israeli hacking group that goes by the name "TheJ0k3r5" claims to have full control on several Iranian websites, one of them is "Iran.tv", and they will escalate if the so called "war" don't stop. They also release a video to prove the hack. ⁴⁴
Continued actions...			
Jan 20			AlienZ hacks a Palestine information website (thisweekinpalestine.com) and leaves a message against Palestine, stating "We are AlienZ. We are Israel's cyber army". The group also dumps on pastebin all the leaked accounts (approximately 4000). ⁴⁵
Jan 21			In light of the latest attacks, Bank of Palestine (bankofpalestine.com) decides to disable its online banking services. ⁴⁶
Jan 21	Hannibal Lecter		Hannibal Lecter dumps a new list of 100,000 emails and facebook accounts of Arabs. ⁴⁷
End of War? Maybe Not!			
Jan 21	Hannibal Lecter		In a new pastebin post Hannibal declares that "Jewish people named him as the general of Israel's hackers". He also states that he received thousands of emails from Arabs who are begging him to stop publishing their bills and hurt them. Since he noticed that the Arab hackers are gone, he declares cyber war termination... Until further notice. ⁴⁸
Jan 21			... And in fact the AlienZ are back and claim to have a lot of information to publish (about 10,000 Iranian credit cards and "countless" emails of Arabs. They start with publishing all the accounts (nearly 200) for e-teacherdiplooma.com. ⁴⁹
And now? A bunch of defacements			
Jan 21	IGT	smiles.co.il	Israeli website smiles.co.il is hacked and defaced by IGT (Islamic Ghosts Team). ⁵⁰
Jan 21	Capo0_TunisiAno0		Israeli insurance website revivo.co.il is hacked by an Hacker called Capo0_TunisiAno0 and defaced. ⁵¹
Jan 22	Dr.Net	Ofra Haza Memorial Web Site	The Cyber War does not spare not even Memorial sites. In this circumstance the target is the site in the memory of singer Ofra Haza (haza.co.il) which is defaced. ⁵²
Jan 22	TheJ0k3r5	Ofra Haza Memorial Web Site	The same web site is immediately defaced again by TheJ0k3r5 with a message that intimates Saudi Hackers to go back. ⁵³
Jan 22	Khalid Islambouli		A sub-domain named "presidentconf" under "Haaretz" main website is hacked by a hacker called Khalid Islambouli. ⁵⁴
Jan 22	TheJ0k3r5		Security & Defense Arabia "SDA" - Sdarabia.com is hacked and defaced by TheJ0k3r5. ⁵⁵
Jan 23	You-r-k@n		The Official Website of King Saud University (KSU) a public university located in Riyadh, Saudi Arabia, is hacked by "Younikan". The leak contains 812 User Accounts in terms of usernames and other personal data such as phones. All passwords are not encrypted. ⁵⁶

Date	Attacker	Target	Description
Again Cyber Guerrilla Actions...			
Jan 22	TKL	npsoft.co.il	TKL, part of Gaza Hacker Team, hacks and defaces npsoft.co.il, a small Israeli development company and leaves a message against Israel. ¹
Jan 22	OxOmar		OxOmar leaves a message against Israel, warning "I will finish Israel Electronically". He also adds "I am one of the stronger haters of Israel. The end of Israel is very close." He also adds he live in Riyadh although this information is controversial. ²
Jan 22	OxOmar	PIRELLI	Pirelli Tires Israel (pirelli.co.il) gets hacked and defaced by a Turkish hacker called HEXBOOT3R (although it appears only a domain registered to the Tires company and not a corporate site). ³
Jan 23	Hitcher	AMITEC	Inside OpFreePalestine, a Pakistani Hacker called Hitcher hacks and defaces Amitec, one of the top most IT innovative Israeli companies. He hacks both the Israeli and English domain. ⁴
More Manifestos...			
Jan 22	ET from	ALIBING	ET from the AlienZ group sends a message to the world to better understand the attacks they are carrying on. They also invite any pro-Israeli hackers to join them. "We want to make a small group of hackers who will work together and help each other to fight Arabs." ⁵
... And More Huge Dumps...			
Jan 22	OxOmer	DATE	OxOmer dumps more than 2000 Saudi's people details (emails plus passwords plus other details) allegedly taken from a Dating Website. He also promises to continue if Saudi Hackers will continue with Cyber War. ⁶ In a subsequent message OxOmer claims he has more Credit Cards and Secret Documents to deliver to IDF or publish. ⁷
Jan 23	Virus Kiss	ISRAEL	A new entry inside the Middle East Cyber War: A hacker called Virus Kiss dumps 185 email accounts belonging to Israeli individuals. ⁸
Countermeasures...			
Jan 23		ISRAEL	In response to the rising Cyber War in Middle East, the Palestinian Authority considers to form a national team specialized in Cyber Security. ⁹
Un unprecedented wave of attacks against Israel			
Jan 24	?	ASSUTA	Is it time for a Cyber Geneva Convention? Maybe since not even Hospitals are safe from the Cyber War. The Assuta Hospital (assuta.co.il) announces its site to be inoperative due to a hacker attack, keeping the site down until the end of the attack. ¹⁰
Jan 24	?	S	Nearly in contemporary another Israeli medical institution is attacked: Sheba Medical Center, Israel's largest hospital, which is taken down by a massive DDoS attack. ¹¹
Jun 25	Watchful Eye Hacker	ISRAEL	In a simultaneous wave of attacks allegedly carried on by Pro Palestinian hackers, several Israeli web sites are defaced with a message Pro-Palestine or taken down. They include: ¹² <ul style="list-style-type: none"> El Al Airlines (this is the second attack to elal.co.il); Dan Bus Company (dan.co.il); Israel Festival (israel-festival.org.il); Israel's CinemaTek Haaretz Hebrew Newspaper (haaretz.co.il).
			Anonymous Palestine (@AnonPS) claims responsibility for the Haaretz takedown;
Retaliation is not late...			
Jan 25		ISRAEL	Israeli National Cyber Command holds its first cyber terror drill called 'Lights Out' to simulate multisource cyber attack on vital Israeli systems. ¹³
Jan 25	Hannibal Lecter	ISRAEL	Hannibal is back and releases a series of Iranian documents, claiming they are just a fraction of the "confidential" data in his possession. The files include a memo on soldier training, the entire Iranian constitution, statistical data and other documents of this nature among which the alleged password of an Iranian Bank. ¹⁴
Jan 25	OxOmer	ISRAEL	In contemporary OxOmer claims to own more 5,000 secret Iran documents. He also invites other "Zionist hackers" to search for more secret documents with the final target to deliver them to the Israeli Government. ¹⁵
Jan 25		ISRAEL	AlienZ dump approximately 16,000 accounts from the following websites and leave a message for Israeli and Jewish hackers to join the cause: ¹⁶ <ul style="list-style-type: none"> http://economistpakistan.com http://edutecher.net http://phdeb.org
...that generate more victims...			
Jan 25	OxOmar	ISRAEL	OxOmar is back and dumps more than 170,000 Israeli web masters' accounts from Area.co.il, a web hosting service. The leak includes: full name, email address, phone, city, login, password. ¹⁷
...and awake old acquaintances...			
Jan 26	IDF	ISRAEL	In retaliation for the attacks to Israeli Web Sites, IDF, Israel Defense Force attacks and takes down the Iranian Ministry of Health and Medical Education and the Iran's television network. In addition three additional Iranian sites (sarallahco.ir, shiadesign.ir, syakh.ir) are hacked displaying an Israeli flag and anti-Arab text in English. ¹⁸
Jan 26	you-r1-k@n	ISRAEL	Also you-r1-k@n is back, and hacks another Saudi website with a direct message to OxOmar. The target of this attack is the "Presidency of Meteorology & Environment Protection" (cmms.pme.gov.sa) that is defaced. ¹⁹
Jan 27	Nuclear Group	ISRAEL	In response to the attacks against Israel, the Nuclear Group is back and dumps 4,000 credit cards ²⁰ allegedly belonging to Iranian citizens. ²¹

