International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 11 Issue 5 –NOVEMBER 2014.

A Detailed survey on Malware and Vulnerability Scanners

Battula Trivikrama Rao

Asst Professor, Department of IT, UshaRama College of Engg & Tech, Telaprolu, Vijayawada, A.P., India

Abstract— Malware stands for Malicious Software. Terms such as Virus, Trojan, Worm, and Bot all have specific meanings. Malware is used to generically describe any malicious software, regardless of its technical category. Vulnerability scanner is a software program that has been designed to find vulnerabilities on computer system, network and servers.

In addition to the manual security test and code review, automatic tools always play their roles to make the vulnerability assessment efficient. There are many aspects that you should consider before using any tool; aspects are including but not limited to the cost, features, reporting pattern or simply management. This article contains the list of the malware and details of top vulnerability scanner tools that you might require in security testing process.

Index Terms— Adware, Botnet, Rootkit, OpenVAS, CoreImpact

I. INTRODUCTION

MALWARE

Adware

A type of Advertising Display Software, specifically certain executable applications whose primary purpose is to deliver advertising content potentially in a manner or context that may be unexpected and unwanted by users. Many adware applications also perform tracking functions, and therefore may also be categorized as Tracking Technologies. Some consumers may want to remove Adware if they object to such tracking, do not wish to see the advertising caused by the program, or are frustrated by its effects on system performance. On the other hand, some users may wish to keep particular adware programs if their presence subsidizes the cost of a desired product or service or if they provide advertising that is useful or desired, such as ads that are competitive or complementary to what the user is looking at or searching for.

BOT

Short for "Robot" a bot is a program that is designed to automate tasks. Initially bots were used in the UNIX world to automate dull tasks that system administrators frequently perform. Some bots will automatically chat with a user, simulating a human response to questions. Bots can also be used maliciously to allow a remote attacker to control a victims PC. The nature of many bots is such that it is as easy to control one PC as one hundred thousand PCs. Bots can be used to send spam, download and store illegal files, such as some types of porn, or to make computers participate in attacks on other computers. A bot can be made to search the victim's hard drive and send confidential information to a remote site on the internet in order to perform identity theft. Computers that are infected with bots are often called drones or zombies.

BOTNET

A botnet is a group of bot infected PCs that are all controlled by the same "command and control center". Recently peer-to-peer (P2P) botnets have been used. These botnets do not have a traditional command and control center but they are all part of the same "army".

Hoaxes

Hoaxes are usually silly pranks, and are a form of chain mail, and are often also Urban Legends. Computer Virus hoaxes try to generate fear, uncertainty and doubt (FUD) in the recipients, bringing them to believe that there is an 'undetectable virus' on their system (how can it be undetectable if you can detect it?). Some have actually been malicious in content, causing the recipient to delete files from their systems. They should simply be deleted. There is no good luck from sending them to 20 of your friends, nor are they a way in which you will learn anything about the security of your computer

Payload

The additional functionality, for instance data stealing, file deletion, disk overwriting, BIOS flashing etc that may be included in a Virus, Worm or Trojan Horse. Note that the payload does not necessarily have to be damaging - for instance the payload of the Form-A virus was to make the keyboard make clicking noises on one day a month - it did no damage other than that. In the case of a Trojan, it is the 'secret' function that the programmer wanted to achieve.

Phishing

Phishing (pronounced in the same way as fishing) is a social engineering attack which attempts to fraudulently acquire sensitive personal information, such as passwords and/or credit card details. Usually this is achieved by sending e-mail (or similar communication) masquerading as a trustworthy person or business with an apparently legitimate request for information. The most common Phishes look as though they come from popular high-street banks, and usually contain some sort of threat of discontinuation of service, or other undesirable consequence if the instructions are not followed. Sometimes a the mail will look very genuine, and will contain branding and content which may have originally come from the source that it is impersonating. Usually there will be a link in the mail that will take the recipient to a website (which also may look very much like the legitimate site), and this site will be used to capture the details being 'phished'. It is important to remember that banks, and legitimate companies like Ebay or PayPal will never request usernames and passwords in unsolicited email. It is also worth bearing in mind that the links in phishing emails although they may look legitimate, will almost always point to a different site underneath. Always open a new browser session and type the correct address into the Address bar when you are trying to get to your internet bank or other online services.

