September 2012

VECTOR

A Net-Square Initiative

A series of articles specially designed for the information security professionals.

Hiren Shah
President, Net-Square
reach him at hiren@net-square.com

Secure • Automate • Innovate

Net-Square Solutions

is a niche Application and Network Security Service provider. Net-Square provides Consulting Services like Vulnerability Assessment, Penetration Testing, Code Review, Reverse Engineering and Security Architecture Consulting

Net-Square also offers Products like Server Defender Vulnerability Protection (SDVP), a web application Firewall for IIS applications and NS Webscan, an automated application vulnerability scanner

Last but not the least is the training programs. Net-Square offers a variety of customizable training programs for the benefit of end users and developers.

~~Breaking~~ Hacking News:

Cybercrime hits 42 million people in India in past 12 months!

A recent annual cybercrime report by Norton reveals that in the past 12 months, 42 million people have been impacted by consumer cybercrime which has cost India around Rs. 42,000 crores! Report further mentions that 56% of adults who go online have experienced cybercrime which makes it over 1 Lac victims per day, 80 victims per minute!

Read more:
http://articles.timesofindia.indiatimes.com/2012-09-13/india/33815436_1_consumer-cybercrime-victim-symantec

What would you like - “Breadth or Depth?

Net-Square is growing, both in terms of number of Customers and number of people. In fact we have the happy problem of having to go out an aggressively hire. But as we realized through the process, it is not so happy problem after all.

The not so happy part is that it is really hard to find good “Breakers” out there. And this has happened due to various factors.

Primary among them is the misconstrued notion among the many young aspirants, who want get into this very promising field, that if they get Certifications, then that will be enough to get them a job. In the last 6 months, I have been in many interviews where the candidate arrived with many Infosec related certifications, but were severely lacking in basic knowledge required for them to even begin working in the domain of Application Security. The number of participants with CEH (Certified Ethical Hacker) that passed Net-Square’s test was in single digits in percentage terms. And contrary to that we found some individuals who had no certifications, but highly talented and skillful in the domain of Black box and White box testing.

When we interviewed many candidates who worked with our peers in the Industry and who showed experience in the domain of black box testing on their CV, we found them ruefully lacking in doing any manual testing. The stock answer was “We run some tools and than check if there are any false positives”. Or we found them to be doing many other functions related to Security Operations leaving them with no time to hone their skills in Application Security. This tool dependent approach does not do justice to Application Testing. There is a very good article that captures this aspect - “Why Johnny can’t Pentest” -> http://www.cs.ucsb.edu/~adoupe/static/black-box-scanners-dimva2010.pdf

Thirdly, it is important to recognize that Information Security function has many different domains. Running Security Operations (like log monitoring) is very different from that of Black Box testing. They both need different skills and therefore different individuals doing it. But in their eagerness to increase business, many Security firms position one, two or three resources that end up doing everything and therefore end up turning into the classic case of “Jack of all and Master of none”.

In my tenure as a CIO, I have always found that niche firms deliver the best value for money. I have always believed that unless the resources deployed by your Partner have more depth than your internal resources in the domain where they are serving your Organization, there will soon set frustration in the relationship. In fact that was my frustration with many Software Services Partners, which prompted me to build my own team.

I humbly request my colleagues from the Industry to recognize this distinction and appropriately adjust their process so that it becomes possible for them to access the best service available. And that will always be with firms who decide to build depth in their offerings rather than breadth.

Until next time, stay safe!

-Hiren
Follow Hiren's views on Twitter @hiren_sh or on his blog: The Thought That Counts

Every day is a 0-day!

Last month, I wrote an article about 0-day exploits and the time it takes to fix them. [Read Vector August 2012]. Little did I know that September would bring FOUR critical 0-day exploits!

The first bomb went off on September 14. The world came to know of a critical bug in IE being exploited in the wild. The vulnerability, now assigned CVE 2012-4969, affects IE 7, 8 and 9 and allows an attacker to execute arbitrary code in a victim's browser. Microsoft was totally caught unawares and so were a large number of users and organizations on the Internet. As usual, anti-virus engines saw no evil, heard no evil and maintained silence. Microsoft issued security bulletin MS12-063 with an emergency patch on September 21. Net result? Intelligence agencies, cybercriminals and script kiddies would have had a glorious week compromising systems left right and centre!

