PenTest magazine

Brothers in Arms: Pentesting and Incident Detection

Risk-Based Pentesting

Debugging the interception of encrypted traffic

Physical Security: Impact on Overall Security Posture

Offensive Security Automation

Penetration Testing & Incident Response

and more...

02/2017 ISSN: 2084-1117

Managing Editor: Sofiia Sharma

sofiia.sharma@software.com.pl

Proofreaders & Betatesters: Lee McKenzie, Jeff Smith, Avi Benchimol, Hammad Arshed, Bernhard Waldecker, Tom Updegrove

Special thanks to the Betatesters & Proofreaders who helped with this issue. Without their assistance there would not be a PenTest Magazine.

Senior Consultant/Publisher: Pawel Marciniak

CEO: Joanna Kretowicz
joanna.kretowicz@pentestmag.com

DTP: Sofiia Sharma

Publisher: Hakin9 Media Sp.z o.o. SK 02-676 Warsaw, Poland
ul. Postepu 17D
Phone: 1 917 338 3631 www.pentestmag.com

Whilst every effort has been made to ensure the high quality of the magazine, the editors make no warranty, express or implied, concering the results of content usage. All trade marks presented in the magazine were used only for informative purposes.

All rights to trade marks presented in the magazine are reserved by the companies which own them

DISCLAIMER!

The techniques described in our articles may only be used in private, local networks. The editors hold no responsibility for misuse of the presented techniques or consequent data loss.

EDITORIAL NOTE

Dear reader,

We offer to your attention our new issue: ‘Brothers in Arms: Pentesting and Incident Detection’.

In this full of expert opinions issue you will find discussions about the role of penetration testing in the incident response process.

Rapid7 and Trustwave in their articles will explain how crucial the connection between Incident Response and Penetration Testing is, while Kroll will show you practical examples of attack response. We hope you will enjoy these contributions , prepared for you by world-wide corporations.

RUNESEC will describe a simple methodology that was used during the engagement to debug the interception of encrypted traffic between an application and a server.

Apart from corporate contributions, inside you will find another enthusiastic piece from Lior Barash, who will continue his discussion about cyber security autonomy.

Praveen J Vackail and Chris Bullock, who are international security experts, provided articles about incident response, fully based on the real-life, practical experience.

Frederick L. Haggerty, who is a Forensics and Malware Analyst and supports the U.S. Marine Corps’ cyber operations, contributed an interesting piece, in which he discusses current challenges of Incident Response process.

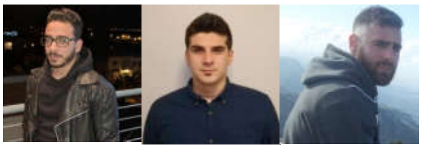
The issue is closed by contributions by Jorge Mario Ochoa and Marcelo Mansur. Jorge will talk about the problem of human factor and the threat is causes for company. Marcelo shared with us the final piece of Ben Chester’s chronicles.

Hope you will enjoy reading this issue,

Yours,

Editorial Team of PenTest Magazine

CONTENTS



CONTENTS

Kroll

Brothers in Arms: How Incident Detection and Pentesting Can Work Together to Improve Outcomes

With **Rapid7**, technology professionals gain the clarity, command, and confidence to safely drive innovation and protect against risk. We make it simple to collect operational data across systems, eliminating blind spots and unlocking the information required to securely develop, operate, and manage today's sophisticated applications and services. Our analytics and science transform your data into key insights so you can quickly predict, deter, detect, and remediate attacks and obstacles to productivity. Armed with Rapid7, technology professionals finally gain the insights needed to safely move their business forward. Rapid7 is trusted by more than 5,800 organizations across over 110 countries, including 37% of the Fortune 1000. To learn more about Rapid7 or get involved in our threat research, visit www.rapid7.com.

Eric Sun as a solutions manager for Rapid7's Incident Detection & Response offerings, works closely with Rapid7's penetration testers and managed SOC to help security teams model their programs after the intruder attack chain. He also brings an understanding of behavior analytics and risk management from his many years in Asia as a professional poker player. Previously, Eric was at custom mobile app developer, Zco Corporation, based in New Hampshire, USA.

Brothers in Arms: How Incident Detection and Pen Testing Can Work Together to Improve Outcomes

Finding gaps in organizations' security programs are table stakes. Defense requires both prevention and detection. Pen testers need to work with incident responders to make sure they're meeting the challenges of today's dynamic threat landscape.

