ITPRO.TV

Penetration Testing: Protecting Your Company the Right Way

How to minimize or eliminate your slice of $6 trillion in cybercrime costs

by Daniel Lowrie
ITProTV Edutainer - Security

IT LEADERSHIP SERIES: ISSUE 9

Just as doctors must probe their patients to uncover hidden maladies or diseases, so too must companies probe their networks, systems, applications, and web assets to uncover weaknesses subject to possible hacking. The practice is called Penetration Testing, or pen testing for short. As with all issues relating to security, there are optimal ways of conduct pen tests and less than ideal ways. This article addresses:

- **The scope of cybercrime and other issues requiring rigorous pen testing**
- **Types of pen tests**
- **Expectations and responsibilities of pen testers**
- **Generally accepted best practices for pen testing**
- **Top tools to assist with pen testing, and**
- **Considerations for performing pen testing by internal staff or an outsourced firm**

Scope of cybercrime

Hardly a day passes when a report of major cybercrime doesn't dominate the news. But just how big is the problem? According to a recently released report from CSO, experts predict that by 2021 cybercrime globally will cost $6 trillion annually or twice what it was in 2015. Astonishing as that prediction is, it's even more remarkable to consider the wealth transfer to bad actors that occurs and the largely unrealized benefits of innovation, investments, and risk taking. Like a rug being pulled out from under companies, the losses are not only large but devastating to their future viability.

Aside from the direct losses from cybercrime, we must also ladle on to this figure the direct costs enterprises spend to fight cybercrime. According to Gartner, currently we spend $86.4 billion on fighting cybercrime, and they project that number to reach $1 trillion between 2017 - 2021. Not factored into this amount is the burgeoning juggernaut that is the Internet of Things and its related technology cousins.

You get it: the problem is huge and the costs enormous. All we need to do is put the best and brightest cyber security employees to work. There's a catch, however. Unfilled cybersecurity jobs are expected to top 3.5 million by 2021, severely impeding companies' ability to effectively secure their enterprise.

Looking to train your team on cybersecurity? Check out the ITProTV course library for engaging training including Pen Testing, Certified Ethical Hacker, and more.

As the Internet continues to explode in content and systems, the number of Internet users is exploding as well. According to Cybersecurity Ventures, six billion people will be on the Internet by 2022, approximately 75% of the world's population, up from 3.8 billion in 2017. With more Internet users comes more potential openings for attacks.

Most insidious of more recent cybercriminal tactics is ransomware. Up from $325 million in 2015, ransomware attacks in 2017 exceeded $5 billion and, according to Cybersecurity Ventures, it will rise to $11.5 billion by 2019. It predicts a ransomware attack will hit every 14 seconds, something that should keep CIOs and their security teams up at night.

This world of constant attacks is the new normal. Security that's treated as an afterthought rather than it being central to an enterprise's DNA is setting out a welcome map for hackers and inviting them in with an extra set of keys.

Types of Pen Tests

To deal with the onslaught of cybercrimes and related issues companies rely on penetration testing. A pen test, also referred to as ethical hacking, is essentially leveraging hacker tools and skill-sets for the benefit of

the company. There are multiple flavors of pen tests depending on the targeted infrastructure. Thus, it's important to understand first exactly what it is you're seeking to uncover or prove worthy. Let's do a quick review of what each type entails.

External Testing

This type focuses on only what's visible on the Internet, such as website, DNS, and email servers. The overall goal is to obtain access, gather valuable data, and leave without being identified or tracked. Think of it like a tester checking the locks on external doors and windows of a building to verify they are actually safeguarding against unauthorized access. The same concept applies except it is against the enterprise's digital space, including servers, firewalls, etc.

Internal Testing

Different from external testing, an internal pen test is one performed behind the firewall. These tests can take multiple forms; perhaps emulating a disgruntled employee, or by way of an insidious phishing attack facilitated by stolen employee credentials. From the inside, the tester would tend to have broader reach into the network(s) and/or systems, including IP address schema(s), source-code, and OS details, slyly avoiding detection.

Blind Testing

AKA Black-Box testing, is a technique used to predict how bad actors will attack a particular enterprise. Many times a blind tester is provided with little more than the name of the company. What unfolds during the test is a likely road map of how bad actors will navigate the

systems to puncture holes in security and then gather data. This type of test affords security personnel real-time insights into each tactic of the tester.

Double-Blind Testing

In these tests, there's no knowledge that a test is about to happen. Security personnel doing their everyday jobs are left in the dark and must react in real time. This type of double-blind test is most like a real-world attack because all parties are unaware of the other side's efforts; first to enter and second to block.

Targeted Testing

As its name suggests, this type of pen test focuses on particular aspects of the organization's infrastructure. Here, both the pen tester and the security team work together to understand, track, and monitor movements.

Expectations and Responsibilities of Ethical Penetration Testers

Given the high stakes of cybercrime, ethical penetration testers must adhere to the clear parameters of their assignment.