Date	Attacker	Target	Description
... and new types of cyber-attacks			
Jan 26	OxOmar	Hannibal Lecter	The pastes of the Israel Hacker Hannibal suddenly disappear from pastebin and are replaced by a single paste by OxOmar, dubbed "Hacked By OxOmar" in which he mocks the rival hacker. ²²
Jan 25-26	SanTi12	ISRAEL	A Pro Israel Hacker called SanTi12 dumps 670 Arab Facebook accounts on pastebin. He also publishes a list of several hacked Arab Web Sites from Saudi Arabia and Iran whose administrative accounts are dumped. ²³
Jan 27		facebook	An exception to the Cyber War: Anonymous Palestine apologizes for the Haaretz takedown on June 25. ²⁴
Jan 28	Israel Cyber Army	ISRAEL	Israel Cyber Army hacks (once again) thisweekinpalestine.com and the accounts of 100 senior reporters. ²⁵
Jan 29	?		Although not directly related to the Cyber War between Israel and Saudi Hackers, this episode shows that the cyber world follow the same rules than real world. In this specific case it may happen that one of the opponents (Palestine) has internal divisions: InlightPress (inlightpress.com), a press agency particularly critical against Palestinian Authority President Mahmoud Abbas is taken down by unknown hackers. ¹ In a later press release the agency accuses directly the Palestinian Authority with the approval of President Abbas. ² At the time of writing the website is currently down for maintenance after a hacking attack.
Back To The Future			
Jan 29	#Hackerdz	ISRAEL	A claimed Muslim Hacker calling himself Hackerdz hacks the Bahrain Duty Free and leaks the database on pastebin containing 12,000 Credit Cards full details. In the same pastebin he discloses his alleged real identity, according to which he should be supposed to be Mohamed Tablit and comes from Algeria. ³
Jan 30	Milto & Nati HackerHaHa	ISRAEL	A couple of Israeli Hackers called Milto and Nati hack an Arab Website (palestineews.xomcom.com) and claim to publish 5227 Facebook accounts. ⁴
Jan 31	?	ISRAEL	DDoS attacks shut down the websites of the two main Palestinian news agencies, the official Wafa (wafa.ps) and the privately run Maan (maannews.net). According to Wafa's chief editor, Ali Hussein, the website of Palestinian President Mahmoud Abbas' Fatah movement was also targeted. ⁵
New Actors Entering the Scene			
Feb 2		ISRAEL	The well known hacking collective @_TeamP0isoN enters the Digital Intifada and, in the name of #OpFreePalestine leaks 26,000 Israeli Credit Cards. ⁶
Sometime They Come Back			
Feb 2		ISRAEL	AlienZ are back and hacks several (heterogeneous i.e. arab and non arab) websites: Al Masraf Bank (arbf.com), businesscenter.pk, Pakistan Science Foundation (psf.gov.pk), National Foundation For Resource Development (nfd.org.pk), The Laureate Business School (thelaureate.edu.pk) and depo.org. ⁷
Feb 4	You-r1-k@n	ISRAEL	You-r1-k@n defaces palestinehotels.ps and leaves a message against the attacks to Israel. ⁸
Date	Attacker	Target	Description
Mutual Defacements and DDoS			
Feb 5	Moroccan Defacer	ISRAEL	Moroccan Defacer takes down the internet site of the Ya'akov Herzog College in the Gush Etzion bloc of Jewish communities, south of Jerusalem. They also a message in which they state that the break-in has been made by the Moroccan central bank. ¹
Feb 6	you-r1-k@n	ISRAEL	Irannewsdaily.com reported that "The news website of state radio and television, www.irib.ir, has been penetrated by unknown hackers". The hacker had previously targeted a website gathering signatures in favor of the presidency of Mohammad Khatami. ² Looks like the defacement dates back to Jan 15 2012 but only a cached copy is available at the moment. ³
Feb 6	CapoO TunisiaoO	ISRAEL	A massive wave of defacements by CapoO TunisiaoO against Israeli Websites. In each defaced page the Hacker leave a message against Israel for Palestine (Phaestine). ⁴
Feb 7	IDF Team Israel Defence Force	ISRAEL	IDF (Israel Defence Force) asks the hosting company nashinet.com to remove the "Hamas" site: qassam.ps. ⁵ After the negative answer the group takes down qassam.ps (Ezdeedeen Al-Qassam Brigades Information Office), hamas.ps (The Islamic Resistance Movement Hamas Information Office), alquassam.ps (Wafa-Ahrar Brigades of the Martyr Izz al-Din al-Qassam). ⁶
Feb 7	?	ISRAEL	The Yedioth Ahronoth server farm is compromised by Arab-based hackers. Access to the media group's major news websites Ynet and Ynetnews, as well as Calcalist and Xnet, is blocked for about 45 minutes. ⁷

