Exploit Security Vulnerabilities by Penetration Testing

Devin Sweigert*, MD Minhaz Chowdhury*, Nafiz Rifat**
*Department of Computer Science**
East Stroudsburg University
East Stroudsburg, USA
Department of Computer Science**
North Dakota State University
Fargo, ND, USA
Email: dsweigert @esu.edu, Mchowdhur1@esu.edu, Nafiz.rifat@ndsu.edu

2022 IEEE International Conference on Electro Information Technology (eIT) | 978-1-6654-8009-3/22/$31.00 ©2022 IEEE | DOI: 10.1109/eIT53891.2022.9813929

Abstract-*When we setup a computer network, we need to know if an attacker can get into the system. We need to do a series of test that shows the vulnerabilities of the network setup. These series of tests are commonly known Penetration Test. The need for penetration testing was not well known before. This paper highlights how penetration started and how it became as popular as it has today. The internet played a big part into the push to getting the idea of penetration testing started. The styles of penetration testing can vary from physical to network or virtual based testing which either can be a benefit to how a company becomes more secure. This paper presents the steps of penetration testing that a company or organization needs to carry out, to find out their own security flaws.*

Keywords- Black Box Test, White Box Test, Hashcat, DoS, DDoS, Kali Linux, Dark Web.

1. Introduction

The first thing that might come to mind is what is penetration testing? Pen testing is discovering vulnerabilities, threats, and risks. These can be risks in the actual infrastructure of a facility or a break in the security of a company's network. This involves the pen tester to find the risks to the system and figure out how they need to go about fixing the issue [1]. During a pen test you are trying to see what parts of the current defenses that are in place you can get past. Once the pen tester figures out what risks there are their job is to report back to the client or company. With the report that is received after the test it is the job of the pen tester to put a plan in place to figure out how the client or company will implement a fix for the vulnerabilities for and put into place a way to prevent any further attack from affecting the company or facility. The idea of pen testing started in the sixties and was not something that was extremely popular. It became more well known as the FBI started using it on their computers in the seventies.

When companies decided that penetration testing could be beneficial to them, it became more of a priority to perform such tests [2]. As hacking became more advanced so did pen testing.

There are two distinct types of virtual pen testing. The first type is white box penetration testing, this strategy looks are going over the entire system with the most amount of prior knowledge to access information in the system. Both on the physical and virtual side this involves taking more of an obvious approach rather than more of a stealthy approach [3]. with this strategy the penetration tester can find the most information because they are granted the most access. One of the downsides to this idea is that would not replicate a fully accurate form of how an actual hacker would be accessing the system. The next method that is used is called black box penetration testing. With black box penetration testing it is the opposite of what white box penetration testing. The black box pen testing is more of realistic way of testing an organizations system or network. This method could be looked at as

978-1-6654-8009-3/22/$31.00 ©2022 IEEE

more of a realistic approach since the tester would be give the same information as the actual hacker would, which is little to not information. This would all be based on how much information the hacker was able to find ahead of time or was able to get from a previous reconnaissance attempt. This strategy is looked at as being more discreet than the other approach since the company or client be evaluated would not necessarily know when the tester would be performing this test. Which is more realistic to how a hacker would perform their attack. When that attack is done it will show how vulnerable the system may be to a real-world attack.

When performing the physical pen test that involves actual breaking into the facility or trying to gain access to sensitive information by the means of locking picking doors or climbing fences for example. First before performing these tactics the penetration tester will produce a plan on how they will perform the physical test by scouting out the location first [2]. In this paper we would like to highlight and explain to the reader what pen testing is and how it is beneficial to a company or organization.

Whether the test is a physical or a virtual penetration test they both involve the same purpose of trying to gain access to sensitive information. And penetration testing is useful in many different environments, and it will allow for more security in many ways since it will stop physical and virtual access for intrusion of sensitive information. One of the main aspects to remember when performing these penetration tests is to make sure the tests being performed are tests that fall in between the law, and no laws are being broken in the process. Along with this you must make sure to keep a good team on hand that can work well together to make sure an appropriate test is being performed for each situation or task at hand. But before starting the test or making plans to perform the test you will have to make sure that you are equipped with the right tools that are needed to get the job done. When getting that portion done that is when you will move on to planning on how to conduct the test you have at hand and what types of strategies are going to be put in place to infiltrate the facility whether it be for a physical test or virtual test or even both. Most test will incorporate at least a little bit of both types of testing, but that is something that comes down to the company and what the needs of the company are. Research shows that, most of the network penetration threats can be categorized and detected from pen test [17]. Hence the dimensions of cyber-attacks are vastly responsible on the performance of pen test [21].