Specifically, all penetration testers should:

- Think and act like actual bad actors intent on causing damage or theft, going right up to the point of almost causing actual harm;
- Be judicious with the information required to perform the penetration test;
- Clearly articulate the type of test to be performed;
- Use any and all means necessary to find flaws that are susceptible to attack from bad actors in defined systems, software, networks, and applications;
- Stick to the agreed schedule to ensure actual pen testing is not misconstrued as actual hacking events;
- Be diligent scientists by carefully logging actions, reactions, issues, etc. so that the test can be repeated as necessary to fully illuminate the areas of concern;
- Take responsibility for any loss in the system, including data and machine performance; and
- Maintain strict confidentiallity with regards to the company data, including any reports generated by the tester, unless specifically released by the company.

Generally Accepted Best Practices for Pen Testing

While companies may have their own penetration testing process and there are always one-offs, edge-cases, and peculiar circumstances that will dictate how a pen test is conducted, there is a mostly broad agreement that entails at least the following five stages.

1. Planning, research, and reconnaissance

This stage focuses on the scope of the test to ensure all parties involved have clear instructions, understand what systems are being tested, what intelligence currently exists with respect to domains, OS, networks, email servers, website, and other valuable infrastructure.

2. Scanning

During this stage, the pen tester will determine how a particular application or system responds to an intrusion, call it the first element of pen stress test. These scans can be performed in a static fashion or dynamically as the application or systems are running.

3. Gaining access

This stage is when a penetration tester pulls out all the stops, leveraging various tools and tactics to launch web application attacks such as Cross-site Scripting(XSS), SQL injection(SQLi), and Man-in-the-Middle(MITM) attacks to exploit a target system's vulnerabilities and users. After securing access, the pen tester will likely use other methods to further explore and exploit the openings. The methods might include escalating privileges, stealing data where possible, and intercepting traffic.

4. Maintaining Access

Depending on the scope of the test, maintaining access after breaching a system or application is important because it shows how a persistent bad actor could remain in place, undetected, over long periods of time. Like a bad strain of bacteria unfettered by an antibiotic, the germ can continue to do damage.

5. Analysis and Reporting

After the test is complete, the pen tester reviews with the security personnel precisely what was done, how systems performed, how long the tester was inside systems undetected, what vulnerabilities exist, and which priorities require

immediate attention. This input is vital to enable the company to adequately remediate certain systems and applications.

Depending on the outcome of the penetration test, the company should immediately undertake another test after red flag areas have been patched to determine if they have been adequately fixed. Further, the company should consider a regular schedule of different types of tests to ensure any new systems or applications put into action do not represent a potential vulnerability.

Top 12 Penetration Testing Tools

Talent being only one part of the equation, penetration testing tools are the other side. Below is a brief review of some of the top tools commonly used to assist security personnel in their pen tests. While there are many other tools, these are most often mentioned in various reviews.

1. Metasploit

Metasploit Pro is an exploitation and vulnerability validation tool that helps divide the penetration testing workflow into smaller and more manageable tasks. With Metasploit Pro, a company can leverage the power of the Metasploit Framework and its

exploit database through a web-based user interface to perform security assessments and vulnerability validation.

2. Wireshark

Wireshark is one of the world's foremost and widely-used network protocol analyzer. It lets companies see what's happening on their networks at a microscopic level by "sniffing" the network packets as they cross the wire and are used across many commercial and non-profit enterprises, government agencies, and educational institutions.

3. Kali Linux

Kali Linux incorporates more than 300 penetration testing and security auditing programs with a Linux operating system, delivering an all-in-one solution that enables IT administrators and security professionals to test the effectiveness of risk mitigation strategies.

ITProTV has on-demand courses on Metasploit, Wireshark and Kali Linux available now.

4. w3af

w3af is an extremely popular and flexible framework for finding and exploiting web application vulnerabilities. It is easy to use and extend and features dozens of web assessment and exploitation plugins.

5. Netsparker

Netsparker finds and reports web application vulnerabilities such as SQL Injection and Cross-site Scripting on all types of web applications, regardless of the platform and technology they are built with.

6. Nessus

Nessus Professional is one of the industry's most widely deployed assessment solutions for identifying vulnerabilities, configuration issues, and malware that

attackers use to penetrate an organization's network. It specializes in compliance checks, sensitive data searches, IP scan, website scanning, and overall excels at aiding the pentester in finding weak-spots.

7. Burpsuite

Burp suite is a web application vulnerability scanner. It ranges in its abilities which includes an intercepting proxy, web crawling for content and functionality, web application scanning, etc.

8. Cain & Abel

This is a password recovery tool for Microsoft Windows. It can recover many kinds of passwords using such methods as network packet sniffing, as well as password cracking techniques including dictionary, brute force, and cryptanalysis attacks.

9. Zed Attack Proxy (ZAP)

ZAP is one of the world's most popular free security tools and is actively maintained by hundreds of international volunteers. It can help companies automatically find security vulnerabilities in their web applications, whether they are still in developing and testing, or already in production.