Date	Attacker	Target	Description
Feb 9	Hacker Team	ISRAEL	Websites. ⁸ A look to zone-h shows that the campaign is still in place. ⁹
Again Credit Card Numbers			
Feb 8	Zcompany Hacking Crew	ISRAEL	In name of #OpFreePalestine, ZHC dumps more than 200 Credit Cards belonging to Israel and United States. In their message they list the UN resolutions against Israel. ¹⁰
Feb 8	Emperor Security Team	ISRAEL	Arab hackers belonging to Emperor Security Team penetrate the Tel Aviv University Security Studies Program website (spirit.tau.ac.il/security), the head of the National Cyber Defense Authority. The hacking is quite ironic, since the National Cyber Defense Authority is supposed to protect Israel from such incidents. The hackers left images of Arabs burning US and Israeli flags. Although the real damage is negligible, the action has a huge symbolic meaning. ¹¹
Feb 9	?	ISRAEL	Another massive wave of DDoS attacks against Israeli Websites including Israel Today Magazine (israeltoday.co.il) and news sites of Israel's best-selling newspaper, Yediot Ahronot. ¹²
Feb 10		ISRAEL	Anonymous releases a video that is directed against Israeli government and its actions. The video announces a reign of terror for Israel in 3 steps: of whom only step one, initiated after the release of the video, is known. It involves systematically removing Israel from the internet. ¹³
Back to DDoS			
Feb 11	?	ISRAEL	According to the PA Minister of Communication and Information, several sites on the Palestine Networks are taken down by a Cyber Attack allegedly originated from Italy. ¹
Pastebin Psypops			
Feb 12		ISRAEL	If you want to be a hero start with saving your own lives. This is the begin of an alleged message for Anonymous from Mossad posted on pastebin. Every war is fought also with psypops and the Middle East Cyber war could not be an exception to this rule. The communiqué follows the video of the Anonymous against Israel ² and contains a dox about several members of the Collective, although there are many doubts on its truthfulness. ³
Feb 12	JERUSALEM POST	ISRAEL	...Meanwhile on the Israeli side, many doubts arise about the truthfulness of the Anonymous video against Israel, claiming it could have been forged by Iran. ⁴
And Traditional Psypops...			
Feb 13		ISRAEL	Gholam Reza Jalali, a senior Iranian military official in charge of head of the Iranian Cyber Intelligence, claims that the country's nuclear facilities have finally been made immune to cyber attacks, in particular he quotes the cyber weapons Stuxnet and Duqu targeting nuclear centrifuges and ICS. ⁵
Feb 13		ISRAEL	Meanwhile, Ammar al-Ikri, the head of Paltel, the Palestinian telecommunications provider states that hackers have escalated cyber attacks on Palestinian websites and internet servers since Palestine joined UNESCO (three months ago). PA communication and information technology minister Mashhour Abu Dakka states however that "we were able to stop 99 percent of the hackers' attacks and only a few of them were successful." ⁶
OxOmar is back			
Feb 13	?	ISRAEL	The website of the Prime Minister's Office and other websites of large Israeli Institutions are attacked and made intermittently unavailable by a distributed denial-of-service attack. According to Israel this is the prelude to a further wave of attacks. ⁷
Feb 14	OxOmar	ISRAEL	...That punctually arrives... OxOmar dumps more than 300,000 accounts and other data from the Israeli Ministry of Construction and Housing (moch.gov.il & tarbut-hadur.gov.il). Leaked data include 300,000 members, contact messages, building licenses, contractors and more. ⁸
Failed counterattacks?			
Feb 16		ISRAEL	Bank Hapoalim, Israel's second largest bank reports a failed attempt to attack the bank's system, apparently from Iran. The attack failed to penetrate a client database server. ⁹
Feb 18		ISRAEL	A cyber attack by alleged US and Israeli hackers against the website of Iran's English-language 24-hour news channel, Press TV, fails to take down the website. According to a Press TV report, the security countermeasures enforced by the Press TV technical team prevented the cyber attack on the website to be successful. ¹⁰

Date	Attacker	Target	Description
Feb 18		ISRAEL	website of Iran's English-language 24-hour news channel, Press TV, fails to take down the website. According to a Press TV report, the security countermeasures enforced by the Press TV technical team prevented the cyber attack on the website to be successful. ¹⁰
Feb 18		ISRAEL	Iran gears up for stronger cyber defense and kicks off the first national conference on Cyber Defense. Tehran says that the reason for its special attention towards the issue is due to the growing number of attacks on Iran's cyber space by US and Israel. ¹¹
Feb 19		ISRAEL	Even if it is not directly related to the Middle East Cyber War, in any case Israel is not the only country to have attracted the attentions of the Anonymous. In name of #OpIran. @s3rverexe hacks the Iran Embassy in Mexico (embajada.ir). ¹²
AlienZ is Back...			
Feb 17		ISRAEL	AlienZ Collective is back and hacks an Islamic site (islamicfinder.org) and a further site called culturecrossing.net. In the first case he dumps the administrative accounts of the server, while the second site has 300 accounts with hashed passwords dumped. Contextually the collective warns the Anonymous not to attack Israel.
New Actions Against Israel			
Feb 21		ISRAEL	A new entry Mauritania Hacker Team dumps 2065 Israel Emails logins in clear text. ² The group also claims to own a total of 15,000 emails.
Feb 21		ISRAEL	Turkish hackers SLVHACKER enter the war and deface 340 Israeli Web Sites. ³
Feb 22		ISRAEL	And immediately after they come out with more than 1000 new Israeli sites defaced. ⁴
But even Iran suffers...			
Feb 22		ISRAEL	Not only Israel attracts the attentions of the Anonymous, but also Iran does. This time is the turn of farapayeh.ir that is hacked and defaced in name of #OpIran. @s3rverexe dumps the system information on pastebin while the site is defaced by the Anonymous. ⁵
Feb 23		ISRAEL	Another Iranian site (salamkermanshah.ir) hacked by @s3rverexe for #OpIran. ⁶
And readily counters...			
Feb 23		ISRAEL	Iran Cyber Army attacks the website of Israel ally, Azerbaijan State Television. The attacks came a month after anti-Israeli hackers broke into the sites of several ministries and the governing party, leaving messages calling the Azerbaijani authorities "servants of the Jews". ⁷
Feb 28	Hezbollah Cyber Army	ISRAEL	Interesting to notice, the real world and the cyber world follow the same storyline. Iran is not so open to reforms and as a demonstration Iranian media report that two reformist websites have been hacked into by the so-called Hezbollah Cyber Army. The two targeted websites belong to the Association of Combatant Clerics, a reformist organization under the leadership of former Iranian president Mohammad Khatami, and the Baran Foundation, another organization linked to Khatami.
Another attack to Israel			
Feb 28		ISRAEL	Mauritania Hacker Team claim to have hacked the Bank of Israel and post on their Facebook page a video in which they show some accounts. They also threaten to post the account on their Facebook page. ⁸

