PenTest magazine

Vol.1 No.2
Issue 02/2011(02) June

PENTESTING SERVICES

WHAT SHOULD YOU LOOK FOR?

WILD HACKING – ATTACKING WITH NO-RULES

CROSS SITE REQUEST FORGERY

SECURE WINDOWS IMPLEMENTATIONS

PenTest magazine

TEAM

Editor: Sebastian Bula
sebastian.bula@software.com.pl

Proofreaders: Jonathan Edwards, Michael Munt,
Edward Werzyn Jr

Betatesters: Daniel Cialdella, Ankit Prateek, Daniel Wood, Santosh Kumar Rana, Scott Christie, Aby Rao, Scott Christie, Aidan Carty, Clancey McNeal

Senior Consultant/Publisher: Paweł Marciniak

CEO: Ewa Dudzic
ewa.dudzic@software.com.pl

Art Director: Ireneusz Pogroszewski
ireneusz.pogroszewski@software.com.pl
DTP: Ireneusz Pogroszewski

Production Director: Andrzej Kuca
andrzej.kuca@software.com.pl

Marketing Director: Sebastian Bula
sebastian.bula@software.com.pl

Publisher: Software Press Sp. z o.o. SK
02-682 Warszawa, ul. Bokserska 1
Phone: 1 917 338 3631
www.hakin9.org/en

Whilst every effort has been made to ensure the high quality of the magazine, the editors make no warranty, express or implied, concerning 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.
To create graphs and diagrams we used smartdraw.com program by SmartDraw

Mathematical formulas created by Design Science MathType™

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.

***Dear Readers**,*
The second issue of our magazine is devoted both to pentesters and those, who would like to benefit from their services. Pentesting is still black (hat) magic to some and it is our ambition to popularize it in the way it will be a common practice for every single enterprise, not only for those bold enough to let strangers through their kitchen door.

Thus, the main question in this issue – apart from the usual how – is why: why to pentest. If you like straightforward explanation through a series of real-world examples dressed in digestible metaphors, take a look at David Small's Why Would You Want a Pentest – check if your IT castle is safe from hacking armies attempting at breaching the walls and stealing from it. Then you can go straight to the pentesting supermarket with Bill Mathew's to-buy list: "What Should You Look For". As Bill warns, all of the products you will find in this shop come with no guarantee (whatsoever), so it might be worthwhile to check why the purchase should be done with extreme care. Iftach Ian Amit will tell you when your pentest is meaningless and how to prevent this meaninglessness, Rishi Narang will provide you with some good statistics on vulnerabilities (with quite a rethorical question – is it worth to pentest?), and Chad Jaenke will share with you his vision on how to add value to pentesting services.

These articles are of course accompanied by a portion of technical how-to writings: don't miss the part on secure windows implementations, or the CSRF.

Enjoy your reading
Sebastian Buła
& Penetration Test Magazine Team

COMMENT

We are open for suggestions and discussion. Don't hesitate to comment on the articles which you've read in this issue. Share your opinion on the subject matter brought up, back up or confront the point of view of the author. The best comments will be published on our site and in our next issue.

FOCUS

04 **Why Would You Want a Pentest?**
by David Small
To get a physical checkup, you go to your doctor and a laboratory. To get a computer security checkup, one part is penetration testing, usually shortened to pentest, which is in the title of this magazine. You do it for the exact same reason you go in each year for a physical; because you (and, frankly, I) want to catch any security problems in your computer systems as early as possible.

10 **What Should You Look For?**
by Bill Mathews
Why would you ever need a penetration test? The answer, per usual, depends on your perspective and needs. Most companies that have sensitive data in their enterprises should look at getting some form of penetration testing. Why do I say, some form? Simply put, there are as many definitions of penetration testing as there are fish in the ocean. Seriously, sometimes I think we make this stuff up as we go along. If you're looking at hiring out a third party to do your penetration test (and you should, reasons later), I think it would be helpful to go through some of the definitions as I see them in the industry.

16 **Your Pentest Is Meaningless**
by Iftach Ian Amit
Traditional penetration testing delivers results that are –for the most part– unusable. Here we take a look at the flaws of the traditional approach, and consider ways in which we can improve the presentation of the results.

20 **Penetration Testing – Is It a Worth?**
by Rishi Narang
Exponential growth in vulnerabilities and ease in exploitation with automated kits demands the security to be on the tows. Every time the topic of information security is discussed, it has to be related to three of its key pillars – Protection, Detection and Response. These pillars, if strengthened well, can lower the chances of any known vulnerabilities be exploited in your network. To keep the security on its toes and its top notch maintenance, a client has to consider a penetration testing engagement to verify the security controls and validate response timings. So, what is penetration testing all about?