If you were to conduct a poll, most penetration testers would tell you they're constantly forced to work with one arm tied behind their back. Red teamers are always under time constraints — both the time allotted for outside reconnaissance and the speed demanded once inside the network and delivering results.

Regardless of how many arms they may feel they're working with, however, most companies' security teams largely fail to detect pen testers on the network. Response teams don't have the context they need for effective triage and are flooded with false-positive alerts; in the chaos, red teams easily sneak by. Add this to the fact that during incident investigations, response teams often are even further bogged down in the tedious work of retracing user or attacker behavior. And it's these two realities that often prevent responders from detecting and catching intruders whether it's during a company test or a malicious attack.

Let's look at three of the most effective means of compromise attackers use to get in, as well as how pen testers can help incident responders improve their detection.

Method 1: Remote Code Execution on Compromised Endpoints

In response to wide industry adoption of antivirus and anti-malware solutions, pen testers are now getting more out of what's already on the victim's machine. For example, exploiting vulnerabilities in well-known, popular software can enable attackers to run malicious code from the original, legitimate process, such as Notepad.exe or Word.exe. This parasitic technique, also referred to as process hollowing, easily bypasses traditional threat detection that relies on identifying known-bad process hashes.

As an alternative means, both pen testers and real-world attackers can use built-in Windows tools, such as PowerShell, to execute commands on the victim's endpoint. Because this doesn't require outside malware to be successful, detection relies on having visibility into user behavior on the endpoint. For this reason, security teams are implementing Endpoint Detection & Response (EDR) solutions to identify both Remote Code Execution and the behaviors around a compromised user (e.g. privilege escalation, log deletion, lateral movement). The big challenge is identifying the scope of the attack when a single malicious behavior is detected. Were other hosts compromised? Where did the attacker move from there? Pen testers must push clients to answer these tough questions — detecting a single indicator on one or two endpoints doesn't tell the entire story.

Method 2: Using Stolen Credentials to Impersonate Legitimate Users

Whether sourced from separate data breaches, phishing, or malware, stolen credentials continue to show up as the top attacker action in breaches. If a pen tester is provisioned internal access to the network, then they have multiple methods to expand the reach of their influence. For example, they may try horizontal brute-forcing — trying a weak password against every account in Active Directory (Feb2017!, anyone?) If this results in a successful log in, the red teamer can dump the credentials from that endpoint and loot either the password hashes or even the clear-text passwords.

Newer methods include variants of Man-in-the-Middle attacks, such as LLMNR and NBT-NS Poisoning accomplished via tools like Responder. For those not familiar, Responder will listen and acquire user hashes of systems responding to broadcast services (LLMNR, NBT-NS, and mDNS, to be exact). From there, passing the hashes with your tool of choice is relatively easy. Our pen testing teams are, in most cases, able to harvest hashes in a matter of seconds using protocol poisoning. This sort of silent eavesdropper is difficult to detect, making it a valuable and increasingly common attack vector.

Detecting the use of these stolen credentials is equally difficult. In order to detect anomalous user logins, each user’s activity across the many services they use — such as Active Directory, Exchange, cloud services, and more — must be logged, centrally aggregated, and analyzed against baselines of usual behavior. The only legacy class of solutions that accomplished this was Security Information and Event Management (SIEM) tools, but they’ve historically only been stretched to detect such actions by the most advanced teams. This has led to the rise of User Behavior Analytics (UBA) solutions, which perform more advanced analyses of log and/or network data to correlate all activity to the users and assets involved. As companies start to consistently detect the use of stolen credentials, we anticipate a new breed of attacks designed to evade UBA driven detection. However, to get there, pen testers need to first understand UBA as well as they have studied traditional SIEMs and push their clients to use them effectively.

Method 3: Lateral Movement Across the Network

Any attacker with privileged credentials is ready to move to the target machines, or those with data to monetize. This movement from machine to machine is known as lateral movement. It’s used consistently during pen test engagements and is as challenging to detect as the first malicious impersonation. Being able to detect lateral movement early is valuable because it increases the chances that the attacker has not yet reached prized, critical assets. This knowledge also accelerates eradication as both hosts can be considered compromised.