2. Background

Now that vulnerabilities are more of a problem it is essential to make sure to have a computer security plan in action. Planning for an attack can be exceedingly difficult since there are several various attacks that have become common withing the computer security field with hackers. And it is easier than ever to watch videos online or read about how to perform these attacks. When first starting with penetration testing it wasn’t something essential that all organizations or companies had access to. It was just used in the military when it first started. In the sixties hacking was not something that was being used for the same purpose at it is today [4]. During that time, it was used to test the performance and see how well the machines ran. It was used more as a test for the computer in a performance aspect. Which is widely different then how we use it today? In the seventies there was more of a worry about hacking when there were people hacking into the phone lines to make long distance calls for free. That is something that is hard to believe since today home phones are not common. However, during that time it was a bad issue, and it was making security something that was profoundly serious. From there in the eighties and nineties were when computers and the internet would become a big start into the world of the internet. That is when the internet started to become what it is today. During the nineties is when you started to see the big names in hacking, and it became widely known as a big issue that would continue to grow. During the early two thousand is when companies decided to take on the idea of using penetration testing as a widespread practice to make sure their company and their data is safe. It was big wakeup call in the mid 2000's and later that if some of the big companies that were affected by hacking would have benefited by using a penetration tester to find the vulnerabilities these companies had and to of stopped these big data breaches from happening in the first place.

Now some companies even employee their own personal penetration testing teams. Now that it has become easier for about anyone to learn how to penetrate physical, virtual security and even personnel security. Companies must step up their game to combat this situation before it leads to companies losing profit and loosing sensitive information that affects the company or the individuals the company is working with. Performing the penetration test is something that a company must weigh out to make sure that the assets being attacked are worth the extra expense. By performing a penetration test it highlights the flaws in a company's security and what they do implement to fix these issues.

There are two different variations of penetration testing. The first being black box testing and the other being white box testing. They are similar but different in a few ways. With the black box testing the person involved in doing the testing they are not giving any prior information and they try to penetrate the network [5]. With white box testing this allows the tester to gain full knowledge of what they need for the network, and this allows the penetration tester to test how secure all the networks are with full knowledge of the systems. This is also a way for the penetration tester to still try and not been identified while doing the testing. There can also be specific requirements that the companies put in place if they only want certain requirements met for the test to be done. It is not only important to have these physical or virtual penetration test done.

It is also important to provide your employees with training on what they can do to stop or to cut down on several types of attacks that the company is at risk for encountering. Using a schedule of six months or sooner to keep your employees informed on the new and constant security issues that are becoming a problem. It is important to keep this a constant practice to make sure your employees are informed of the practice's hackers are using today. This is something that is constantly changing that needs to be kept up on. If you do not constantly and consistently keep up on this, it can be something that some individuals may not know. That is because the tactics hackers are using are becoming increasingly advanced and it is even hard for experts in the field to even keep up with this.

3. Mandatory Tests

When performing a penetration test it is more important to make sure that every aspect the company wants to be tested is tested. This is important for so many businesses because so much of their information for these companies is based on a network or stored in a cloud. This allows for many ways for hackers to identify the weak points in the system [2]. By hacker, it means all the categories of hacker, including ethical or white-hat hackers [12][13].

There are some companies now that make this a mandatory process to perform yearly or quarterly penetration tests. Where this comes to be a huge benefit for a company is by the penetration test showing what aspects of their system has vulnerabilities that need to have more money invested into protecting. The results though with a penetration test can be mixed depending on different companies approaches and the individuals doing the tests. This can cause the results of two penetration tests to differ. With these tests there is not a standard for the company performing the penetration test to go by. These tests can be broken down into several types of tests. A physical penetration test or a virtual/network penetration test.

4. Pen Testing Steps

This is where the steps to penetration testing come into play. The first step would be reconnaissance. As mentioned previously this is where the pen tester will either be given a job based on white or black box testing. Which decides how much information the tester will be given for this portion of the test. Either way they will do their own observations. Whether it be physically by trying to gain as much information prior to seeing the location or virtual by getting domain names or checking on the network to see what is accessible [6]. The next part of the test is scanning, with the scanning portion of the test it involves scanning the network to see what is available. As well as scanning the physical environment to see how the tester will approach the situation and what tools will be needed. The next step in the phase is Gaining access, during this process this is where the user will try to gain control of the system whether it be breaking into the network and gaining access to the required information the user is trying to access physically. During this step is where you could use social engineering to gain information during this step. The next step is maintaining access; this is where the tester tries to continue access, if possible, without being detected to gain the most amount of information possible. This step is more applicable to the virtual side.