26 **Selling Penetration Testing Services: Two Words, Adding Value**
by Chad Jaenke
As an external pentester, you need to recognize the constraints that many organizations are working under and tailor your services to fit their needs. Yield better results in selling pentesting services by thinking outside of the box and break free from the traditional thoughts of pentesting. Exploiting a system and reporting the findings should no longer be the sole purpose of a pentester.

HOW-TO

28 **Post Exploitation Using Metasploit Pivot & Port Forward**
by David J. Dodd
A very nice feature in metasploit is the ability to pivot through a meterpreter session to the network on the other side. This tutorial walks you through how this is done once you have a meterpreter session on a foreign box.

NETWORK SECURITY

34 **Secure Windows Implementations**
by Dhananjay D. Garg
Nothing is unbreakable, but we sure can make it hard for others to break into our systems. Back in 2001, it was declared by some that Microsoft Windows XP was Microsoft's most secure operating system ever. Although this has been proved wrong by many security experts, Microsoft Windows XP still remains the most used operating system worldwide. Local vulnerability assessments show that a properly configured XP can thwart many unsolicited attacks. Many Windows systems can be compromised due to poor administration.

STANDARDS

42 **Wild Hacking – Attacking With No-Rules**
by Christian Navarrete
Each Penetration test is different, and is tailored to the customer size, their infrastructure, running systems and applications and sometimes specific hardware. So, what would happen if our current resources in terms of methodologies doesn't fit, or even mention, how to test a complex infrastructure or an embedded device? This situation is where you are first realizing the importance of leaving the rules behind!

VULNERABILITIES

46 **Cross Site Request Forgery (CSRF)**
by Sudhanshu Chauhan
Cross site request forgery or session riding is a kind of attack which forces an end user to execute unwanted malicious actions without their knowledge or intent on web application in which they are currently authenticated. It basically exploits the trust a website has in user's web browser.

Why Would You Want A Pentest?

For: Non Technical People

Most of the fundamental ideas of science are essentially simple, and may, as a rule, be expressed in a language comprehensible to everyone (Albert Einstein). I'd like to promise you that in this article, I won't drown you in computer terminology. I like Albert Einstein's view on science and I'll write this article in as plain language as possible.

Plain Talk

To start off, let me ask you this:

How's your health?

Hopefully you can reply to me, *Oh, pretty good*.

And then I'll ask you one more question:

How do you know?

You'll probably tell me that you went in for a *yearly physical health check*, a doctor checked your reflexes, eyes, ears, heart, and so forth. Then you went to a laboratory which drew your blood and checked various indicators; your cholesterol levels were in a healthy range, your blood work didn't show any signs of problems (for example, your blood sugars were normal, so you're not developing diabetes).

So, essentially, you know your health is *pretty good* because you went in for medical *testing*. *You would not know your health is good without these tests*.

There's also a time factor here. You go to a yearly physical to help catch any problems *early*, because a lot of problems can be treated, but they're more effectively treated if they're found *early*. For example, the melanoma on my shoulder (translation: a cancer) was caught early, and removed completely before it began to spread everywhere, or I definitely wouldn't have written this article.

So, as you can imagine, I'm a big believer in checkups. To get a physical checkup, you go to your doctor and a laboratory. To get a computer security checkup, one part is *penetration testing*, usually shortened to *pentest*, which is in the title of this magazine. You do it for the *exact same reason* you go in each year for a physical; because you (and, frankly, I) want to catch any security problems in your computer systems as *early* as possible.

Everyone with a computer worries about someone on the Internet getting into their computer systems and wreaking havoc. And we worry for very good reasons!

There's a up-side to the Internet – I'll just mention how Google and Wikipedia are so very good – but there's also a down-side – viruses and related junk, and people breaking into someone else's computers.

Your Computers: Castles

A useful analogy is to think of your computer systems as a castle. Its walls are made of rocks mortared together; its gate is made of thick wood; you get the idea. The rocks are numbered and called *ports*.

If your systems are connected to the Internet, then, in effect, you've opened some ways from the inside of your castle to the Internet outside. This is usually necessary for e-commerce, but can be very, very tricky for system security. As a quick for-example, rock #80 is where sending or receiving a web page takes place.

There are people out there who will *very* persistently pry at the rocks of your castle's wall.

Here's where the odds are stacked against us: *If* they can pry *just one* rock loose, then they can get inside to

Penetration Testing

What Should You Look For?

So you're in the market for penetration testing? Do you know what you're buying? Do you know how to buy it? I will attempt to define the types of penetration testers out there along with a sound Request for Proposal process for penetration testing. Be careful what you buy, you only get what you ask for.

So right off the top, a disclaimer: I earned a living for many years as a penetration tester and now run the penetration testing team at Hurricane Labs. Now that I have that out of the way, here we go.