Brothers in Arms: How Incident Detection and Pen Testing Can Work Together to Improve Outcomes

As with the initial use of stolen credentials, SIEM and UBA solutions are now starting to baseline typical machine-to-machine interactions to define what's "normal." If Bob in Marketing suddenly authenticates to the Finance Server with his privileged credential but from an endpoint he has never used before, then the analytics trigger an alert. If pen testers can advance blue teams to detect this level of nuanced lateral movement on an engagement, they are truly improving their clients' security posture.

It's vital for organizations to detect the above three behaviors so penetration testers transition from using them to evade detection to teaching how to detect them as quickly as possible. By integrating red team knowledge and real-world testing experience into your incident response program, pen testers can be as impactful on your detection as they've historically been on prevention and mitigation.

Experience Share about Interconnection of Pentest and Incident Response Process by Chris Bullock

After Chris his 10 year, full-time law enforcement career to part-time in 1996, he moved into a very successful private sector cybersecurity career. Chris became certified as a CISSP, CCFT, CCE, GWAPT and GaCSI Instructor between 2003—2013. He has held several executive security positions in his career across quite a few large, Atlanta based corporation's subsequently building and maturing their cybersecurity programs. Chris combines and utilizes his unique hybrid of experience and training in specialized technologies, executive management and law enforcement to build effective cybersecurity programs and to protect companies' most valuable trade secrets and sensitive customer and employee data. Chris has built these programs from the ground up and has experience across many verticals, including retail, financial, energy, government, gaming and healthcare.

Chris Bullock

Managed the first information security program for the Georgia Lottery Corporation.

Was voted 85th Top Ranking CISO in the United States for 2012 http://execrank.com/2012/08/chief-securityofficers/

Was a speaker at Secure World, FBI Infragard and the CISO Summit.

Has experience managing multimillion-dollar budgets

Seasoned penetration tester
Computer forensics/e-discovery specialist
Incident response specialist

Introduction

As cyber security professionals, we have become extremely familiar with the devout need to test our systems for security vulnerability through technical ethical hacking techniques. Basically, we want to know where our weaknesses are before the bad guys find them, so we hack ourselves. We also know that to be prudent in our practice of the tradecraft we must perform regular incident response tabletops to test our ability to respond to a cyber-attack should one occur. These two areas of cyber security are the two basic cyber security pillars known as:

- The red team
- The blue team

This reference is from a military term wherein the red team is the team that attacks and the blue team is the team that defends, derived from capture the flag exercises. These teams can also be thought of as the penetration testing team and the incident response team of an organization.

As a veteran CISO, I have always created the personnel, process, and technology structures of my programs with the implementation of a risk validation team (red team) and an incident response team (blue team). This has become commonplace in the industry amongst CISOs globally. Where I have seen the waste and error in the industry is through the failure of CISOs in not using one to fortify the other, particularly when

Chris Bullock Experience Share about Interconnection of Pentest and Incident Response Process

performing their regular penetration testing.

This can lead to three major failures:

- Failure to locate deficiencies with detection
- Failure to locate deficiencies with logging
- Failure to maximize response efficiency

Any credible CISO fully understands the value of regular penetration testing and realizes it must minimally be performed on an annual basis if not more frequently. What I found many CISOs do not realize, is they should be getting more bang for their buck, killing two birds with one stone or any other relevant slang phrase you can imagine that belongs here. What this means is we should use our regular penetration testing exercises to test our incident response program and not doing so can lead to those three primary failures which I will expound upon starting with the failure to locate deficiencies in our detection capabilities.

Detection

Detection is the key to responding quickly and appropriately to any cyber security attack because it is the first step. Detection is also the shortest step compared to understanding and figuring out how to address the incident, which will take far longer (Ponemon, 2014). If your detection capabilities are not sufficient, then the rest of your incident response program might as well not exist. The best way to ensure you are indeed detecting various attacks is by having your blue team verify they are seeing evidence of the penetration team's attack methods during your regular penetration testing. Even if the penetration testing team is a top-notch team using slow and go attack methods, there should still be some evidence available through your detection capabilities which reflects what was taking place. This can also help your team know exactly what a "needle in a haystack" may look like.

In other words, by coordinating with the red team, the blue team can lay their eyes on the minuscule logging evidence created during a slow and go attack and become familiar with what it may look like. This helps log entries which may not otherwise have stood out to them, begin to stand out, particularly since they knew an attack was in progress as part of participating alongside of the red team during the penetration testing. You can capitalize on your penetration testing expense by doing these tests in parallel, not only testing your fortification but also your response and ability to investigate the attack.