Rootkit

A rootkit is a collection of one or more tools designed to covertly maintain control of a computer. Initially rootkits appeared on the UNIX operating systems (including Linux) and were a collection of one or more tools which allowed an attacker to gain and keep access to the most privileged user on the computer (on UNIX systems this user is called 'root' - hence the name) On Windows based systems, rookits have more commonly been associated with tools used for hiding programs or processes from the users. When installed a Windows rootkit uses functions in the operating system to hide itself, so as not to be detected, and is often used to hide other malicious programs such as keystroke loggers. The use of rootkits is not necessarily malicious, but they have come to be increasingly associated with undesirable behavior and malicious software.

Scams

Scams are very similar to phishing, but are not usually interested in obtaining your details, they often appeal to a sense of compassion or to human greed. For instance, almost every disaster (earthquake, flood, war, famine) has generated large amounts of scams, usually in the form of appeals for charitable aid for a 'worthy' cause. Advanced Fee Frauds (sometimes called 419 scams) offer you the opportunity to get a large amount of money by supposedly helping the scammer to transfer even larger sums of money out of a country (often an African country such as Nigeria). These scams always result in you being asked to send the scammer some money to cover "administration" costs (often this is several thousands of dollars). Sometimes, these scams have resulted in the person being scammed disappearing, either killed or kidnapped after traveling to another country to meet their 'benefactor'. In less extreme cases, many people have lost thousands and thousands of dollars to these frauds. Some tips for avoiding such scams: Legitimate charities usually only send appeal emails to people who have explicitly chosen (opted in) to receive emails from the organization. Unsolicited, such emails are almost always fraudulent - particularly ones that appear quickly after a disastrous event Don’t be fooled by appearance. E-mails can appear legitimate by copying the graphics and language of a legitimate organization. Many include tragic stories of victims of the disaster. Don’t click through to links: links in emails can lead to “spoofed” Web sites that mirror the look and feel of a genuine organization. There's no such thing as a free lunch - If it looks too good to be true, it almost always .

Spyware

The term Spyware has been used in two ways. In its narrow sense, Spyware is a term for Tracking Software deployed without adequate notice, consent, or control for the user. Often the tracking is done by reporting information (anything from browsing history to credit-card or personal details) to a third party. Some Spyware is delivered as part of another program (much the same way as a Trojan Horse), but some is delivered as a Payload to a Worm, or via websites which exploit vulnerabilities in browsers to silently install the programs in the background. There are also many programs which pretend to be Anti-Spyware programs, but are themselves Spyware. In its broader sense, Spyware is used as a synonym for what the Anti-Spyware Coalition calls “Spyware and Other Potentially Unwanted Technologies.” This can include some types of cookies, commercial keyloggers and other tracking technologies.

Trojan Horse

A Trojan Horse, often referred to as just a Trojan, is a program which purports to do one thing, but actually does another. Not always damaging or malicious, they are often associated with things like deleting files, overwriting hard-drives, or being used to provide remote access to a system for an attacker. Classical Trojans include keyloggers being delivered as game files, or file deleters masquerading as useful utilities. Trojans can be used for many purposes including Remote Access (sometimes called Remote Access Tools or RAT's, or Backdoors), Keylogging and password stealing (Most spyware falls into this category)

Virus

A virus is a program which replicate by copying itself, either exactly, or in a modified form, into another piece of executable code. Viruses can use many types of hosts, some of the most common are: executable files (such as the programs on your computer) boot sectors (the parts of code that tell your computer where to find the instructions it uses to 'boot' or turn on) scripting files (such as Windows Scripting, or Visual

Basic script) macros within documents (this is much less common now, as macros in, for instance Microsoft Word, will not execute by default)

When a virus inserts itself into other executable code, this ensures it is run when that other code is run, and the virus spreads by searching for other 'clean' hosts every time it is run. Some viruses overwrite the original files, effectively destroying them, but many simply insert themselves in a way that they become part of the host program, so that both survive. Depending on the way they are coded, viruses can spread across many files in the system, across networks via file shares, in documents, and in the boot sectors of disks. Although some viruses are spread by email, this does not make them viruses, and in-fact, most of the things that spread in email are actually worms. To be a virus, the code simply has to replicate, it does not need to do a lot of damage, or even spread vary widely.