Why would you ever need a penetration test? The answer, per usual, depends on your perspective and needs. Most companies that have sensitive data in their enterprises should look at getting some form of penetration testing. Why do I say, "some form"? Simply put, there are as many definitions of penetration testing as there are fish in the ocean. Seriously, sometimes I think we make this stuff up as we go along. If you're looking at hiring out a third party to do your penetration test (and you should, reasons later), I think it would be helpful to go through some of the definitions as I see them in the industry. This list should then help you form some intelligent questions to ask the companies you are considering. After the definitions we'll review some questions you should include in your RFP to help weed out some of the pretenders.

Definition Number 1 (N1)

Let's scan them and hope they never actually get attacked.

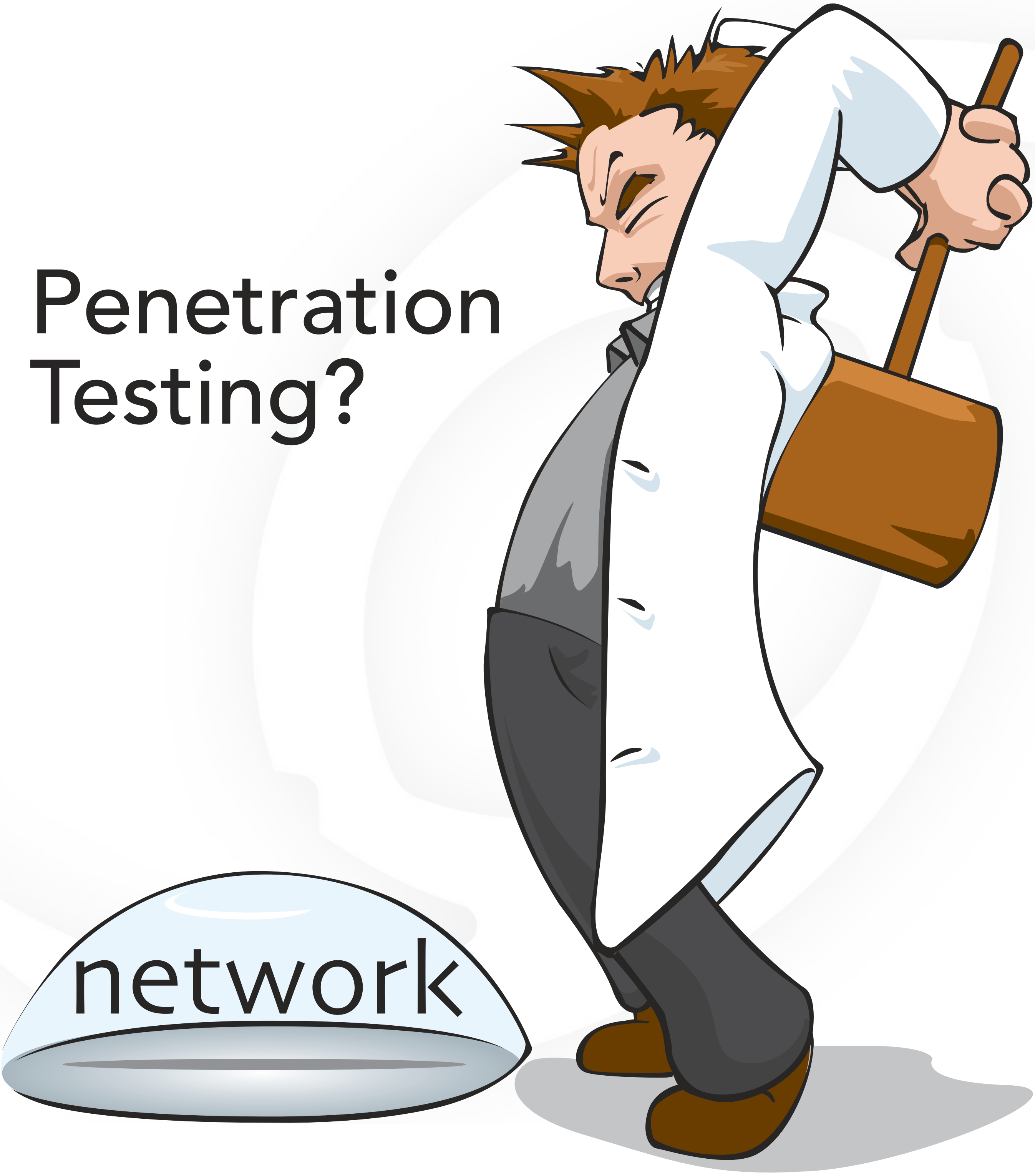
This is my least favorite of the varieties out there, mainly because I thought this breed of service was long dead. Sadly I still see it out there almost every week or so. These are the guys who point Qualys, Nessus, or worse, turned all the way up, at your network, press submit and watch the fireworks. Typically they do no tuning of the scan and just let it go. This is dangerous on so many levels, and this sort of thing can quickly bring down your whole network. You'll recognize them because their salespeople will say all the right things but their slicked back hair will give it away. Ask them about their manual testing methods and soon you'll realize they have none. By the way, these are the sorts that will give you a clean bill of health in a day or so and offer no real opinion on your applications or network. Avoid this sort of tester at all costs.