An example I recall is with a penetration test I elicited from one of my regular testing vendors wherein they attempted to run an exploit in memory to avoid A/V and malware tool detection. The test was through an internal attack vector so they were coming from our internal network. We were using one of

Offensive Security Automation

for the greater good Part II

Lior Barash

Lior has 16 years of experience in the CyberSecurity domain, doing offense and defense both as a researcher and as a hands-on guy. He has been teaching and researching methodologies for about 12 years at academy institutes and professional schools. Lior has been practicing different realms in the cyber security world such as Systems design and architecture, Systems hardening, Systems security assessments, System exploitation, Infrastructure systems & Security systems development, Threat modeling and general Risk assessment. He has been providing services to a large verity of sectors such as Gov & HLS, Medical, Telco and IP rich startups.

Lior is the founder and CTO of attollo and the founder of Attofensive, an offensive security solution startup.

Being able to automate ‘offensive security’, I would argue it is pro bably one of the most important tasks at hand these days; not to say that automating ‘defensive security’ is less important or might have lesser implications, though it is, from my perspective, not only the darkest portion of our cyber space map but also the most dangerous one, if we were to disregard the dangers from a false sense of a strong security posture.

We need to define two things before we can begin this journey:

- Automation.
- Offensive security.

Let’s consider automation as the unattended occurrence of a predefined task that can be triggered either manually or by an occurrence of another event, and once the process started, there will be no need for any sort of intervention until the next closest break point in which the operation might have came to its end or another process/subprocess is supposed to start. This might be a portion of a larger set of instructions or the complete set; either way, the rules apply.

Offensive security, for the sake of this subject, would be any action that would result in a manner not expected by the user or designed by the system architect, as long as it produces a non expected/designed outcome that also has a value. The value should be either scaled by the importance to, and impact on, the user or by the importance to the attacker and the impact and leverage it will bring with it.

Before we begin with a short review of some open source frameworks and tools aimed at automating offensive security at the subdomain of penetration testing, let's look at some basic automation concepts; for the sake of this example, I'll assume you're familiar with the ARP protocol and that each network device, once connected to a standard Ethernet network with a standard TCP/IP stack, would send and receive ARP information, including, but not limited to, its own MAC and IP addresses and at least the gateway MAC and IP information. If you were to analyse this information directly by decoding network traffic flowing over the network interface hardware and software, it would probably take much more time than you'd like to invest in the process; so you'd probably choose to use an automation tool, such as the 'arp' tool available basically on any OS, and ask it to read the ARP table for you and print it out nicely and clearly. This is probably the most basic automation we're so used to that we don't even remember it's an automation, we just call it a 'tool' or a 'command'.

A few steps forward and now let's examine one of the probably most common tools, NMAP. What NMAP can do today is much more than what I would like to discuss at the moment so let's focus on a single flag it offers, which is the '-sn' option; if you'd run the tool NMAP with the flag `'-sn'`, you would actually make it perform a ping scan to detect online hosts that might respond to ping requests, while this is not much different than actually using the ping command to ping hosts on the network you're on and assess by the output whether or not they are responsive and thus 'alive'. Another nice option NMAP supports is that you could specify a range of IP addresses for it to scan; the complete command would look something like this `'nmap -sn 192.168.0.0/24'` and would not only test to see if a host is responsive but will test to see which host within a range is. Thank you automation.

Another advance towards more complex automations would be a tool such as LiveHosts from a few years ago, though this specific tool has much less functionality than the previous one we talked about. It is built in a manner that is important for this point; this tool would run with an argument defining an IP range and would return a list of 'live' hosts within the range specified. What's important to us at this point is that this tool is no more than a shell script calling NMAP to execute a single command, or a set of commands, and evaluate the NMAP output in order to print the results back to the user. This is important because it's an automation of an automation and that is where things start to get a bit more interesting in terms of what we can expect.

Incident Response and the Role of Penetration Testing

Trustwave helps businesses fight cybercrime, protect data and reduce security risk. With cloud and managed security services, integrated technologies and a team of security experts, ethical hackers and researchers, Trustwave enables businesses to transform the way they manage their information security and compliance programs. More than three million businesses are enrolled in the Trustwave TrustKeeper® cloud platform, through which Trustwave delivers automated, efficient and cost-effective threat, vulnerability and compliance management. Trustwave is headquartered in Chicago, with customers in 96 countries.