Four more days go by and we have a hat trick of vulnerabilities on September 25. The first of them was a backdoor inserted in phpMyAdmin which allows an attacker to execute arbitrary commands. A malicious PHP file called server_sync.php was inserted in one of Sourceforge's mirrors in phpMyAdmin version 3.5.2.2's code repository. Sourceforge confirmed around 400 downloads of the backdoored phpMyAdmin before they shut down the compromised mirror. This isn't the first time an open source software repository has been compromised. This begets the question - do you verify checksums and hashes on open source software that you download? I confess that I don't do so all the time.

Cut over to Ekoparty 2012 - one of South America's famous hacker conferences held in Buenos Aires. Ravi Borgaonkar demonstrated a really simple yet evil trick which triggers an unstoppable factory reset in a majority of Android phones! The trick is achieved by forcing the phone to dial USSD codes using a "tel:" URL in three easy steps. Step 1. Create a web site which embeds a "tel:*2767*3855#" URL. A URL shortener can also do this job. Step 2. Lure the victim to this website. Step 3. Watch victims see their phones blank out before their very eyes. Mobile browsers automatically dial the USSD code without prompting the user! This behaviour is an example of undesired functionality. To test if your phone is susceptible to this bug, point your mobile browser at http://tinyurl.com/testussd. It is uncertain when this problem will be fixed.

The last vulnerability is more of an announcement at this point. Adam Gowdiak, once a member of the Polish hacker crew "LSD", has announced that all versions of Java 5, 6 and 7 suffer from a major sandbox bypass vulnerability. A Java applet loaded in your browser can execute arbitrary commands on your system. All operating systems running Java are affected since the vulnerability lies in the core Java Virtual Machine itself. The vulnerability was announced on the Full Disclosure mailing list on September 25. The full text of the announcement is available here - http://seclists.org/fulldisclosure/2012/Sep/170. A word of advice, please disable all Java plugins on your browsers!

0-day exploits are the Black Swans in the world of information security. We tend to turn a blind eye to the high impact of these hard-to-predict rare events and react with irrational shock, amazement and disbelief when they occur. Will the next day be another 0-day? Who knows.

- Saumil Shah, CEO, Net-Square

Daisy-Chain Attacks
A Hacker's new tool

Application attacks and hacking accounts for critical data is soon becoming a thing of past. Attackers are now moving to hybrid attacks, where they try to get information from various sources and means. This includes a combination of stealing information through social engineering, social media, personal accounts, and websites. This proves to be a deadly weapon in a hacker's armory as they can cripple an organization or an individual causing unthinkable damage! Most vulnerable seem to be various accounts and assets which are usually linked together for ease of remembrance and use. Here is how recently, a technology reporter got his Amazon, Apple, Google, Twitter accounts hacked which were daisy-chained together.

A hacker broke into this reporter's Amazon account with some not-so-clever social engineering. The hacker got to see the last 4 digits of credit card which Amazon thinks are unimportant. He used this to break into the reporter's Apple account. He reset the reporter's Google account as it sends recovery information to the Apple mail account. He also reset the reporter's Twitter account as it sent recovery information to the Gmail account. Not only this, the hacker also wiped the reporter's iPhone, iPad and MacBook remotely. Hacker then deleted the reporter's Google account, took over his company's Twitter account linked to his personal account. The twitter account was utilized to post racist comments! Unbelievable, isn't it?

Interesting point to note is some of the basic information, like last 4 digits of credit card number could be retrieved by other simple methods too. Individually each service's recovery policy might be secure, but when you solve the jigsaw puzzle of recovery policies of individual services, you see how vulnerable it can be!

So how can we avoid this? Seems we need to go back to our old days and utilize some of the better techniques we used to adopt. Some of the preventive measures which can be used include a Regular Backup of data, turn on two-factor authentication if available, do not daisy chain vital accounts, and last but not the least, do not use core accounts for recovery. As the old idiom says, Prevention is always better than cure!

- Sanjay Awatramani, Software Architect, Net-Square