Definition Number 2 (N2)

The Old Smash and Grab

I wish I could take credit for this but it was coined by a colleague of mine (*Rick Deacon @rickdeaconx*). Basically these are the guys who come in and simply destroy your network and applications with no regard for your business or money lost. They are also scanner heavy and generally are in love with BackTrack and Metasploit but only know enough to break things and usually offer no recommendation on fixing them. These are also the types that will drop a 120-page report (single-spaced) on your desk and disappear. They are generally only slightly better than number one in that they employ some tools that take slightly more skill than just pressing

Auditor Discount
Pacifier Price Reduction
Rich Kid Rollout
Smash and Grab Deal


network

Your Pentest Is Meaningless

– How To Turn Tech-speak Into Value

Traditional penetration testing delivers results that are –for the most part– unusable. Here we take a look at the flaws of the traditional approach, and consider ways in which we can improve the presentation of the results.

First, let's take a look at the Wikipedia definition of penetration testing: *A penetration test is a method of evaluating the security of a computer system or network by simulating an attack from a malicious source, known as a Black Hat Hacker, or Cracker. The process involves an active analysis of the system for any potential vulnerabilities that could result from poor or improper system configuration, both known and unknown hardware or software flaws, or operational weaknesses in process or technical countermeasures. This analysis is carried out from the position of a potential attacker and can involve active exploitation of security vulnerabilities. Any security issues that are found will be presented to the system owner, together with an assessment of their impact, and often with a proposal for mitigation or a technical solution. The intent of a penetration test is to determine the feasibility of an attack and the amount of business impact of a successful exploit, if discovered*.

Putting on our business hat for a moment, what does this presentation of results actually mean for the corporate employee who has to make their business more secure and less prone to information breaches? That's right; not much. Unfortunately, this is a question rarely asked by those performing penetration testing.

Your technology will bow to my skillz.

Often, penetration testers come with a self-assured attitude that they're going to be able to find fault and bend and break any technology. But actually, this way of thinking misses the point. I can name countless customers where technology isn't the issue at all. I could pop shells at their boxes all day, and it still wouldn't make any difference to their business. It's really not about the technology, but rather about what the technology DOES for the business. Penetration testing is not an exercise in satisfying our need to show how great we can handle the technical challenge to bypass a certain security mechanism, or to break a certain technology… first and foremost it's about identifying what the relevance of such an exercise is for the customer.

High, medium, low. That'll get you on your way to figuring out what to do with these findings.

Another problem is the use of broad categorizing in the results. Most penetration tests categorize their findings using *high, medium, low* scales, which are completely useless to the client. They are also rather arbitrary, for example, do you always classify an XSS as medium or low? How about a SQL Injection–always medium or high? Root shell–always high or critical?

And without context or an understanding of what the specific system you *own* does to the business AS A BUSINESS, the findings cannot be classified. For example, fixing a remote shell could be completely meaningless to the security posture, its impact on reducing the risk of being compromised in terms of valuable information being stolen, availability of services

Your Pentest Is Meaningless – Q&A

Ankit Prateek: The article states that *penetration testing is not an exercise in satisfying our need to show how great we can handle the technical challenge to bypass a certain security mechanism, or to break acertain technology*. In my opinion, pentesting should rather be such an exercise, how else can one think and work *beyond and out-of-the box*?

Iftach Ian Amit: I personally do believe that pentesting is not JUST an exercise in breaking technologies. It's also an exercise in breaking businesses... This is exactly where the *thinking outside the box* comes in – not just in the technological factor, but also on the human, process, physical and other factors that affect a business operation.

AP: Another interesting fact was taking care of the budget of the company. Is someone actually thinking about saving money on maintenance?

IIA: Not necessarily – if that budget can be used to close gaps that could reduce the risk of that company in rates that are much higher than the risk that would be assumed by keeping a maintenance contract for some *useless* box...

The point is to be able to articulate RISK to the company, not just technical vulnerabilities. Once RISK is the question, we can look at the financial impact of such risk (which we can't do for technical vulnerabilities), and adjust the company spending on security appropriately (i.e. – in ways that reduce risk the most).

AP: I totally agree that a pentester is expected to *provide actionable advice rather than merely technical advice* in his *presentation that should not be just shelved*, and that it should be *the best advice*. Concerning the budget, are you suggesting that after the testing the pentester should propose various levels of the *solution*, from which the best *in budget* choice can be made? What will it be like?