For more informtion: https://www.trustwave.com

Trustwave®
Smart security on demand

Will Harmon is a military veteran with nearly 20 years of experience in the cyber security space. He has extensive experience in both the public and private sector performing penetration testing, vulnerability management, intrusion detection, incident response, and application development. He currently serves as the Trustwave SpiderLabs Government Solutions practice lead. Prior to Trustwave Government Solutions, he held various senior leader positions at the Department of Homeland Security, Pentagon Federal Credit Union, and Verizon Communications.

He maintains active CISSP, CEH, and GCFE certifications and holds an MBA from the Darden School of Business at the University of Virginia, a MS in Information Systems Technology from The George Washington University, and a BGS in Computer Information Systems Management from Jacksonville University.

James Antonakos is an Incident Response Consultant for the SpiderLabs team at Trustwave, where his work involves computer forensics in PCI investigations, malware research, security analysis, and conference presentations. James is passionate about all things Information Security, especially things related to PCI, IT security auditing, computer forensics, eDiscovery, and malware analysis.

Prior to Trustwave, James was a Forensic Investigator at WhiteHat Forensics, as well as a fellow at the National Cybersecurity Institute (NCI), in which he advised the NCI on current cybersecurity trends and issues.

Incident Response and the Role of Penetration Testing

Introduction

Cybersecurity threats continue to increase quicker than organizations can implement measures against them. Attacks have grown significantly in complexity, rendering the majority of “off the shelf” detection solutions, such as commercial antivirus programs, ineffective. It is estimated that over one million new malware variants are released every day. At that pace, it’s inevitable that a compromise will occur and organizations need to continually ensure the time between compromise, incident detection, and incident containment, is minimized as much as possible. Penetration testing is an excellent capability to use to add value to the incident response process.

Penetration testing is a process in which the vulnerabilities of an organization are probed for weakness. These penetration tests are typically used by organizations to assess the security of systems and applications.

Areas tested include:

- The network (both outside access as well as inside access) and network devices, such as routers and switches.
- The client and server computers and their applications.
- Security policies and procedures.
- The security awareness of the employees.

A penetration test should not damage or compromise a network or system but instead find ways they could be damaged or compromised.

Why Pentest?

Penetration testing is one component of a security audit or risk assessment. Penetration testing is also a requirement for certain compliance standards, such as PCI, and must be performed at specific intervals during the year.

The findings of a penetration test are used to strengthen the security posture of the organization by addressing the discovered weaknesses. This is accomplished by adding or enhancing controls, creating or revising security policies and procedures, and improving security awareness training for all employees.

Subject: Don't Waste Your Time and Money If You're Not Going to Test It!

Frederick L. Haggerty

Frederick Haggerty is a Forensics and Malware Analyst currently supporting the U.S. Marine Corps' cyber operations. He routinely performs digital forensic examinations and malware analyses in response to network intrusions and Command investigations. With a career in Information Technology spanning over 18 years, his background as a Software Engineer developing mission critical systems has granted him the technical knowledge and insight needed to perform thorough examinations of computer information systems, personal computers, servers, and other digital media.

Digital forensics, malware and reverse engineering, incident response, and data recovery.

Certified Information Systems Security Professional (CISSP)
GIAC
Certified Forensic Analyst (GCFA)
Computer Hacking Forensic Investigator (CHFI)
Qualified/Forensic Expert (Q/FE)
Certified Data Recovery Expert (CDRE)

Over the last several years, malicious computer attacks have intensified for both individuals and businesses alike — becoming more common, lasting longer, causing more permanent damage to the target systems, and costing businesses millions of dollars each year. These attacks are shutting down business computer systems for hours or even days, and sometimes longer. Malicious attacks can range from automated or scripted programs that scan a network for vulnerable hosts or devices to an experienced attacker trying to penetrate a network and install malicious software, such as a Trojans, rootkits, key loggers, and data encryption software, such as ransomware.

Whether personal or business related, information has become increasingly valuable to criminals. Regardless of where the information is being stored, cybercriminals target this valuable information and attempt to steal it so they can use it for fraudulent activities such as identity theft and credit card fraud or to ruin or severely impact the reputation of the victim. Computer crimes pose new challenges for investigators, such as law enforcement and incident response teams, because of their speed, anonymity, and complexity.

