University Of Agder

DAT 211

Networking and Security

Vulnerabilities

Author:
Bendik Egenes Dyrli

Supervisor:
Sigurd Kristian Brinch

2015

1 Introduction

Several computers expose services over the network. Depending on how these services are implemented, they might expose a vulnerability. This can be caused by bug that was created by a programmer. Though not on purpose but something that appeared either in development but wasn't found or, that after it was deployed into production the bug appeared and created a vulnerability. There are two kind of people who appear when the category seeking vulnerability. Black Hat and White Hat are the kind of people you'll hear about when it comes down to exploiting vulnerabilities. However this will be described more thoroughly in this essay, as well how to keep your system protected against hackers who want to harm massive computer operations.

2 What is a Vulnerability

A vulnerability is known error or hole in the application, though it can be a design flaw or it might be a bug that appeared while implementing a new feature, which can allow an attacker to cause harm on the owners of the software. [1, 2]

2.1 How do you find a vulnerability

There is something called vulnerability scanners, which is a tool that can allow you to pick a target, and search for vulnerability on any desired service. you can find most of these tools all over the Internet, or on the sectools.org[3] site where they will rate all the tools and tell you what each do. This site is a great place to find new tools to look for vulnerabilities on your websites. Many of these vulnerabilities scanner uses CVE when referring to Vulnerabilities if they've been found in your system. CVE [1] [4] CVE is like Wikipedia for vulnerabilities. Though if a criminal was to find a vulnerability, they wouldn't share their "secret" on how they produced the vulnerability. That would then try out this vulnerability and exploit to the universe and beyond.

3 The Western hats

When it comes to exploiting these vulnerabilities, there are mainly two different types of people. Those who do it for the fame and money, and those who do it to cause harm of computer systems, and or sell the exploit to criminals on the dark web. If we see things in perspective, you'll find that black hat hackers and white hat hackers is somewhat similar to the western. You have the black hat which is the bad guys, and then you have the white hats who's like the sheriff. So the sheriff will always keep repairing things that are broken so the black hats won't use that "vulnerability" to cause harm on the citizens of this town. Then you have the grey hats, which will shift back and forward from being both the good and the bad guy. [5]

[1] Common Vulnerabilities and Exposures

3.1 Ethical Hacker aka White Hat Hacker

Ethical hacker is the kind of hackers which, can get hired to check the security of your computer systems. Basically they'll get payed to break into your systems and use all kind "tricks" to do this, like for example social engineering [2] is one technique they can use to get access to their system. [6, 7]

4 Conclusion

What we've found out is that there are more to vulnerabilities, than just people who just want to do harm on massive computer operations. There are also a certain type of people who gets hired to hack into companies systems, to check their security, and how their workers will react when they see someone is trying to get access to the system, however not every one will notice it. Thus is only a job that certified Ethical hackers get, black hat hackers are in most causes or always a person who tries to find a back doors to a company that has a high level of customers, and a trust by it's customers that their sensitive information won't be share out on the WWW[3]. However now in these times there is no assurance that your information stored by a service, will be secure for all eternity.

[2] Social Engineering is a blend of science, psychology and art. While it is amazing and complex, it is also very simple.

[3] World Wide Web

References

[1] Owasp.org, "Category:Vulnerability - OWASP", 2014. [Online].
https://www.owasp.org/index.php/Category:Vulnerability
[Accessed: 17- Jan- 2016]

[2] Niatec.info, "Glossary of Terms", 2015. [Online]
http://niatec.info/Glossary.aspx?term=6344alpha=V
[Accessed: 17- Jan- 2016]

[3] Sectools.org, Vulnerability scanners ; SecTools Top Network Security Tools [Online] *http://sectools.org/tag/vuln-scanners/*
[Accessed: 18- Jan- 2016]

[4] cve.mitre.org, The Standard for Information Security Vulnerability Names [Online] *https://cve.mitre.org/about/index.html*
[Accessed: 18- Jan- 2016]

[5] How To Geek, "Hacker Hat Colors Explained: Black Hats, White Hats, and Gray Hats" 2013. [Online] *http://www.howtogeek.com/157460/hacker-hat-colors-explained-black-hats-white-hats-and-gray-hats/*
[Accessed: 17- Jan- 2016]

[6] Social-Engineer.org, "What is Social Engineering? - Security Through Education" [Online] *http://www.social-engineer.org/about/*
[Accessed: 18- Jan- 2016]

[7] Lifehacker.com, "Career Spotlight: What I Do as an "Ethical Hacker" " [Online] *http://lifehacker.com/career-spotlight-what-i-do-as-an-ethical-hacker-1706940692*
[Accessed: 18- Jan- 2016]