IIA: Actually my suggestion is that the pentester will take into account the damage that each of the findings will cause, take into account the additional business related costs associated with such incident, and then factor in the cost of fixing the problem, or placing additional controls to minimize such damage. This should all be in light of the potential cost of such incident, and compared to the cost of fixing or placing controls.

AP: A pentester, no doubt, must be aware of the various ways of *doing away the vulnerability*, so with the *improved presentation* he can recommend the solutions too. But isn't it the work of the *white collar and tie-people* to calculate the *cost-effectiveness of the advice*? It might be a distraction for a pentester, doing all that management work.

IIA: I'm not saying that pentesters should start selling security solutions. On the other hand, I do claim that pentesters and consultants should provide a service that is not merely technical, and is custom tailored to the business. Otherwise, the business could have just licensed out some scanning software and kept running it forever. For a pentester the exercise of calculations is reasonable in my mind, as the pentesting should be done for each business according to the specific needs and environment. Hence – the pentester is already in a position to custom-present the findings with the business' *numbers* in place. The solutions part can be as simple as *you should spend no more than $X to fix this issue, because the worst case scenario will have an impact of $(1.2*X)* …

AP: As I see it, you might be asking too much from a pentester and still wanting him to fit in the budget. Well, every Company is going to love that.

IIA: Here we disagree – I'm not asking the pentester to „fit into the budget". I'm asking it to acknowledge that companies do not have unlimited budgets, and as such they need to provide actionable advice rather than merely technical advice.

Penetration Testing – Is It A Worth?

Vulnerabilities are increasing by leaps and bounds and any industry – technical or non-technical has to grow its security in sync or else, it is highly vulnerable and lucrative target. There is news of data loss, breaches every now and then.

A rough estimate of the growth of vulnerabilities (as reported) over last decade (1995-2008) is shown in Figure 1. This accounts to vulnerabilities as reported, wherein there are hundreds of active (non-reported or un-patched) vulnerabilities floating underground which are in the hands of money driven and black hat profit driven attackers.

This exponential growth in vulnerabilities and ease in exploitation with automated kits demands the security to be on the tows. Every time the topic of information security is discussed, it has to be related to three of its key pillars – Protection, Detection and Response (Figure 2). These pillars, if strengthened well, can lower the chances of any known vulnerabilities be exploited in your network. To keep the security on its toes and its top notch maintenance, a client has to consider a penetration testing engagement to verify the security controls and validate response timings. So, what is Penetration testing all about?

Penetration Testing (or PT) is a widely used term with a broad meaning. It is generally referred to as a method to evaluate the security posture of a network, system or a device by simulating an attack or hacker's activity. Though it is very much conjugated with Vulnerability Management (or VM) but there is a difference in their application and implication. While VM is commonly a part of any PT or risk assessment, but on a general note PT has more to do with active exploitation of the resources in scope, where in VM has to deal with the identification and quantification of vulnerabilities but not their exploitation. Overall a PenTest provides assessment support on all these pillars – verifies the security controls to check if they can be bypassed, and verifies the log, monitoring and alerting systems.

We are living in an era where cyber war and cyber-attacks are no more fictional plays. Even cyber espionages are also a part of controversial theories and discussions. We have hundreds of portals with security feeds, malware news and recent vulnerabilities available online. But are all these news, podcasts and blogs important for your business? You have deployed a number of software and devices in your network and you specifically need a risk assessment report that can cater to your requirements and technology setup instead of all the white papers shouting of exploitable applications which are not even installed inside your enterprise perimeter. An enterprise PT report usually has three main sections as shown in Figure 3, customized to the enterprise business model.

Each of these sections can be further categorized into sub topics as per application/network setups, security controls, technicalities/processes and compliance terms & conditions etc. On a short note the *background information* refers to the type of business the client is involved into. The main reason for this is to prioritize the severity ratings and provide remediation methods

Selling Penetration Testing Services:

Two words, Adding Value

The security of an organization's information assets is increasingly being scrutinized. Risk Management and Security have traditionally been an afterthought and have rarely been integrated into the business processes.

Today, most organizations are faced with the task of cutting cost. Unfortunately, this means that companies are trying to do more with fewer resources. This normally translates to those few resources, focusing on maintaining the IT environment versus the development of process improvements.

Although security awareness has increased and organizations recognize the need to have security talent on staff, many companies still do not have dedicated resources. This typically means the security responsibilities for the organization is transferred to someone with interest in security (i.e. *Network or System Engineer*). As an external pentester, you need to recognize the constraints that many organizations are working under and tailor your services to fit their needs. Yield better results in selling pentesting services by thinking outside of the box and break free from the traditional thoughts of pentesting. Exploiting a system and reporting the findings should no longer be the sole purpose of a pentester. Make it your mission to teach organizations the benefits of implementing a holistic security program and use the pentest results as the beginning of building that business case

Organization Discovery

When engaged in selling a client on the need for penetration testing, take the time to ask questions about the organization, its processes, and what keeps the CIO/CISO awake at night. Don't be afraid to ask probing questions to gain insight into the information security framework or philosophy, processes, and the tools used. Ask questions such as… Are peer code reviews being completed? Who performs the reviews? Who is responsible for the security in the products and services? What is your process for testing or verification? What is your process and procedures for remediation?