Interview

with **Vivek Ramachandran**

Founder of SecurityTube.net



A man that you have to respect....

1. Can you introduce yourself to Security Kaizen Readers? (your biography, experience, ...etc)

My name is Vivek Ramachandran, I am the Founder and Chief Trainer at SecurityTube.net. I discovered the Caffe Latte attack, broke WEP Cloaking, a WEP protection schema in 2007 publicly at Defcon and conceptualized enterprise Wi-Fi Backdoors. I am also the author of the book "Backtrack 5 Wireless Penetration Testing". My book "The Metasploit Megaprimer" focussed on Advanced Metasploit usage for Pentesting and Exploit Development is up for release in June 2012.

I currently run the SecurityTube Wi-Fi Security Expert (SWSE) and the SecurityTube Metasploit Framework Expert (SMFE) online course and certifications which are currently being taken by students from over 40+ countries around the world. I also conduct in-person trainings in the US, Europe and Asia.

In a past life, I was one of the programmers of the 802.1x protocol and Port Security in Cisco's 6500 Catalyst series of switches. I was also one of the winners of the Microsoft Security Shootout contest held in India among a reported 65,000 participants. I had also published multiple research papers in the field of DDoS, ARP Spoofing Detection and Anomaly based Intrusion Detection Systems.

My work on wireless security has been quoted in BBC online, InfoWorld, MacWorld, The Register, IT World Canada etc. places. I had spoken/trained at top conferences around the world including Blackhat USA and Abu Dhabi, Defcon, Hacktivity, Brucon, ClubHack, SecurityByte, SecurityZone, Nullcon, C0C0n etc.

2. Can you give us more information about your web site "securitytube.net" (its goal, services provided,...etc)

SecurityTube.net was founded in 2007 to serve as a platform for security knowledge sharing using videos. Today, we feel we are positioned to build an information security knowledge portal around securitytube which will be free for everyone to use.

3. What made you take the Free Information Sharing Route instead of selling your knowledge?

I grew up in India living with my grandparents. My grandmother was a teacher in a city school and in the evenings she used to teach poor students for free. She always felt that if quality education could be provided to one and all, without a bias towards who can afford or not, then the world would be a better place. This value system stuck with me forever and has been the guiding light to me in making quality content free to one and all. I am proud to announce that SecurityTube is the only infosec training company which provides its core content for free to everyone and only charges when you want to certify.

4. When did you start securitytube.net and how did the idea come to your mind?

During my interaction with students and infosec enthusiasts, I found that most of them could not find quality learning material for free and thus found it very difficult to enter the field. There were good quality courses and certifications available even back then, but the cost was exorbitant. I thus decided to start ST to create a free yet valuable knowledge resource.

5. What Problems did you face at the beginning?

In order of difficulty:

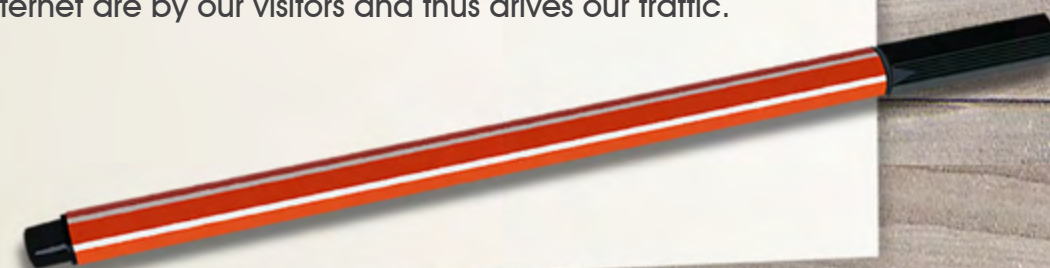
- I used to make large videos, but my Internet connection in India was so slow that I could not upload the videos ☐ Had to really work to bring down the video size.
- My accent was difficult to follow for many, but now I've managed to try and have a neutral accent as much as possible
- Hosting and Video bandwidth was very expensive and I had to really cut down on my expenses to fund the site from my own pocket

6. When did you feel that securitytube.net idea will boom ?

I really don't know. Infosec has become more important than ever today, and thus infosec education is definitely a MUST HAVE for most, rather than a good to have. I am just happy people enjoy the site and the videos.

7. Did you make any marketing for your website or it is just the word of mouth that brought you traffic

In the beginning, I used to cross post my videos to various forums on the Internet to get people to use. I never spent a \$ on any formal marketing. Today, most of the links posted on the Internet are by our visitors and thus drives our traffic.



8. Do you have a team behind that amazing work or it's only you?

Till the time I was running ST as a side project, I was pretty much alone with help from some community members like Amit Vartak, Vitomir, Prateek, Andrew, Bennett.

Once i decided to offer certifications, I had my old friend Shubhi Saxena join me as a partner and then we hired our first engineer Ashish to help build the site further. We are still continuing to get part time help from our friend Bennett, Prateek and others.

In my mind, all the visitors to SecurityTube are our extended team. I really wish to meet all of them someday face-to-face.

9. can you give us some statistics about your website now e.g number of videos uploaded, number of users watch your videos per month,... etc

We get over 100,000+ unique visitors per month and have averaged around 1 million unique visitors in the past year. We have over 15,000 registered users and around 100 unique uploads per month.