Worm

In computer terms, worms are really a subset of viruses, but they have the ability to replicate by themselves, they do not require a host file. Simply put, viruses infect hosts, and worms infest systems. Often worms exploit vulnerability in services in network facing services. Such worms can spread very quickly across networks of vulnerable systems, as they do not require any intervention from users to run. However, the commonest types of worms are carried in emails (it is important to note that it is not the email which is infected, but that they carry the worm files). In the case of the email borne worm, the recipient of the email is the vulnerability that is exploited, usually with an enticing subject or message. Usually worms are much easier to remove from a system than viruses, because they do not infect files. Worms often try to add themselves to the startup folder, or modify registry keys to ensure that they are loaded every time the system starts. Again, worms do not necessarily have to do any damage.

II. VULNERABILITY SCANNERS

A. *Nessus*

The Nessus vulnerability scanner provides patch, configuration, and compliance auditing; mobile, malware, and botnet discovery; sensitive data identification and many other features. Nessus and Nessus Perimeter Service™ subscriptions for commercial organizations and enterprises Nessus evaluations for commercial organizations. Nessus Home for personal use in a non-commercial, home network

Operating System: Windows, Mac OS X, OpenBSD, FreeBSD, Solaris, and/or other UNIX variants

B. *OpenVAS*

The Open Vulnerability Assessment System (OpenVAS) is a framework of several services and tools offering a comprehensive and powerful vulnerability scanning and vulnerability management solution. The actual security scanner is accompanied with a daily updated feed of Network Vulnerability Tests (NVTs), over 33,000 in total (as of December 2013). All OpenVAS products are Free Software. Most components are licensed under the GNU General Public License (GNU GPL).

Operating System: Linux, Windows and other operating systems.

C. *Core Impact*

As network security continues to harden, it's no surprise that cyber criminals have shifted their attack techniques to focus on applications and end users. With the release of version 12.5, CORE Impact Pro takes vulnerability assessment and testing far beyond traditional exploitation -- allowing commercial and government organizations to actively and accurately test the security of their network and application infrastructure using the same Advanced Persistent Threat and password-based techniques employed by cyber attackers.

D. *Nexpose*

Nexpose, the vulnerability management software, proactively scans your environment for mis-configurations, vulnerabilities, and malware and provides guidance for mitigating risks. Experience the power of Nexpose vulnerability management solutions by knowing the security risk of your entire IT environment including networks, operating systems, web applications, databases, and virtualization.

Exposing security threats including vulnerabilities, mis-configurations and malware. Prioritizing threats and getting specific remediation guidance for each issue. Integrating with Metasploit to validate security risk in your environment.

Operating System: Windows, Linux

E. *GFI Lan Guard*

Research consistently demonstrates that many of the vulnerabilities cybercriminals exploit can be prevented with updated software patches, and addressing of misconfigured network gear and unauthorized devices on the network. GFI LanGuard scans and detects network vulnerabilities before they are exposed, reducing the time required to patch machines on your network. GFI LanGuard patches Microsoft ®, Mac® OS X®, Linux® and more than 50 third-party operating systems and applications, and deploys both security and non-security patches.

Operating System: Windows Price: Paid

F. QualysGuard

QualysGuard Enterprise is an award-winning cloud security and compliance solution. It helps global businesses simplify IT security operations and lower the cost of compliance. It delivers critical security intelligence on demand and automates the full spectrum of auditing, compliance and protection for Internet perimeter systems, internal networks, and web applications.