There tends to be two types of responses to the above inquiries. First, there is no such thing as a security team, process, or program implemented within the organization. Secondly, if the organization has an internal security team (or something that resembles a security team) they will conduct internal reviews. These reviews normally consist of utilizing commercially off the shelf tools and same will apply to their QA department when they ensure everything else meets standards through their tools and reviews. Because if a tool says the application or system is secure, then it surely has to be secure.

Provide Value = Strong Relationships

Confusion between a penetration test and vulnerability scanning is common. Take the time to explain the difference between the two and the value that each bring to the company. Also explain what is commonly accepted for a penetration test and the expected

Post Exploitation

Using Metasploit Pivot & Port Forward

A very nice feature in metasploit is the ability to pivot through a meterpreter session to the network on the other side. This tutorial walks you through how this is done once you have a meterpreter session on a foreign box.

The Meterpreter is an advanced multi-function payload that can be dynamically extended at run-time. In normal terms, this means that it provides you with a basic shell and allows you to add new features to it as needed. Please refer to the Meterpreter documentation for an in-depth description of how it works and what you can do with it. The Meterpreter manual can be found in the \documentation" subdirectory of the Framework as well as online at: *http://www.metasploit.com/documents/meterpreter.pdf*.

Once we have compromised a system on the network the goal is to learn more about the target environment and find openings by directly interacting with the target systems. The objectives include determining the addresses used by systems including hosts (servers and clients), network equipment (firewalls, routers, switches), and other devices. We want to learn the environment creating a diagram, a network map that we can plan further attacks. We want to determine the operating system, list of listening TCP ports, which ports are open, and a list of potential vulnerabilities. To accomplish this goal we will be using the victim as a pivot to attack deeper into the network.

The Metasploit Framework is a penetration testing toolkit, exploit development platform, and research tool. The framework includes hundreds of working remote exploits for a variety of platforms. Payloads, encoders, and nop slide generators can be mixed and matched with exploit modules to solve almost any exploit-related task. You can download metasploit from here.

Here is a network diagram (Figure 1) of the network I will be discussing. Notice that the attacker machine is connected to a router with the IP address of 192.168.1.132 and our victim is connected to the same

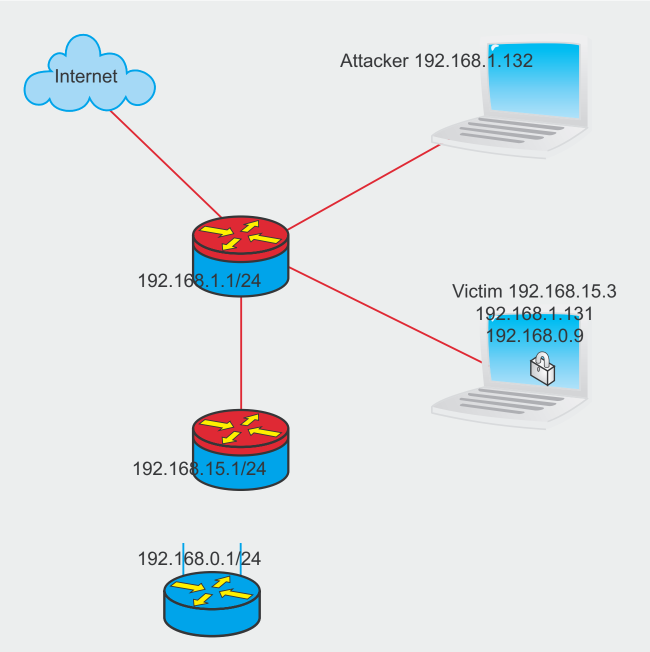
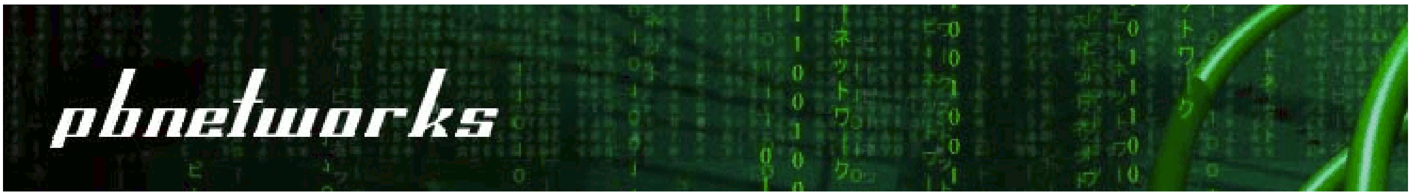


Figure 1. *Network diagram*

a basic version of pivoting through the meterpreter payload. The scan we performed went through 192.168.1.131 to 192.168.15.0/24 network and the 192.168.0.0/24 network. We then used the `portfwd` command to display the internal web pages, telnet, and ssh locally over SSL.