5. Virtual Pen Testing Tools

The virtual side of penetration testing can be traced back to how the entire system is setup. From the start if the system was not properly setup this can allow for weak passwords or lacking security. To find and fix this lack of security there are some common tools used by penetration testers. One of the big tools the pen testers use is Kali Linux. Kali Linux is a variant of Linux that has tools built into the software for trying to perform offensive tactics by trying and testing how secure a company's network is [7]. And it shows the major flaws in the system by using the supplied tools in the software. Most of the tools mentioned can either be installed or are already installed on Kali Linux for example a tool included with Kali Linux is Wireshark. Wireshark is a tool that is used to monitor packet loss, view network traffic and any variant of malicious activity that is happening on the network. Another tool available for Kali Linux is Hashcat which is a hash cracking tool. It uses password attacks such as mass and dictionary techniques to try and crack passwords. A tool on the virtual side as important would be Nmap. Nmap is a port scanning software. This is important because this allows you to scan all the ports available and check for unwanted activity on these ports [7]. Extreme caution should be used when port scanning because it is easy to accidentally cause a DoS or DDoS (denial of service) attacks [10][11].

Nmap is also a tool available on Kali Linux, all the software tools talked about are available on Kali Linux, so it is obvious that Kali Linux is such an important broad tool with other added tools that make it essential for good penetration testing. Kali Linux allows for a lot of expansion of tools based on the situation and case that needs to be addressed. Despite Kali Linux's usability, this Linux distribution is inherent to security flaws [9].

Recently machine learning is relying on the pen test historical datasets to train the infrastructure for future intrusion detections [8][16][17].

6. Physical Pen Testing Tools

There is a very wide variety of tools used for the virtual side of penetration testing. On the physical side of penetration testing, this will vary job by job. Some of the tools used are bolt cutters, binoculars, ladders, hammers, crowbars, and other various tools that are required for breaking into the building/office or other type of building. Most locations are going to have a similar approach on how to gain access to the facility. If the job These tools are quite different than the tools used on the virtual penetration test, but it is all part of doing the same job. Most of the tools are typical tools that you would think of someone breaking into a building would use. There are a lot of factors of the building that play into what is required.

Each part whether it be the virtual or physical side of the penetration testing is for the same purpose of making sure that at the end when the company receives the final report that they have all the information needed to make their system more secure than it was before the penetration test was done. If this is not taken into effect, then companies will continue to have the same issues they had before without any improvements.

Once these tests are done it is the job of the tester to show everything that was found and everything that they were able to access on the virtual and physical side. This is the opportunity to provide a solution for preventing the same issues again. That is when the company has testers come back to perform testing again. It is also important that the company makes the necessary changes that the testers bring up to them. If not, then the whole test will become useless for stopping any kind of threat if there is no such action take for these issues. since knowing does not fix the problem it just makes you more aware of it. An organization shall protect its assets from threats by regular pen testing its assets, especially to check the possibility of an attack from the Dark Web. Dark web facilitates the black hat hackers [14].

7. Conclusion

We think that the takeaway for this should be that more than ever penetration testing is almost essential for a company. We think that it is a wonderful way for a company to find the flaws that may not be obvious to the company since a penetration tester has a different mindset or way of thinking than the company or business would. There are very few downsides to have a penetration test done for a company. It is only beneficial for them to find vulnerabilities and fix them if there was an issue or prevent future problems with data loss and sensitive information getting into the wrong hands. With lots of big leaders of large companies becoming the targets of even small-scale attacks it makes obtaining sensitive information a hot commodity. There have been major benefits for companies who have had penetration tests done to their establishment because it has helped them determine the problem areas for their security. They are also an effective way for the pen tester to inform you with information that you can pass on to your employees to educate them in what is a vulnerability. It can also be effective to allow for the company to have meetings every couple of months to inform employees of all the threats they are vulnerable to. That is because the weakest link in security comes to the user themselves. By eliminating this factor out of the equation for a “hacker” then this makes it harder this to become a weak point in the security of a business or company. Then at that point it comes down to the business or company to make the necessary fixes to make sure that there is nothing that allows either the virtual or physical side to be accessed. Which is in the best interest of the company to make the necessary changes. It is important to make sure that if there are issues, they are addressed. The penetration testing team can come back out later to reassess and make sure no new vulnerabilities were made. Also making sure that the company made the proper changes to make sure nothing is comprised. Without penetration testing being introduced it would allow increased attacks to continue small and large companies alike. But it can only be beneficial if the right precautions are taken to safeguard the information provided to these companies.