Operating System: Windows Price: Paid

G. MBSA

The Microsoft Baseline Security Analyzer provides a streamlined method to identify missing security updates and common security misconfigurations. MBSA 2.3 release adds support for Windows 8.1, Windows 8, Windows Server 2012 R2, and Windows Server 2012. Windows 2000 will no longer be supported with this release.

Operating System: Windows Price: Freeware

H. Retina

With over 10,000 deployments since 1998, Beyond Trust Retina Network Security Scanner is the most sophisticated vulnerability assessment solution on the market. Available as a standalone application or as part of the Retina CS unified vulnerability management platform.

Retina Security Scanner enables you to efficiently identify IT exposures and prioritize remediation enterprise-wide. Retina Network Security Scanner, the industry's most mature and effective vulnerability scanning technology, identifies the vulnerabilities – missing patches, configuration weaknesses and industry best practices - to protect an organization's IT assets.

Operating System: Windows Price: Paid

I. Secunia PSI

Don't let one vulnerable PC open your corporate network up to cyber attacks - Combining private and corporate Patch Management provides a 360° overview of all vulnerability threats

The Secunia Personal Software Inspector (PSI) is a free security tool designed to detect vulnerable and out-dated programs and plug-ins, which expose your PC to attacks. Once installed, the Secunia PSI can help you patch vulnerable programs and stay secure.

Operating System: Windows Price: Freeware

J. Nipper

Nipper (short for Network Infrastructure Parser, previously known as Cisco Parse) audits the security of network devices such as switches, routers, and firewalls. It works by parsing and analyzing device configuration file which the Nipper user must supply. This was an open source tool until its developer (Titania) released a commercial version and tried to hide their old GPL releases (including the GPLv2 version 0.10 source tarball).

Operating System: Windows, Apple MAC OSX, Linux

III. Conclusion

As internet has become a huge part of our daily life, the need of network security has also increased exponentially from the last decade. As more and more users connect to the internet it attracts a lot of criminals. Today, everything is connected to internet from simple shopping to defence secrets as a result there is huge need of network security. Billions of dollars of transactions happens every hour over the internet, this need to be protected at all costs. Even a small unnoticed vulnerability in a network can have disastrous affect, if companies records are leaked, it can put the users data such as their banking details and credit card information at risk, numerous software's such as intrusion detection have been which prevents these attacks, but most of the time it's because of a human error that these attacks occur. Most of the attacks can be easily prevented, by following the rules. As new and more sophisticated attacks occur, researchers across the world find new methods to prevent them. Numerous advancements are being made in the field of network security both in the field of hardware and software, it's a continuous cat and mouse game between network security analyst and crackers and as the demand of internet shows no signs of decreasing it's only going to get a lot harder. In this paper, we tried to bring awareness on the potential malwares and vulnerability scanner tools.

IV. REFERENCES

[1] Daya ,"Network Security: History, Importance, and Future ,"University of Florida Department of Electrical and Computer Engineering , 2013. http://web.mit.edu/~bdaya/www/Network%20Security.pdf

[2] Li CHEN,Web Security : Theory And Applications,School of Software,Sun Yat-sen University, China.

[3] J. E. Canavan, Fundamentals of Network Security, Artech House Telecommunications Library, 2000.

[4] A. R. F. Hamedani, "Network Security Issues, Tools for Testing," School of Information Science, Halmstad University, 2010.

[5] S. A. Khayam, Recent Advances in Intrusion Detection, Proceedings of the 26th Annual Computer Security Applications Conference, Saint-Malo, France, pp. 224-243, 42, 2009

[6] M. M. B. W. Pikoulas J, "Software Agents and Computer Network Security," Napier University, Scotland, UK.

[7] R. E. Mahan, “Introduction to Computer & Network Security,” Washington State University, 2000.

[8] Q. Gu, Peng Liu, “Denial of Service Attacks,” Texas State University, San Marcos.

[9] M. A. Shibli, “MagicNET: Human Immune System & Network Security,” IJCSNS International Journal of Network Security, Vol. .9 No.1, January 2009