DAVID J. DODD

David J. Dodd is currently in the United States and holds a current 'Secret' DoD Clearance and is available for consulting on various Information Assurance projects. A former U.S. Marine with Avionics background in Electronic Countermeasures Systems. David has given talks at the San Diego Regional Security Conference and SDISSA, is a member of InfraGard, and contributes to Secure our eCity http://securingourecity.org. He works for pbnetworks Inc. http://pbnetworks.net a small service disabled veteran owned business located in San Diego, CA and can be contacted by emailing: dave@pbnetworks.net.



Secure Windows Implementations

Nothing is unbreakable, but we sure can make it hard for others to break into our systems. Back in 2001, it was declared by some that Microsoft Windows XP was Microsoft's most secure operating system ever.

Although this has been proved wrong by many security experts, Microsoft Windows XP still remains the most used operating system worldwide. Local vulnerability assessments show that a properly configured XP can thwart many unsolicited attacks. Many Windows systems can be compromised due to poor administration.

Plug & Play Disable

XP autorun feature enables the system to begin reading a drive as soon as it is mounted. Many malicious drives containing the *autorun.inf* file which automatically installs the malware into the system. It is possible to disable this service. (See Figure 1)

Step1

Go to *Run>Type: gpedit.msc* (Group Policy Editor)

NOTE

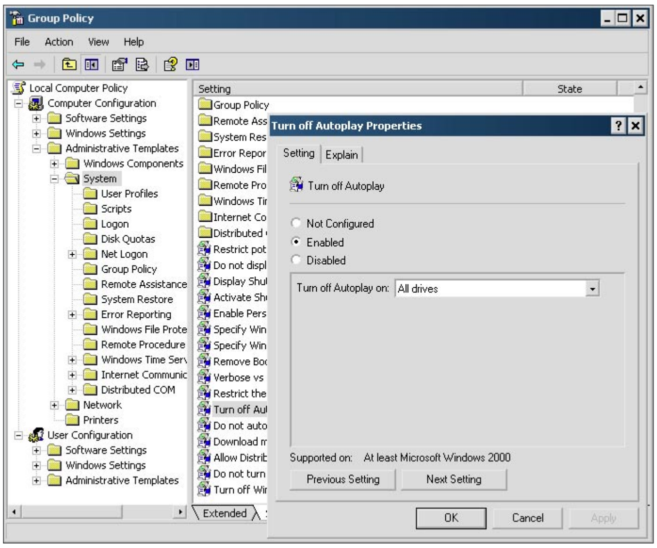
The contents of this article is only meant for reference, education and information purposes. The author or editor will not be liable to any person for the consequences suffered as a result of any action taken or not taken on the basis of the contents of this article. If you are unsure what you are doing with the host security of your Windows Operation System, then it is recommended you create a Restore Point before making any changes to the default configurations.

Step2

Go to Computer *Configuration>Administrative Templates> System>Turn off Autoplay*

Step3

Double click this item and select *Enabled* among the three radio buttons and select for the *Turn off Autoplay on* option, select *All drives* from the drop down menu. Hit *OK*.



Turn off Autoplay Properties

Turn off Autoplay

○ Not Configured
● Enabled
○ Disabled

Turn off Autoplay on: All drives

Supported on: At least Microsoft Windows 2000

Figure 1. *Turn off Autoplay Properties dialog in System folder*

Wild Hacking: Attacking with no-rules

Regular Penetration testing engagements -a.k.a. guided assessments- sometimes do not provide the coverage that a real Internet attacker could inflict against corporate servers, systems, networks, applications. In this article we are going to talk about the differences between following the manual and acting like a real intruder: attacking with no-rules.

How many of us have heard the phrase *thinking like an attacker* when talking about assessing vulnerabilities? Well, in terms of PenetrationTesting there is a misconception about what this means. For many security companies who provide these types of professional services *thinking* means *acting* but these acts are not well performed –or at least not well enough. This will continue until pen-testers, analysts and all the people involved in the security assessment area, start thinking about adding a layer to their current procedures -or methods in performing PT's – by adopting the techniques that are used right now *In the Wild* by the attackers on the Internet.

What is meant by attacking with rules?

We currently have various security testing standards such as: OWASP Testing Guide, OSSTMM, ISSAF or the NIST's methodologies which help companies execute the acceptable steps. These have been proven by many International organizations, and security companies will use them when performing security assessments, which is totally good, and obviously it works. I agree.