References

[1] W. Allsopp, Unauthorised Access. Wiley, 2010, pp. 19–25.

[2] P. Engebretson, The Basics of Hacking and Penetration Testing, Second Edition. Elsevier Science, 2013, pp. 1–5.

[3] Anonymous, “Research and Markets: Unauthorised Access: Physical Penetration Testing for IT Security Teams,” M2 Presswire, p. 1, 2009.

[4] J. Wallingford, M. Peshwa, and D. Kelly, “Towards Understanding the Value of Ethical Hacking,” in, Reading, 2019, pp. 641–645, Accessed: May 01, 2021. [Online]. Available: https://search-proquest-com.wilkes.idm.oclc.org/compscijour/docview/2198531122/abstract/B52C9FC164CE4BDEPQ/1?accountid=62703.

[5] N. Mehrotra, “The Importance of Penetration Testing,” Open Source for You, pp. 1–3, Apr. 13, 2020.

[6] H. Singh and Dr. J. Singh, “Penetration Testing in Wireless Networks,” International Journal of Advanced Research in computer Science, vol. 8, no. 5, pp. 2213–2214, 2017, Accessed: May 01, 2021. [Online]. Available: https://search-proquest-com.wilkes.idm.oclc.org/compscijour/docview/2417496474/D7F618DF4EA5433DPQ/8?accountid=62703.

[7] J. M. Porup, “11 Penetration Testing Tools the Pros Use,” Proquest, Feb. 21, 2021. https://search-proquest-com.wilkes.idm.oclc.org/docview/2359786534/BEB8A649D625466FPQ/8?accountid=62703 (accessed May 02, 2021).

[8] Ahsan, M.K., 2021. Increasing the Predictive Potential of Machine Learning Models for Enhancing Cybersecurity (Doctoral dissertation, North Dakota State University).

[9] Matthew R. Yaswinski, Md Minhaz Chowdhury, Mike Jochen, Linux Security: A Survey, the 18th Annual IEEE International Conference on Electro Information Technology, May 2019, South Dakota, USA.

[10] Will Bonasera, Md Minhaz Chowdhury, Shadman Latif, “Denial of Service: A Growing Underrated Threat”, Proceedings of the International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME), 7-8 October 2021, Mauritius.

[11] Michael Pokrinchak, Shadman Latif, Md Minhaz Chowdhury, Distributed Denial of Service: Problems and Solutions, the 2021 IEEE International Conference on Electro Information Technology, May 14 - 15, 2021, Mount Pleasant, MI, USA.

[12] Sean Vandervelden, Md Minhaz Chowdhury, Shadman Latif, “Managing the Cyber World: Hacker Edition”, Proceedings of the International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME), 7-8 October 2021, Mauritius.

[13] Logan Smith, Md Minhaz Chowdhury, Ethical Hacking: Skills to Fight Cybersecurity Threats, the 37th International Conference on Computers and their Applications, March 21-23, 2022, Virtual, MT, United States.

[14] Rhiannon Cole, Md Minhaz Chowdhury, Shadman Latif, “Dark Web: A Facilitator of Crime”, Proceedings of the International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME), 7-8 October 2021, Mauritius.

[15] Ahsan, M., Gomes, R., Chowdhury, M. and Nygard, K.E., 2021. Enhancing Machine Learning Prediction in Cybersecurity Using Dynamic Feature Selector. Journal of Cybersecurity and Privacy, 1(1), pp.199-218.

[16] Nygard, K.E., Rastogi, A., Ahsan, M. and Satyal, R., 2021. Dimensions of Cybersecurity Risk Management. In Advances in Cybersecurity Management (pp. 369-395). Springer, Cham.

[17] Ahsan, M. and Nygard, K.E., 2020, March. Convolutional Neural Networks with LSTM for Intrusion Detection. In CATA (Vol. 69, pp. 69-79).