YGN ETHICAL HACKER GROUP

Article

How to be A Security Professional

By

d0ubl3_h3lix

Mon Jan 28 2008

Table of Contents

Introduction

This article may not be a complete guide for you to become a security professional you have ever dreamt of. But I hope it provides you a quick start idea. As far as I see, there are few guides on how to become a hacker or security professional. The reason is because this is intuitive. It means if you learn deeper and deeper into IT security, then you automatically become security professional. Try not to boost the world but to feel the enjoyment of battle of attacking and defending. Please be aware of the job of security professional. It is at anytime risk of being arrested if you do misuse your skills. There is no true anonymity in the Internet. You can’t hide your malicious activities completely. In real world, security issues are often hidden to suppress general public worries. For instance, concerning with Wireless Security, an average administrator might think 128-bit WEP key is stronger than 64-bit one; the true hidden fact is that the security flaw does not rely much on those key size but has to exist due to the fact that Initialization Vector (IV) is transmitted in the plaintext and only 24-bit in size.

Hacker Culture

Hacker culture is one of the prevailing communication styles among hackers in the western. Plethora of styles are out there. If you have time, it's worth to spend some time to study it. You can Google it for hacker culture, or language. Basically you should at least be able to write hacker speak conversion.

E.g. Hacker Culture == > the h4X0r cul+ur3

Initiatives

Script Kiddies ===> HardC0re Hacker ===> Security Professional

a. Level 1 (Script Kiddies)

Hacker Newbies are willing so much to hack. They know only to hack. They know only to penetrate systems using tools they've got freely. Imagine! Think so wisely! This lasts for a few moments. When security holes are patched, they have to take pains to hunt new tools for new victims/holes. They will never end up working with tools. They have no detailed technical ideas why they work with tools.
However, this is a level of Script Kiddies or Click Kiddies - also a level of every advanced hacker has to start from.

To know if you’re Script Kiddies or not, ask yourself ‘To use SQL Injection tool, have I already known what SQL Injection is and what impact it poses on targeted system?’

b. Level 2 (Hardcore Hacker)

Script Kiddies got ideas on working with hacking tools. They started to realize if they know how to code these tools very well, they could easily create new tools which may be far more advanced than they had got. They started to learn some extreme programming and underlying architecture. They knew how the whole system/application works. They got its whole image and got better ideas for exploiting it. At this stage, depending on their dedication, their skills became more and more advanced.

c. Level 3 (Security Professional)

[Note: Because of the fact that I define this stage as highest, please don't misunderstand that security professionals are smarter than hackers. I don't mean that way. I simply mean, if you don't know the knowledge of hacking in details, you can't protect hacking your system. The reason is you have no idea about hacking.]

As they could get all technical know-hows, they then realized how to protect from exploits. At this stage, they started to write defensive-codes for patching vulnerable applications/systems. Level2 and Level3 are like Chess game. Black Hackers beat Security Professionals and vice versa. As you see, hacking and security is a competition of black and white hackers. For example, blackhats find a bug and exploit it to gain access to your system. Then whitehats fix that bug and implement further countermeasures to prevent similar exploits. Again, blackhats study such countermeasures and launch counterattacks. Fighting is never ending.

Specialization

As far as I've seen, hackers live in group. They combine their individual expertise to create extreme hacking. Similarly, in security world, security professionals have their own specialized areas like firewall specialist, network/web/database/IDS/ ...etc.
I don't mean you should learn only area. You should have at least intermediate level of knowledge in all IT Security. It's obvious you can't hack a particular stuff if you don't know it well - [To be an advanced hacker, drop script kiddies' idea which can always hack with tools developed by skilled hackers, though knowledge of using tool is necessary for penetration testing to find known/published vulnerabilities.]

a. IT Security

Security rules all fields of IT in -

- Data & Database (the life of e-commerce applications)
- Web Application (the blood of e-commerce applications)
- Desktop Application (the only income of software industry)
- Network (the only communication medium of today's business)
- Operating System (the only thing we use for everyday processing)
- ... etc

There are much more titles under IT security.

b. Building up and Applying skills

Personally, I believe building up skills and required knowledge is the first step. If you know well how routers work in detail, then you can search in Google:

'Router Vulnerabilities'
'Hacking Cisco Router'
'Attacks/Holes on Router'

Then Google should return router weaknesses in security. Together with you should also learn how to mitigate such risks. In this case, you should keep up with the latest information. Old attack types on newer router provide you fictitious signs, track your actions in honeypot, and finally squeeze your life in court.

Research

Security Professionals are in fact researchers and daily learners. All must do research almost every day.

a. Tool Knowledge

“What is a carpenter without a hammer? Hackers require tools for penetration.”

Practical knowledge in hacking and defensive tools is a must-have for security professionals because they automate such hacking and defensive activities with ease. Before you use such tool, you must strongly understand the underlying exploits and holes. To use WEP cracker, you must first know what WEP is. Or else you’re still in a script kiddies level. Some underground sites are script kiddies sites. Why? Most of them are teenagers and have a lot of time to test one tool after another. They feel proud of themselves cracking or defacing web servers with holes. They have no idea on what the tool is or how it works. They then hunt for next victims to crack again.

To be a security professional, you must be at home in both hacking and defending. You must be skillful in using hacking techniques, tools and exploits. What is better and more desirable, you should do well in how to defend such security-weak systems even before vendors publish patches and fixes. Yes, this is to protect further more

Zero-day attacks. If you can’t do, the business must be stopped entirely and the loss will be indefinite.

b. Penetration Testing

Exploits and holes are being disclosed per daily basis. You need to keep track of them perhaps to protect those you’re being responsible for protection. Maybe the company you are working for use CMS like Wordpress. Then you must aware of Wordpress exploits every day. If your company is using vulnerable version, then you must quickly patch it. We all have enemies. Your company has enemies like competitors and unsatisfied customers. This is your first defensive arsenal.

Second, you must create your own exploits for pen-testing your company applications. Note that not all exploits are disclosed. Hackers with same skillset definitely happen to find vulnerabilities at the same time or so. They usually keep them for their various benefits. So, due to this fact, all system/network administrators cannot always rely on news like vulnerabilities. The only remedy is to proactively watch and guard your networks! Bad guys are not always willing to see your network is being secure.

Conclusion

People that I have found in my country when I began to enter into IT told me that I should choose one key area to be learnt and dedicated for life. This is true for an average IT professional but to be a security professional you must need to know and understand every latest tech both theoretically and practically as possible. If you don’t know and understand what a thing is then how do you penetrate it supposing you want to the pioneer of finding its flaws? If you don’t even know what JavaScript is, then XSS attack method will never mean much for you. Similarly, don’t do SQL Injection unless you haven’t learnt what, how and why of databases. If you don’t know how web application works and flows or worse you haven’t any experience of building web applications, then it is useless if you want to be a web application hacker. If you don’t follow my advice, you’ll always be script kiddies.