10. Acunetix

Acunetix is a web vulnerability scanner specifically for web applications. It provides SQL injection, cross-site script testing, PCI compliance reports etc. along with identifying a multitude of vulnerabilities.

11. John The Ripper

John the Ripper is a password cracker, currently available for many flavors of Unix, Windows, DOS, and OpenVMS. Its primary purpose is to detect weak Unix passwords, but is also effective against Kerberos AFS, Windows LM Hashes, MD4, etc.

12. Retina

The Retina Network Security Scanner is one of the more sophisticated vulnerability assessment solutions on the market. Available as a standalone application or as part of Retina CS Enterprise Vulnerability Management, Retina Security Scanner enables companies to efficiently identify IT exposures and prioritize remediation enterprise-wide.

Robust pen testing often involves use of many different tools to cover all aspects of the test. Thus, it's not uncommon to leverage most, if not all, of the tools on this list in some form or

fashion. Sophisticated pen testers react to the systems they encounter with the right mix of tools.

Considerations for Internal vs. Outsourced Penetration Testing

Penetration testing is best left to experienced professionals who understand the various tools, technologies, and techniques because there are inherent risks associated with the test themselves. For example, whether performed manually or via some automated system, pen tests can "gunk up" a network, slowing it down and turning computers into sluggish nodes, or, worse yet, even causing systems to crash, which could have harmful effects on the business. If your company has trained and certified security professionals skilled in the art and science of pen testing, then it's fine to proceed with the requisite caution.

If, however, your internal staff does not have the chops to perform the tests and lacks the experience, it's wise to consider outside third parties who are better equipped to avoid potential negative business/system impact. They will likely have seen far more diverse scenarios of vulnerabilities which will be of benefit to your company.

Below are some questions you should ask of those third party penetration testers you're considering hiring:

- What industry certifications does the company hold and who specifically in the company holds them?
- How many penetration testers does it employ?
- What is the name of the individual(s) who will carry out the penetration testing for your company?
- What professional qualifications and certifications do they have and how experienced are they?
- What services does the company provide in helping to scope the test?
- Can it follow these up with security awareness anti-phishing training?
- How would it carry out a penetration test, and on what time scale?
- What will the test cost, and under what circumstances might the scope of the project increase?
- What steps do penetration testers take to minimize possible effects on your business?
- What insurance does the company have if it inadvertently causes damage?
- What reports and recommendations will be provided after the test, and how much detail will they include?

Conclusion

Penetration testing should become, if it's not already, a regular occurence in most enterprises. To stay ahead of the bad actors who seek to cause damage, it's vital that testing not be sporadic but rather almost constant as each change in a system, application or database can have ripple effects through which vulnerabilities can be easily exploited.

Daniel Lowrie

ITProTV Edutainer - Security

About the Author

Daniel worked as a systems and network admin before moving into teaching. He was drawn to ITProTV because he himself is a visual learner and that's key to ITProTV's content. He holds certifications in A+, Network+, Linux+, CEH, and MCSA.

Connect with him @Daniel_ITProTV

ITPRO.TV

Flexible training.

Bingeworthy content.

ROI proven.

Learn more

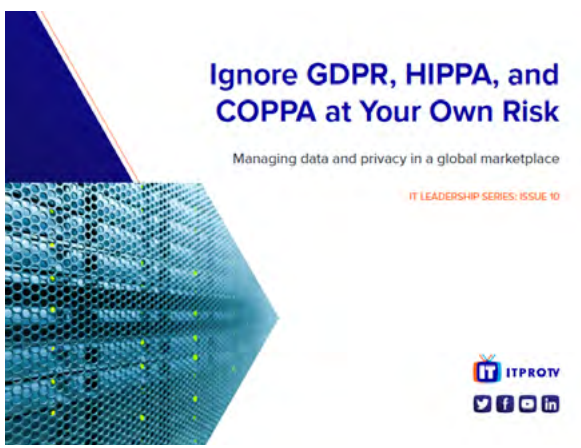
About ITProTV

ITProTV is an eLearning company that delivers engaging content to train IT professionals in every stage of their careers. With training that's more like a talk show, you'll watch your 'edutainer' engage with a host and an online audience to create a better-than-classroom experience that you'll look forward to watching. Access 3,300 hours of friendly content, with new content added daily, plus practice exams and virtual labs. Flexible and cost-effective options are available for both corporate teams and individual learners. Learn on the go, at your desk, or wherever is most convenient. ITProTV delivers proven ROI on training to businesses and individual learners worldwide.

You may also like...

Ignore GDPR, HIPPA, and COPPA at Your Own Risk

Managing data and privacy in a global marketplace



Align Your Business & IT Strategy in 10 Steps

Ensure your IT team can support business goals

The 3 Biggest IT Challenges with Managing a Mobile Team

Tips to manage mobile workers, mobile devices, and mobile assets


ITPRO.TV