10. What do you ask from Security Kaizen readers to do regarding securitytube.net ? (More comments about your videos, upload more videos ...etc)

I would request your users to use the website, download all the free content and our courses and share them with everyone. If they are good in a particular topic in Infosec, then they could even make videos and share it with others.

11. Why did you choose Metasploit to be your first Certificate and do you get any support from Rapid7?

Our first certification was the SecurityTube Wi-Fi Security Expert (SWSE) and born out of the lack of quality practical certifications in the field of Wi-Fi security. Also, most people had a misconception that Wi-Fi Security is all about WEP cracking, when it is actually way beyond that. This is what the course illustrates.

<http://securitytube-training.com/certifications/securitytube-wi-fi-security-expert/>

Metasploit is a fantastic tool and we wanted to leverage it to show what are the fantastic things one can do with it during a pentest. The SecurityTube Metasploit Framework Expert (SMFE) is a SecurityTube offering, Rapid 7 or the Metasploit team has no involvement in it. We are however very thankful to them for creating such an amazing tool.

With the Metasploit tool, we also launched our online live labs where we have a dozen vulnerable machines which our students can exploit and learn new techniques at their own pace.

**12. What is your plan for 2012.Are you thinking of new certificate or any improvements in securitytube.net?**

We are planning to line up a couple of new certifications and also re-design the whole website ☐ Stay tuned and keep coming to the site for it

13. What is your Comment about Security Kaizen Magazine? And what is needed to rank it as one of the best magazines in Information Security field in the world?

You have a fantastic magazine in place with a motivated team pushing it. I am sure that Security Kaizen will emerge as one of the better magazines in the world. The most important task is to ensure that you create and publish new and relevant articles so that your readers look forward to every edition.

14. In your opinion, what are the top 5 magazines in the Security World?

Every magazine has its own merits and demerits. Having run a community website I know it takes a lot of effort to create something and put it in front of the world. In this spirit, I personally would like to encourage everyone rather than create a top 5 list

15. Which Security Conferences are you keen to attend every year?

Defcon for sure. I love the crew and friendly atmosphere at Brucon, SecurityZone and Hacktivity. These are definitely must-attends for me



Best Practice

“Wireless Security Threats are LIVE in your Network”

I can imagine that some of the readers are saying, thanks god, I have not allowed Wi-Fi in my network so, I'm secure and I can flip the paper BUT, wait, unfortunately YOU ARE under Wireless threats even you've chosen not to install it and even if you believe that Encryption is enough for protecting your existing Wireless Network.

Actually, we are living in an era that connectivity and number of communication channels is dramatically increasing, everybody is bringing his own Device and/or Technology inside the corporate (BYOD/ BYOT Phenomena) and would like to use that in Business, everybody needs to be online with his corporate email through his Smart Phone and/or Tablet and asking IT to provide that and commonly Security is sacrificed for Functionality or usage in such cases. One of the technologies that mostly used by these Devices is Wireless LAN or Wi-Fi and organizations are trying to entertain the connectivity by having such great technology but another aspect always over sighted which is Security.

Although, you have allowed a set of your users to be connected to your network and saved a lot in Passive Work, Cabling, Management of Floor switches, but your

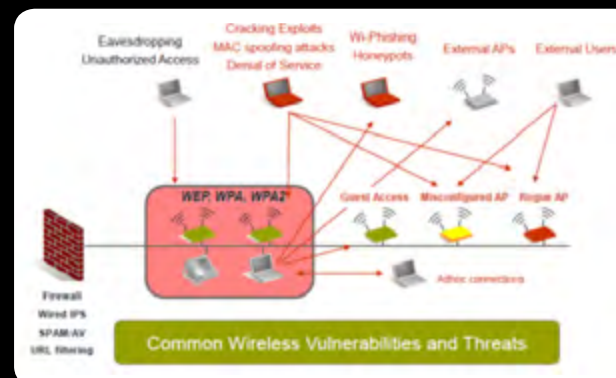
security posture is jeopardized, Security is all about Trade-off and how you choose between functionality and Security and ease of use.

What makes the matter more complex is whether or not you choose to install a WLAN, you are vulnerable to some kind of Wireless Threats, but how & what kind of threats you are talking about here..... so, let's have some scenarios to be more practical.

Scenario #1; you don't have a wireless network at all, but one of your employees who have a laptop or having a wireless card, that can be easily purchased from local market by 20-30 USD, and trying to connect to your neighbors network which they have an open network and they have a good internet speed, good advantages that hackers usually used to offer to victims, and he is sending a sensitive documents or internal email through this neighbor's network, so he typically leaked some data/information outside the organization without IT/ Information Security Departments doesn't know about that at all, but the organization will know if these information is related to their corporate advantages and if you are a popular company or a bank you will be heading a next day's news.

The above threat is widely known as “Connecting to Un-Authorized External APs”

Scenario#2; you have a wireless network and its SSID called “XYZ” which is your company name, and one hacker sits simply outside your network inside his car and published a wireless network via his Window 7 Machine called the



same name “XYZ”, but you were that expert and you have encrypted your legitimate “XYZ” by WPA2, but hacker makes it Open with internet access, so, users starts to connect to un-legitimate “XYZ” as its open and have open internet connection - with no-proxy – and starts to leaks and hacker starts to sniff and you know the rest of the story.

The above threat is widely called “Honeypots or Wi-phishing”

Scenario#3; you have a wireless network, and one of your employees purchased an Access Point – costs 20-30 USD & maybe less- and plugged it into Switch port and spread your network outside the organization, and you know the rest. The above threat is widely called “Rogue AP”

The above three scenarios are only examples and there are a lot of scenarios with its associated threats such as, WLAN Denial of Service (DOS) or Distributed DOS (DDOS) where hackers will try to make your network down and affects availability of the network, Ad-Hoc Connections is also one of the wireless attacks where users connects to each other's and share sensitive information and you won't have any idea about such communication, Misconfigured Access Point which relates to the IT/IS operation of the organization which could make your network vulnerable through missing one encryption parameter in a single Access Point, MAC-Spoofing which widely used in open encryption network with Web Authentication.

