July 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

"To ~~Be~~ DO" or "Not to ~~Be~~ DO"

In continuation of my series of "To" or "Not to", I present here the ultimate dilemma facing many of our friends from the Corporate Information Security groups. And that dilemma is "whether to do PT (penetration testing) of an application on the live environment or Not"? Having been in that situation myself in the past, I fully empathize with the fact that this question does not have an easy answer.

On one side is the desire to test the actual deployment of the application so that you have the very true picture of the vulnerabilities and can provide as close an environment to the testers as the attackers would have. While on the other side, one doesn't want to jeopardize business because of the application downtime, which maybe caused by the PT. Allow me to share my views on how to approach this challenge.

The starting point of getting an answer to this question is how critical is the application, not from a business perspective, but from a risk perspective. In my view, every application that is exposed on the web should be considered critical. Why? Because if that application is not secure than it will become a gateway to other applications on the Organization's internal network being targeted. Any other application, which stores vital business information, should be considered critical whether they are exposed to the web or not. We advise clients to do a formal risk assessment, as that tends to help in arriving at criticality from availability, confidentiality and integrity perspective. Any application that has significant consequences on any of those three aspects should be considered critical.

Now having identified the critical applications, it should be easy to perform PT on a live environment since most industry regulations require critical applications to have a disaster recovery set-up. If there is PT being performed on a live environment, which has a DR than that reduces the risk of downtime as the DR site can be invoked in case the live environment is affected by any chance.

Doing PT on live environment has its own benefits. The obvious one is that you are getting testing done on an environment, which is exactly the one that the attackers will be accessing. You will not miss any configuration change or difference in code upload that may introduce new vulnerabilities after the PT.

So next time you have the inclination of doing your PT on the live environment and are facing the dilemma, use the DR card with your business team / IT team and "Just Do it". For all you know, you may even get the DR part tested as a precursor to the PT testing!

Until next time, stay safe!

-Hiren

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

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:
Major Trojan attack uncovered by Japanese Finance Ministry
A Trojan cyber attack on computer systems which lay undetected for almost 2 years was discovered recently by the Japanese Finance Ministry. The Trojan was free to steal confidential data from Jan 2010 to Nov 2011. A total of 123 computers inside Ministry were infected out of around 2000 checked so far. To read more visit:

http://news.techworld.com/security/3371587

My Annual Blackhat pilgrimage

As my aircraft touched down in Las Vegas, I couldn't help but tell myself, "Year 14, here I come". My first introduction to Blackhat was in 1999 as a Unix hacker at E&Y. Blackhat and Defcon were fledgeling conventions, attended by a group of individuals who were truly passionate about information security. I have never seen a more diverse group of indivuals from all walks of life driven by a common creed, a quest to push the boundaries, explore the unknown and to "boldly go where no one has gone before!". For me, it has become a place of pilgrimage.

Over the years, I have seen the infosec scene evolve and grow. Back in 1999, society at large was oblivious to cyber threats and attacks. "Yes, but this wouldn't affect me, would it?" was the general response from people who heard me talk about my research and my job. Today the whole world is well aware of cyber threats. Planting a virus to take down a nuclear weapons manufacturing factory was a thing of science fiction three years ago. Governments and military divisions are treating cyber warfare as an important strategic theatre. Large corporations are employing internal red teams for proactive information security. And the threats to an individual have increased manifold.

Technology penetration over the past decade has been of staggering proportions. Today, we carry an Internet signal with us in our pockets, wherever we go. Along with technology comes its slew of threats. For years, the industry has been trying to fix information security problems with technology - a strategy that hasn't done well at all. I heard predictions about the death of buffer overflows in 2002. I heard that managed endpoint security would prevent all threats to the desktop. I heard that firewalls and anti-virus will save us all. And yet here we are talking about more of the same things in 2012! This year, I was teaching advanced exploit development as a part of pre-conference training. One of our class modules was on exploiting Android. I couldn't help but laugh at how we are transported back to 1999 when buffer overflows and malware were rife on desktops. We see the same happen on mobile platforms today.

Social engineering, coupled with social networks has become a very successful attack vector, where the hacker's target is the human brain. In our overloaded digital lives, it is easy to be blindsided with a sophisticated social engineering attack. 2012 has revealed many interesting observations. We are seeing a convergence of different types of attacks coming together, to create a potent cocktail of digital weaponry.

Another lesson learned from these past thirteen years is that "as one door closes, another door opens". We have seen a number of good and bad solutions from the industry to neutralize attack vectors. 1999 was the year of RPC buffer overflows and we had a field day popping shells in penetration testing exercises. Firewalls put an end to that by preventing connections to the RPC ports. Come 2000 and we shifted our focus to web hacking, attacking what was available through HTTP. No more layer 3 attacks. It was all about layer 7, the application layer. In 2005, the focus moved to desktops and browsers, catalysed by broadband networks and growing social networking sites. USB Autorun came next with the proliferation of removable mass storage. Today we have complex hybrid attacks involving multiple vectors chained together.

At Blackhat, I have truly experienced the adage "the more things change, the more they stay the same". And it is these insights that keep bringing me back to Blackhat. It has become my moment of religious observance. One that if I don't partake, it would be blasphemy!

- Saumil Shah, CEO, Net-Square

"Smart"phone ≠ "Smart"security

Recently, I spoke with the CISO of a well-known Private Sector Bank in India. He said, "I am currently not much concerned about my Web Application or Network Security, because we are well covered on that. But it is the mobile application security that is bothering me."

According to a report by marketsandmarkets.com titled 'World Mobile Applications Market (2010 – 2015)', the total global mobile applications market is expected to be worth $25 billion by 2015. And it is growing at a rate of 29.6% (CAGR)! Currently the Smart phone market is hogged by iOS, Android and Blackberry. With more than half a million apps on each of these platforms, how can Apple, Android or Blackberry check whether these apps are not vulnerable from the same kind of issues that desktop application vendors or websites are.

Blame it on market competition, but the mobile application developers today focus more on user attraction with excellent GUI rather than the security of application itself. The rush for going live keeps developers away from testing or rather securely coding applications. The result is unintended vulnerability holes that create access points for hackers!

So why should a CISO of an Organization become so worked up over mobile security? After all the issue lies at the door of these platform providers like iOS or Android or at the most with third party app providers? The reason is simple. If the Smartphone is infected with malware and is also connected to the corporate network for e-mail or other mobile-based applications and those applications are not checked for vulnerability, it won't be long before the corporate network is penetrated through these devices. Just the same way malwares are being used on desktops! After all mobile is only a device - path to the real information.

At Net-Square we saw this coming some time ago and therefore have build the capability to test both Android and iOS based applications. And many of our clients are now using our services to have their mobile apps tested. But there's more to it. Only doing AppSec testing may not suffice in case of mobile applications. Mobile appsec testing has to be combined with a concerted effort to make people aware of the risks posed by Social Media since that is one big utility of Smart Phones. Conducting Social Media Threat Evaluation is very important. That will give the Infosec leaders insights into the use of Social media by their people. They can than define the right policy and conduct roadshows on the use of social media sites like FaceBook, Twitter etc. whether on Smart phones or otherwise. Otherwise it won't be long before someone puts the most coveted trade secret on Facebook with a message "I got a pat from my boss for this today!"

-Hardik Kothari, Business Development, Net-Square Solutions