May 2012

VECTOR

Perspectives on what's happening in the world of Information Security

Saumil Shah
CEO, Net-Square
reach him at saumil@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.

Our Analyst gets a pat from Microsoft:

Recently, Jigar Soni, one of our young and energetic analysyt found Cross Site Scripting vulnerability in one of Microsoft's online web applications.

As an ethical practice, Jigar disclosed the vulnerability directly to Microsoft. Microsoft appreciated and acknowledged Jigar's contribution in their bulletin → Click here

Jigar works on many of our consulting engagements

PEBKAC!

The über geek readers will be smiling already. The acronym has been popular for over two decades, yet it is only now that I can fully understand its implications in the information security arena. 2001 was a turning point of sorts in information security when attacks moved away from network services towards HTTP. It was the dawn of "web hacking". When I was writing my book "Web Hacking: Attacks and Defense", there were a handful who fully grasped the implications of the next wave of attacks. Today, Johnny the Pen-Tester is busy compiling reports full of SQL injections and XSS attacks.

2011 marks the sunrise of advanced social engineering attacks. We are talking attacks beyond phishing and scams. A few years ago, "spear phishing" - targeted attacks towards key individuals or organizations - existed only in science fiction. Early this year, Net-Square was engaged in a very unusual penetration test. One that was aimed at testing the "Human Security Factor". Are the individuals in our organization resistant to a security breach? Can our organization detect and defend against such a breach? And can sensitive data be exfiltrated without being noticed?

Here is what happened:

Monday: A Linked-In invitation appears in the inboxes of employees of a financial services company. A new smart trendy kid out of Wharton has joined the marketing team, promoting the company in today's digital age. We had over 300 connections at the end of the day.

Tuesday: Articles being sent around, initiatives being discussed, connections made on Twitter and Facebook. We are getting personal. We start understanding the hot topics being discussed.

Wednesday: The marketing wizard recommends a piece of software to be installed on everyone's desktops, to "keep up with the trends". 15 installs in a matter of 3 hours. Our custom software incidentally does more than help users keep up with the trends.

Thursday: PDF documents circulated, with the title "allegedly leaked from boardroom meetings". What was not mentioned was that they contained one of the latest exploits, custom written to run a few harmless commands on the reader's desktop.

Friday: End of exercise. More than 30 desktops compromised. Custom software with advanced stealth data exfiltration capabilities installed. Sample data exfiltrated out of the inner belly of the company. Suspicious activity detected by anyone in Client's Organization: NIL.

You are looking at the penetration testing methodology of the next decade. It is easy to be victims of tunnel vision. On one hand you have compliance reports to worry about. Your firewalls and IDS are blinking incessantly. There is a non-stop download of Antivirus updates. DLP agents on every computer. SIEM dashboards. Log aggregators. UTM. WAF. It is a long list. We are missing one major area of attention. What about us? The humans? The users themselves?

The socially connected Internet makes it a breeze for attackers to target individuals and sneak into the organization by hiding in plain sight. The vulnerability being exploited here is a simple one - PEBKAC. Problem Exists Between Keyboard And Chair.

So if you want to test the PEBKAC in your organization call us to perfrom a SERT – Social Engineering Response Test. E-mail us at info@net-square.com. – Saumil Shah

"The safest computer is one that is turned off. Everyone knows that!" … well not anymore!

If you ask any sysadmin "which is the safest computer", she (btw, this is the new trend of being politically right) will reply that the safest is one that is turned off. But this is no longer true! Thanks to a new auxiliary module available in the latest release of metasploit. This is possible by making use of the Wake-On-LAN (WOL) feature used by administrators to remotely power up a computer on the local network.

WOL makes use of 'magic packets' which consist of 6 bytes of 255, followed by the target's hardware MAC address repeated sixteen times. This packet could be sent as a UDP datagram to port 7 or 9, or it could be sent directly over Ethernet as EtherType 0x0842. The packet itself is broadcast to all hosts on the network. While this service usually works over the local subnet, certain switches, such as Cisco Catalyst layer 3 switches, can be configured to support WOL across VLANs. The consequences of this are that systems, which were not thought to be reachable, can now be powered on. Currently, you need to know the MAC address of the target system. But it is a relatively simple task to modify the module to generate frames for a range of MACs or MACs belonging to a particular manufacture. WOL also features a password feature that is 4 or 6 bytes long. But this too can be brute forced because of the relatively short length.

So does this mean that all systems automatically vulnerable to attacks? No. But it does help an attacker find another attack vector into the network that has been missed by the administrators.

So how do we address this issue? If WOL is not required, the feature needs to be turned off from within the bios. At the very least, a 6 byte should be set for each system that has this feature enabled (if the password feature is available). Furthermore, MAC access lists could be used to prevent anyone other than the Administrator from sending WOL frames. IDS and IPS can also be of use here to detect any abnormal frames on the network, such as a multitude of WOL frames.

-Rohan Braganza, Net-Square Team

Check the URL in your browser….

I have seen interesting messages from Financial Institutions on the web and at other places educating customers on checking the url in the browser before putting in the login id and password. But will that really help given the instant response that users normally have to any instruction that they receive in e-mails and online? Unfortunately not! The problem lies in how we as humans are wired to perceive online threat. In the Online world the only sense that can be used is "sight". One tends to decide if something looks "fishy" only based on what they see. But it is very easy for fraudsters to even fool this one key sense.

Recently we came across a very interesting vulnerability where, a user can be redirected to a phishing page on a website where the URL would look absolutely genuine. The fraudster would send this link in an e-mail to the target victims or host them on many of the online social media sites with more of a marketing message like "login and sign up for low interest rate loan offer". The url shown on the browser would look absolutely like the original url, fooling even those clients who check the url in the browser before doing anything.

We therefore strongly recommend a simple message from the Financial Institutions to their clients - "Just do not click on any links period". Similarly they should post other messages like "Do not access your our site at a cyber café" not "Change your password after accessing our site at a cyber café". Yes, that limits the options for the customers, but isn't it better to be safe than sorry!

- Sanjay Awatramani, Net-Square Team