The below figure is showing the attacks that widely known for wireless;

And as you see by not having a WLAN or applying a good encryption only will not make you ahead of these threats, which makes your role harder but don't forget that WLAN brings a lot of advantages and it is the time to pay the price.

The Good news that most wireless vendors are aware of that and they are trying to implement some techniques in their solutions to be ahead of these threats, some of the vendors are implementing

that as an integrated solution such as, Cisco, Juniper Trapez, ARUBA... and some trying to protect organizations by having an overly security solution such as AirTight, Motorola AirDefense, AirMagnet...

Actually vendors are trying to implement WIPS – Wireless Intrusion Prevention System to monitor the airwaves & detect wireless threats and to be able to classify, detect, prevent & locate wireless threats.

It's Paramount to mention that neither a single product nor Technology would help you to protect yourself against such threats, its Security Strategy, collaborative defense approach and applying Security Best Practices would do but from the other hand, WIPS can help you to complete the Defense Policy and stay ahead of such threats.

The WIPS solution usually should do the following as listed in the below table, and if you would to build your own WIPS you should make the below as your minimum requirements coupled for sure with your business requirements;

Criteria	Description
Classification	WIPS would be able to classify who are the legitimate APs and which are not (External and/or Rogue) and also, which Users are Legitimate to connect to my network and which are not (External users) and by doing so, we can classify the friends and enemies – although it is an initial role but it is very important, imagine if you classify an external AP or user as legitimate!
Detection	If you would be able to detect the attacks such as Honeypots, MAC Spoofing, DOS...you will have a good view of your airwaves and easily can see the threats – this function can help you at least to know what is going on.
Prevention	if the system is good and can detect the above mentioned threats so, it will be better to be proactive and prevent these threats and make that network clean.
Locating	The system would be able to locate the source of the attack or the location of Rogue APs.
Compliance	As standard and benchmarks are becoming more mature and should be followed for certain organizations, WIPS solution would help you to meet Standards like ISO27001, PCI, SOX...

So in summary, living in a challenging era like today would have a lot of security challenges that should be looked carefully and organization should look at how the evolving communication channels and/or technologies are affecting the organization security posture and try to update its Security strategy and think thoroughly in Confidentiality, Integrity and Availability and how that can be applied in People, Process and Technology.



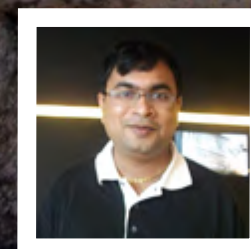
Mohamed Enab
CISSP, CCSP, SSCP

Risk Management in a Web 2.0 Environment

Introduction: Web 2.0 refers to what is known as the second generation of web development and design. Web 2.0 has brought about significant change in the internet such as web-based communities, hosted services and applications such as social networking sites, wikis, blogs video sharing sites, RSS Feeds and much more. Today, Web 2.0 delivers a new kind of Web experience that is interactive, real-time and collaborative. Although many of the underlying technical components of the Web have remained the same, the use of the Web as a platform on which to build rich applications is transforming our experience online. Organizations are also investing in Web2.0 technologies to harness the power of Web 2.0 to draw in more customers. The participatory approach of web2.0 is also taking governments by storm leading to the next generation of governance called e-governance 2.0.

As with any paradigm shift, technologies and processes can take us to a new level of user experience and productivity, but those same technologies also present us with a new level of threats and risks. Whether inadvertent or intentional, the threats are equally dangerous to the people, customers business and countries. These risks if identified and controlled in the proper way can bring a lot of benefits to the organization and society as a whole.

Managing and mitigating risks in web 2.0 requires a more diversified approach rather than a single straight approach. As per a recent study by KPMG insider report a significant percentage of the organizations are not confident on the security measures that are in place for Web 2.0. This is done through an integrated approach of people process and Technological Controls. Before we delve deep into the mitigation strategies we will analyze the threats that are evident through Web 2.0 Technologies



Vinoth Sivasubramanian

I am a founding member of ISSA UAE and a working committee member of International Cyber Ethics. CEH, ABRCIP, ISO 27001 LA,

Threat Sources for WEB 2.0

Threat Source	Vulnerable Areas
Humans	Social Networks, Blogs Instant messenger private Email etc
Systems/Networks	Browsers, unpatched systems and Servers
Application related	Applications
Improper Controls	Entire organizations is exposed

The threat table given above is not comprehensive and is intended to organize the rest of the article and is not intended to be complete, but can be used as a sample to map out threats and their implications.

Now with some familiarity on threat source, now let us analyze some of the strategies that could be implemented for mitigating and controlling the threats caused by the above sources. Threats discussed above can be mitigated through a multi layered defense process of Internal Controls, Technological controls and process.

1. Human Threats: People are the weakest as well as the strongest link in an organization. Social networks such as LinkedIn, MySpace are some of the major social networking sites where people working within the organization can leak some of the sensitive data deliberately or inadvertently. Organizations cannot block social networks because they will become the base infrastructure for business and personal interaction of the future. For effective social network usage in the workplace and to ensure that valuable data is not leaked organizations must ensure the following minimal steps

1.1 Define a policy for virtual environments: Clearly document what are the websites/activities that are allowed within the corporate environment. Also document what are the activities that are allowed in virtual environments. Take the help of a legal counsel and document the actions that would be initiated in the event of not complying with this policy.

Threat Source	Implication
Loss of sensitive data knowingly or unknowingly	Loss of Reputation in the eyes of public.
Malware, virus, spyware, logic bombs and a host of other threats	Loss of CIA, Legal Implications and Financial losses.
Malware, logic bombs	Loss of CIA, legal and financial implications.
Loss of data, virus, logic bombs etc.	Loss of CIA, Legal Implications, Reputation damage and Business losses.

1.2 Monitor virtual environments: As workplace is not the only place vital data can be leaked, therefore monitor virtual environments regularly. IT heads must make sure that they organize an internal team to monitor virtual environments for slanderous comments, sensitive data and other objectionable content. This must be done periodically at least once in a month and reports stored, deviations if any must be reported to the Management and actions taken in accordance with local laws and organizational policies.