In this new age of cyber related attacks, there are plenty of media reports that highlight the latest damaging and embarrassing data breach that paints the picture that cyber defenders are failing or having a difficult time protecting their expanding threat landscape.

Physical Security and its Impact on the Overall Security Posture of an Organization

When not performing Incident Response, Network Monitoring, Forensics, Data Recovery and compliance I enjoy learning more each day on my life's passion-Cyber Security, training, teaching, traveling with my family and outdoor activities. You can reach me on LinkedIn.

Davide Capote

One often overlooked aspect of an overall robust, well architected, mature security program is the physical security posture of the organization. In fact, physical security is often an easy target for Hackers and Pentesters.

In this article we'll explore some of the advantages of having strong physical security, how not having it can lead to a breach, and what to look for when testing for physical security.

First of all, why is this an issue in the first place? I have done consulting for numerous organizations, from small, under 100 user firms, to global, Fortune 500 firms with 200K plus users, and while Cyber Security has a large presence in the minds of the executives, especially at the larger firms, few take into account, in a systematic and well thought out way, how their physical security impacts the overall cybersecurity posture of the organization.

There are three main advantages to having a strong Physical Security plan; first, it strengthens the overall security posture of an organization, secondly, it's a deterrent for cybercriminals or others wishing to harm an organization, finally, it's a type of control that will impact your other controls in a security program. Let's talk about each of these in detail. It's all about defense in depth or the layered security model. Let's dive in.

Having a strong Physical Security plan strengthens the overall security design of your organization. Physical security is often the entry point into a company. By locking down the physical access

Brothers in Arms

Debugging the Interception of Encrypted Traffic

RUNEsec

RUNESEC is a Cyprus company that offers OFFENSIVE Information Security Assessment Services, formed by a small team of highly-skilled individuals who share a strong passion for Computer Security. We strive to provide an uncompromising quality of work through our pursuit of knowledge and desire to hone our skills. Our combined experience in providing Information Security assessment services includes clients such as Government agencies (local and foreign), the biggest Banks and largest Telecommunications providers in Cyprus, Payment Gateway providers, Forex companies, Insurance agencies, Oil & Gas multinationals and global Construction companies.

WEBSITE: https://www.runesec.com EMAIL: info@runesec.com **LinkedIn:** https://www.linkedin.com/company/runesec

TELEPHONE: +357-22262653 **PGP:** Fingerprint: 05CA 12FF 9336 3AA0 B7D9 7AEA A4E2 384D 3841 71EF

Nicolas Markitanis is a Penetration Tester professional at RUNESEC, a Cypriot company specializing in offensive Information Security Assessment services. Previously, Nicolas worked as an Information Security Engineer/Researcher for a cyber security firm. He graduated with honors from Northumbria University at Newcastle with a degree in Computer Science and a masters degree in Cyber Security from De Montfort University in Leicester. Nicolas is currently in the process of starting his PhD. He is interested in mobile application security and likes to dabble in a little bit of everything, especially sciences and books.

Marios Nicolaides is currently working as a Penetration Tester at RUNESEC, a Cypriot company specializing in offensive Information Security Assessment services Previously, Marios worked as an Information Security Specialist at KPMG Cyprus and Westpoint LTD (UK). Marios holds a BSc Computer Science degree from Northumbria University and an MSc degree in Cyber Security from the University of York. He is passionate about web application security and likes to spend his free time mastering his backgammon skills.

Simon Loizides is a Pentester at RUNESEC, a Cypriot company specializing in offensive Information Security Assessment services. Previously, Simon worked as a Penetration Tester for KPMG Cyprus. He graduated with a BSc (Hons.) in Computer Science from King's College London. He is interested in post-exploitation, and likes to climb trees when he can.

Debugging the Interception of Encrypted Traffic

Introduction

We were recently contacted to test out an online, multi-player game, where we needed to be able to proxy the encrypted traffic sent from the game client to the server. We were not aware of the underlying protocol beforehand, only that the communication took place over TLS.

The purpose of this article is to describe a simple methodology we used during this engagement to debug the interception of encrypted traffic between an application and a server, where the interception is not simply a case of installing any self-signed certificate in the trust store of the browser or operating system.

This article is targeted towards junior pentesters and is useful when testing thick clients that handle their own certificate verification, but where SSL pinning is not implemented (out of the scope of this article).