When we talk about rules, we are talking about following a standard process for a specific activity, but how precise and successful is the application of the rules of that process? Talking about rules and procedures, and expecting and experiencing the same behavior, it is important to note that they are not *fool-proof* which means that even if you are following the rules, the procedures may not be quite right. Each PenetrationTest is different, and is tailored to the customer size, their infrastructure, running systems and applications and sometimes specific hardware. So, what would happen if our current resources in terms of methodologies doesn't fit? For example, how would we test a complex infrastructure or an embedded device? This situation is where you first begin to realize the importance of leaving the rules behind!

Cross Site Request Forgery (CSRF)

Cross-Site Request Forgery. Session Riding. Sea Surfing. Web Trojans. Confused Deputy. Client-Side Trojans. CONFUSED? This is the same vulnerability, as widespread as its names.

Is the e-commerce or banking website you are accessing making you lose your hard earned money, even if it says that all the measures of authentication, identification, and authorization have been properly taken care of? Then it might be a CSRF attack. Cross site request forgery or session riding is a kind of attack which forces an end user to execute unwanted malicious actions without their knowledge or intent on web application in which they are currently authenticated. It basically exploits the trust a website has in user's web browser. This type of attack uses the privilege and identity of the victim user to perform undesired function. The user is a victim as well as an accomplice (unknowingly). One such vulnerability in Gmail was discovered in January 2007 which allowed an attacker to steal a user's contact list.

How does it work?

Attacker's main intention to accomplish this attack is to make the user click a URL. Typically, an attacker crafts an URL with embedded HTML or JavaScript code and tempts the user through an email or website (using Social Engineering) to launch the malicious URL through his browser. As the victim sends the request (unknowingly) and not the attacker himself, it becomes very difficult to determine that it is a CSRF attack. This kind of attack is very dangerous as it can be performed even if all the security measures of authentication, identification and authorization have been taken by the developer. Figure 1 shows a basic CSRF attack.

What can be done with it?

A successful CSRF attack gives the attacker almost all the privileges of the authenticated user. An attacker

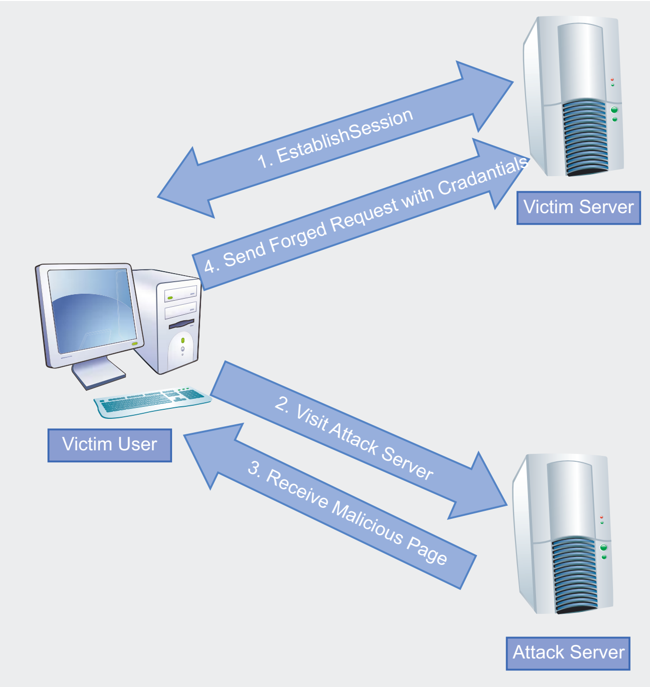


Figure 1. *Basic CSRF Attack*

Say Hello to Red Team Testing!

Security Art

Security Art's Red Team service operates on all fronts on behalf of the organization, evaluating all information security layers for possible vulnerabilities.

Only Red Team testing provides you with live feedback on the true level of your organizational security.

Thinking creatively! That’s our approach to your test.

Security Art’s Red-Team methodology consists of:

1. Information and intelligence gathering
2. Threat modeling
3. Vulnerability assessment
4. Exploitation
5. Risk analysis and quantification of threats to monetary values
6. Reporting

Ready to see actual benefits from your next security review?

info@security-art.com

Or call US Toll free:
1 800 300 3909
UK Toll free:
0 808 101 2722

www.security-art.com

In the next issue of Hakin9 magazine:

WEB APP SECURITY

Available to download on June 30th

Soon in Hakin9!

RFID, SQL Injection, Stuxnet, Hacking Facebook, Port scanner, IP scanners, ISMS, Security Policy, Data Recovery, Data Protection Act, Single Sign On, Standards and Certificates, Biometrics, E-discovery, Identity Management, SSL Certificate, Data Loss Prevention, Sharepoint Security, Wordpress Security

If you would like to contact Hakin9 team, just send an email to en@hakin9.org. We will reply a.s.a.p.