1.3 Educate End Users: Security is everyone's responsibility. Educating End Users in the current day on security awareness has changed a lot, it becomes essential that they be taught not only the traditional Email, System and web security jargons. Educate the staff members on what can be discussed/posted on virtual environments.. Also educate them on the effects that would follow suit if inappropriate behavior is found out. Also educate them on the Potential risks that the organization is exposed to if browsing from an airport/coffee shop. Have a training manual, distribute them to everyone and keep them updated. Conduct regular security training awareness programs.

1.4 Invest in Training and Development: Keep the security people busy, invest in training the security personnel on latest threats and protection through internal resources or external training, and make sure that they stay updated on the latest trends and technologies. Security personnel who do not keep themselves

updated on latest technologies, trends pose a threat by themselves. Senior Management should ensure that these people are updated on latest trends and technologies through internal seminars conferences etc. The IT department can subscribe to good security journals such as ISSA, ISACA, IEEE etc which provide a wealth of information on security and related research.

1.5 Imbibe Ethics and Integrity into the culture of the organization: This is by far the most potent weapon for creating an almost infallible security within the organization but also the most difficult. Outlined are some simple points to imbibe a culture of integrity and ethics within the organization.

* Have a written code of ethics in place involving all business leaders, ensure that every employee sign it and make them aware on the advantages of having one in place, how and where to report in case of violations. Have regular Ethics awareness training programs for the staff members.

* Leaders and senior management must practice integrity and fairness in all their dealings, this way it spreads and percolates as a culture within the organization.

* Have and develop a mature people compliant mechanism using fair rigorous performance management systems. This will ensure that right people are retained, trained and motivated. Have incentives linked for ethical behavior and acts, measure the effectiveness over time and keep innovating for having a highly positive culture.

2. Protect System Assets: System Assets Include the servers, desktops, PDA, Blackberry's, laptops and any other asset that is used for accessing data in an organization. Since Web 2.0 Runs on all web browsers, exploitation can occur both at the server side and the client side, which can get distributed therefore it becomes mandatory to harden servers, desktops, PDA, Laptops. Some suggested

best practices for protecting systems assets are

1. A baseline standard like NIST can be used for hardening the Servers, operating systems, PDA, Desktops and Laptops.
2. Make sure an updated antivirus runs on all the system assets in the organization.
3. Make sure the necessary patches are updated on all the system assets.
4. Implement Host Intrusion Prevention Systems with proper configurations to test for anomalies on servers that host Web applications
5. Finally make sure you test all the system assets regularly to keep them updated against emerging threats.

2.1 Network Hardening: A hardened network implemented with proper next generation firewalls and necessary controls provide a vital defense for the organization against any kind of attack. Fortifying networks is probably the first level of defense and must be properly done.

Some of the basic and necessary steps that need to be performed are the following apart from the technological solutions that need to be implemented.

1. Harden all the network devices using standard baselines such as NIST.
2. Manage Change effectively on the networks. If a new route has to be added on the firewall/router make sure they go through a change management procedure and update the configuration management database.

2.1.1 Implement Next Generation Firewalls: legacy URL filtering solutions are insufficient. They rely only on categorized databases of URL entries that only update a few times a day. What is needed is a "reputation system" that assigns global reputations to URLs and IP addresses, and works alongside the categorized databases for the ultimate protection. A sophisticated, third-generation reputation system provides a mechanism for determining the risk associated with receiving data from a particular Web site. This reputation can be used in conjunction with

categories in an organization's security policy, allowing them the ability to make the appropriate decision based on both category and security reputation information. This reputation-based URL filtering solution needs to be global in scope and internationalized to handle Web sites in any language.

It is critical that the reputation system provide both Web and messaging reputation. Since malicious attacks are multi-protocol, the reputation system must be aware of both email and Web threats. A new domain without content cannot be categorized, but if it is associated with IP addresses sending email and they have a history of SPAM, phishing or other malicious activity, then the Web reputation for this uncategorized domain can immediately be determined and security protection provided to those who try to access it.

Organizations should deploy email gateways that utilize sender reputation to stop malicious attacks, often launched via spam and social engineering. Email reputation is also critical as spam, phishing and other malicious emails will include an URL or IP address that needs to be immediately fed back into the Web gateway security infrastructure.

2.1.2 Ensure That All Caches and Proxies are "Security-Aware":

Objects that are cacheable must be filtered for malware, security reputation, and URL filtering policy prior to delivery to the requestor's browser. Cached objects must have these filters applied each time the object is delivered to the end user because the reputation may have changed since the object was originally cached or the security policy of this requestor may be different than the previous requestors. This policy might be different in any of these areas: security reputation, URL filter policy or malware. Deploying caches and proxies that are not security aware runs the risk of delivering malicious code to the user.

2.1.3 Enable Bidirectional Filtering: Ensure that Bi-directional filtering and

application control are implemented at the gateway for all kinds of web traffic. This will scan all incoming and outgoing web traffic which will assist the IT security personnel in having a greater view of what comes in and goes out; filter unwanted traffic, monitor violations, incident response and forensics. Store the data onto a syslog server and archive it after a certain interval of time.

2.1.4 Implement Deep Content Protection: There are many products available in the market today for implementing deep content protection. Web sense for an example. But for achieving success organizations must make sure they have taken the following steps

1. Have a clearly defined security policy on what should be done by whom.

2. Defined what are sensitive and what is not sensitive with reference to data.

Once the above necessary steps are done then the Deep Content Protection takes care of things, Information that is classified can be ensured not to be sent over to personal Email IDs even through Official IDs. Deep content protection also empowers the IT security personnel to granularly control what users will be able to do in the virtual world using the organizational network; example users can be allowed to view social networks but can be restricted access to post.

2.1.5 Use Comprehensive Access, Management, and Reporting Tools

Enterprises should deploy solutions that provide "at-a-glance" reporting on the status and health of their services. They also need both real-time and forensic reporting that allows them to drill down into problems for remediation and post-event analysis. Providing robust and extensible reporting is a critical function to understand risk, refine policy, and measure compliance.

3.0 Application Hardening: Developing a successful and secure application involves many phases, while there are a plethora of articles and standards

available online on the application related vulnerabilities of Web2.0 and how to deal with them, we will focus on the overall picture including the soft concepts. We do not dwell into each and every exploit here but outline those basic steps that need to be taken which has been overlooked in comparison with technical related vulnerabilities. Following these simple steps can ensure to a good extent that the applications are securely built, Future Vulnerabilities can be easily dealt with if these simple guidelines are followed.

