This is a recommendation for the blog entry of Group M:
https://github.com/ovi28/UFO/blob/master/Readme.md

- Manish Shrestha, cph-ms659

Introduction

This blog discusses their encounter with attacks on their web application project for Large System Development(LSD). I personally found the blog very intriguing as I am passionate about security, good or bad. Good security implementation leads to more research on how it is done and how I can put into practice. And on the other side of the spectrum, it is just fun to find and exploit vulnerabilities of people's hard work.

Recommendation

As interesting as it is to read on the group's encounter battle with web scanners and bot attacks, it lacks the introduction of what they quote as "**muieblackhat**" and "**w00tw00t.at.blackhats.romanian.anti-sec:)**".

For this very reason, I would highly recommend a quick read through

1. Attacks by ZmEu or w00tw00t robots - The Linux Page (a community forum): https://linux.m2osw.com/zmeu-attack

2. Getting a little sick of ZmEu - Phil Riesch (an article) http://philriesch.com/computersecurity_zmeu.html

These two resources gives a fantastic overview of what ZmEu is, what it is doing and the precautions users should take to prevent from future attacks.

On the first recommendation, the community forum, the original post details on what ZmEu is, attack logs and prevention tactics. There are also a few comments posted by the readers providing very simple tactics to prevent from these attacks to be successful. For example, to quote a user named *chuck*: "Do NOT - DO NOT!!! have the letters "admin" anywhere on your system. If you notice every attempted break in has the word "admin" in it." and "If your website is for a cab company in (say) Kansas City there is no need for someone in China or Moscow to access your site."

Moving on to the second article, the author recommends to redirect the request from obvious attacks to an “abuse page” conveying the appropriate message that they don’t take very kindly to attacks on their web server, as he comments these attacks are mostly from script kiddies.

The blog from Group M could also have briefly talked about other types of attacks and vulnerabilities readers should be aware of. This Botnet Wiki, http://jpdias.me/botnet-lab//anatomy/types-of-attacks.html, is a fantastic resource to do just that. It briefly explains what each of the attack is and how it is implemented.

And lastly, we, the students, were asked to test the vulnerability of other group’s web application during LSD lectures using Offensive Web Testing Framework, aka OWTF, https://owtf.github.io/. It is an automated penetration testing tool developed using Kali Linux. It tests every techniques to check and expose vulnerabilities of a web app.

Conclusion

The blog peaked my interest and made me realise what I had missed during our project development. But for an outside reader, it goes into technical details from the beginning and lacks to introduce what they wanted to convey. Whereas for someone who truly wants to defend themselves from these attacks, the blog lacks the proper method of prevention and provides a very basic form of security.