Approach

The first thing we needed to do was see what kind of traffic was being sent between the client and server. Our initial setup was as follows:

- Game client running on Windows VM
- Host OS used for testing (Linux)

Step 1 – Gain an initial understanding of the traffic

By running Wireshark and firing up the game client, we were able to capture traffic and gain an indication of what protocols were being used for communication. It was at this point that we observed the fact that Transport Layer Security (TLS) was being utilized to encrypt communications. We also observed the fact that the destination port on the game server was 443/tcp hinting at the possibility that the underlying protocol could be HTTP, but at this point this was only an assumption.

Risk-Based Pen-Testing as an Enhancer of Cyber-Security Incident Management Capability

Praveen Joseph Vackayil

https://www.linkedin.com/in/v

A former PCI QSA, Praveen brings experience from more than 40 audits conducted for organizations spread across 3 continents.

Praveen is a CISSP, CPISI, ISO 27001 LA and ISO 31000 LA.

Praveen is an information security professional with focus on Compliance and Risk Management. Praveen was behind the Middle East's first e-commerce certification in PCI DSS. He was part of a team that developed the world's first PCI Risk Assessment tool. Praveen is also a seasoned trainer and has trained more than 1800 professionals on various security subjects. He is a regular speaker at security conferences. He is also a regular contributor at security journals. This is Praveen's third publication at PenTest Magazine. He holds a Masters in Information Systems and Management from Warwick University, UK and a Bachelors in Electronics and Communications Engineering from Anna University, India.

Introduction

2017 promises to be a very interesting year in cyber-security. If ‘ransomware’ was a buzzword in 2016, cybersecurity experts may expect to witness dronejacking and BEC Attacks as the emergent challenges of 2017. Whilst threats are rapidly taking over new and innovative forms, it appears that organizations are still grappling with the realities of implementing a mature and highly efficient cyber-security organization.

Recent incidents, such as the DYN Attack, the Bangladesh Bank attack and the Ukraine power-grid shut down, indicate a trend of substantial targeting and extreme complexity in cyber-attacks. Corporations are recognizing the need for a robust incident detection and management capability, and are fortifying their borders with increased spending on cyber security incident management. VAPT teams, SIEM solutions, forensic investigation tools, etc. are deployed to augment overall cyber security incident response capability. When faced with a real incident, however, challenges continue to persist with regard to achieving exceptional degrees of performance.

To be highly effective, a cybersecurity incident response team must:

- be quick to detect attacks
- possess the relevant subject matter expertise to analyze the attack.

- be agile enough to rapidly design and implement steps to contain, remediate and recover from the incident.

In today’s context, however, these continue to remain rather utopian ideas, far from the realities of operational inefficiencies and domain knowledge vacuums plaguing organizations.

The purpose of this article is to explore how pen-testing, with a risk-based approach applied to it, can be used to overcome these process inefficiencies and boost the overall capability of organizations’ incident management capabilities.

Risk-Based “Anything”

Risk Assessment has gained recognition in recent years as a tool to accurately evaluate an organization’s security posture. Risk assessment helps to prioritize the organization’s assets, then capture and articulate threats and vulnerabilities pertinent to those assets. A good risk assessment enables well-informed risk management decisions. Security professionals have, particularly within the last five years, recognized the value of a risk-based approach to many security endeavors. Classic examples are risk-based audits, risk-based authentication, risk-based network monitoring, etc. Quite unsurprisingly, pen-testing has been no stranger to this trend. Literature abounds on risk-based approaches to pen-testing. But can applying risk as the driving element of the entire pen-test approach offer any tangible benefits? Can these benefits, if they exist, be exploited in other areas of the security organization? Let us try and find out.

Deriving the Key Facets of a Risk-Based Pen-Testing Approach

It is of value to understand, at least strategically, the key concepts of Risk and derive, thereafter, the key facets of a Risk-Based Pen-Test approach.

Risk Assessment

Scope, Assets, Threats and Vulnerabilities are the founding elements of a formal risk assessment. Scoping is the first step and defines the boundaries of the environment being assessed. Scope can be a set of teams (people), a specific business unit (processes), a specific technological environment (technology) and even physical premises. For instance, scope can consist of a team of network admins, the finance department of a company, an individual network segment defined behind a public facing firewall, a particular floor within an office building, etc.