1. Have/ Hire competent programmers in place who are also deft at handling application security. Develop a culture of secure programming within the IT Team. Have the Information Security personnel participate in the development process.

2. Practice good coding standards using baselines and other standards available from various resources, one good resource is (www.owasp.org). Ensure that they are strictly followed by the programming team.

3. Create a Threat model of the application using known and unknown incidents and do stressful penetration tests on the application before they go live. Document the recordings of the tests. This will serve as a reference point for building future applications and saves time and money.

4. Have a matured risk assessment/ management process in place that has a holistic approach towards the application going beyond applications. By having a matured risk management process in place, process becomes repeatable which saves a lot of time when newer applications are built.

4.0 Process and policy Control Mechanisms:

4.1 Security Policies In place: Have effective security policies in place and ensure that they are followed by everybody. Always have them current in line with changing trends of security and business and measure their effectiveness by conducting regular awareness quizzes. Monitor for violations using technology,

process and people. Record and rectify them.

4.3 Incident response: In spite of the best firewalls and effective security policies and audit and the best people, breaches and threats can be realized and if such an incident happens make sure there is an incident response plan in place on how to deal with that situation. Train People on Effective Incident Management procedures.

4.4 Conduct Continuous Risk Assessment: Conduct Regular risk assessments on Web applications with a holistic approach towards security and check to see if the controls are to an optimum and desired level as expected by the business units and executive management.

Following Bench Marks: Finally benchmark your protection strategy at regular intervals against global standards or other best practices followed by your peers or other organizations. Align them to your business needs if needed.

Conclusion: Web 2.0 is a boon and if implemented and managed properly organizations societies and countries can benefit from the participatory approach of Web2.0. Organizations and governments spanning countries must come forward with good regulations, measures for making this new trend a success for one and all as cyber security and websites cannot be restricted to a single country alone.

References:

Jacques Bughin and James Manyika, how business are using Web 2.0 Mckinsey Global Survey 2007.
Claire Le Masurier, Risk concerns stall uptake of Web 2.0 Technology in the workplace, A KPMG Insider Report 2008.
Web 2.0, www.wikipedia.org
Web 2.0 Security Threats, www.enterprise2.0.org
Losing Ground global Security Survey 2009 from deloitte.

احجز اختبار

CEH
Certified Ethical Hacker

منحة خاصة

لعشرة متدربين فقط

الأولوية بأسبقية الحجز

Security



CEH
Certified Ethical Hacker

اختر أحد العرضين مجاناً

2

المادة العلمية الأصلية
مجاناً



1

دورة تأهيلية
مجاناً



nen
National Education Network

في إطار خطة تطوير الأداء و تنمية الكوادر البشرية لمواكبة متطلبات سوق العمل، تقدم الشبكة الأهلية للتعليم عرض خاص بالبرامج التدريبية المعتمدة دولياً في مجالات أمن المعلومات و الاتصالات.

و نود ان نوجه عناية سيادتكم ان شركتنا معتمدة من الجهات الآتية:

- شريك تعليمي لكل من: Microsoft - CompTia - Oracle - CWNP - EC-Council - Mathworks - CIW
- مركز اختبارات لكل من: ETS_TOEFL IBT - Prometric - Pearson VUE - ICDL
- شريك للدعم الفني لكل من: Symantec - National Instruments Juniper - Cisco
- معتمد من هيئة اتحاد النقل الجوي الدولي IATA في تقديم الاختبارات الدولية والتدريب الخاص بالطيران
- معتمد من مجلس التدريب الصناعي (ITC) التابع لمركز تحديث الصناعة (IMC)
- معتمد من هيئة تنمية صناعة تكنولوجيا المعلومات ITIDA
- معتمد من غرفة صناعة تكنولوجيا المعلومات

مميزات العرض

- الشركة حاصلة على جائزة احسن مركز جديد في افريقيا و الشرق الاوسط
- المدرب حاصل على رخصة ECI واحد من 9 في مصر
- التدريب يتم على المعامل و البرامج الاصلية المعتمدة CEH Lab Setup Guide
- الشركة توفر المادة العلمية الاصلية مجاناً
- الطالب يدرس محتوى الدورة المعتمد بالكامل
- العرض يشمل الاختبار الدولي
- الشركة توفر لك تصريح دخول الاختبار خلال 24 ساعة مصروفات التصريح 100 دولار تحصل من خلال E-Council
- الاختبارات تتم داخل فروع الشركة
- الطالب يحصل على عضوية EC-Council
- الطالب يحصل على كود المرور الخاص بملفك سيمست و المسجل به حتى الان 11280 هاتركز على مستوى العالم
- الطالب يحصل على كود فرانكشتين الخاص ببرامج الهاكرز الاصلية

لمزيد من المعلومات والاستفسارات: 01114702711 - 01068827096 - 01068827099 البريد الالكتروني: eccouncil@nen-global.org

nen
National Education Network

www.nen-global.org



CENTRAL BANK OF EGYPT
Egyptian Banking Institute

Information security training??

At EBI

International experts,

exceptional quality

competitive prices!



INTERNATIONAL COOPERATION



UPCOMING COURSES

Vendor Name	Course Name	Date
HP	Certified IT Manager	6 - 8 May 2012
IIR Middle East	Business Continuity Management and IT Disaster Recovery	7 - 10 May 2012
EC Council	Ethical Hacking and Countermeasures v7.0	13 - 17 May 2012
CISSP.COM	Certified Information Systems Security Professional "CISSP Official Review Course"	20 - 24 May 2012
EC - Council	Certified Hacking Forensic Investigator	20 - 24 May 2012

Ask about the
Early Bird
Discount



For further enquiries, you can email us at: ITTraining@ebi.gov.eg or call us on Tel: (202) 24054472- Ext (530) (556) (403) Fax: (202) 24054471 Address: 22 A, Dr. Anwar El Mofty St., Tiba 2000 Bldg. Cairo, Egypt P.O. Box: 8164



A BI WEEKLY LIVE ONLINE SHOW



2day adv. 01000255359

MEET THE INFORMATION SECURITY EXPERTS

[HTTP://WWW.BLUEKAIZEN.ORG/BK-RADIO/](http://www.bluekaizen.org/bk-radio/)