The Underground in 2011

by **ninjashell**

ninjashellmail@gmail.com

I. The Underground in 2011

This paper aims to give an overall up-to-update review, evaluation and analysis of the underground scene of black hat hackers and/or cyber criminals. I aim at raising the awareness level in the general public as well as private companies meaning this is for educational purposes only. You may re-distribute freely without changing my name or the content.

II. Black Hats - Attack Methodologies

The emphasis of this section is on the various methodologies used by black hats/cyber criminals (both skilled and "script-kiddie" alike). If you read all the information carefully, I am sure you will improve your security awareness and probably detect security issues within your business/website.

1. Materials

* A computer
* Good Internet connectivity
* Perl/Python installed
* Notepad+
* A browser
* A VPN/Proxy
* A brain

Only these simple "materials" are needed for black hats/cyber criminals to hack into your corporation and steal your clients personal data.(excluding very sophisticated and targeted attacks)

2. A step into their world

To see how we can protect ourselves, we must first understand how attackers "see the world" - what and where is open and how to exploit it for maximum profit/efficiency. In the next section we are going to start a brief penetration test on an imaginary target which will help us understand how a "black hat hack" is done.

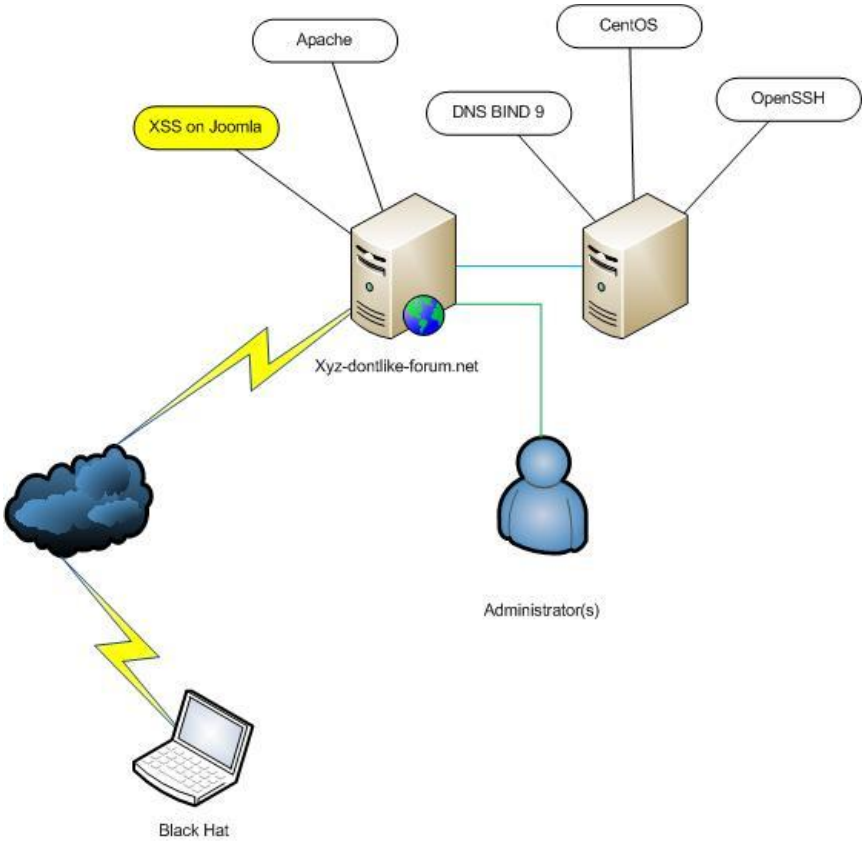
3. Pentest – the black hat way

Let us presume that **xyz-dontlike-forum.net** is our target/victim and we are the black hat. We shall attack this forum because we have been ordered by a client who will pay us good amount of money. Taking this in mind, we will do everything to compromise the target and get to the wanted data by our client. Let's start analyzing the various vectors which a black hat hacker would start to check.

3.1 The first vector is the web application one. One of the things that springs to mind is doing a reverse IP/site to see if it's on a shared hosting. An example tool to check that would be http://www.domaintools.com/research/reverse-ip/ . Afterwards we start to plan our attack against the forum/website itself. Once decided, we can to check in the main page source code for clues what software it is running on the web application platform.(*at the moment we restrict ourselves only to web application layer*) Presuming we have found out that Joomla is used for the main website and phpBB for the forum. It looks as if it's a 2.X version and to verify that we go to **xyz-dontlike-forum.net/phpBB/docs/CHANGELOG.html** to see the exact version. We are wrong. It's a fully-updated which leads us to the idea that the administrator(s) is/are in some-what way security aware (we note that down). Next we look at their main page and start identifying what plugins are they running on Joomla since there are many vulnerable to various attacks… **XYZ-dontlike-forum.net** runs no plugins but instead of that it's on Joomla 1.6 which happens to be vulnerable to XSS(http://seclists.org/fulldisclosure/2011/Mar/157). We simply google, find PoC and get ready… for analyzing the next get-in way. You might ask "Why not attack directly?" As we have noted down there is/are administrator(s) that might not be fooled that easy so we will look for a way in without human interaction. We move onto Google hacking! Before starting that, we simply look in **xyz-dontlike-forum.net/robots.txt** to see if there are any hidden directories and we don't find anything there too. A simple query in the lines of "site:xyz-dontlike-forum.net" exposes all content on the website, if we would like to see all .SQL files we can add "-ext:sql" or "filetype:sql" – all Google dorks can be applied here. We have now decided that the web application vector has one exploitable way and the information it holds – administrators, moderators, forum structure, respected members and all of this we note down…

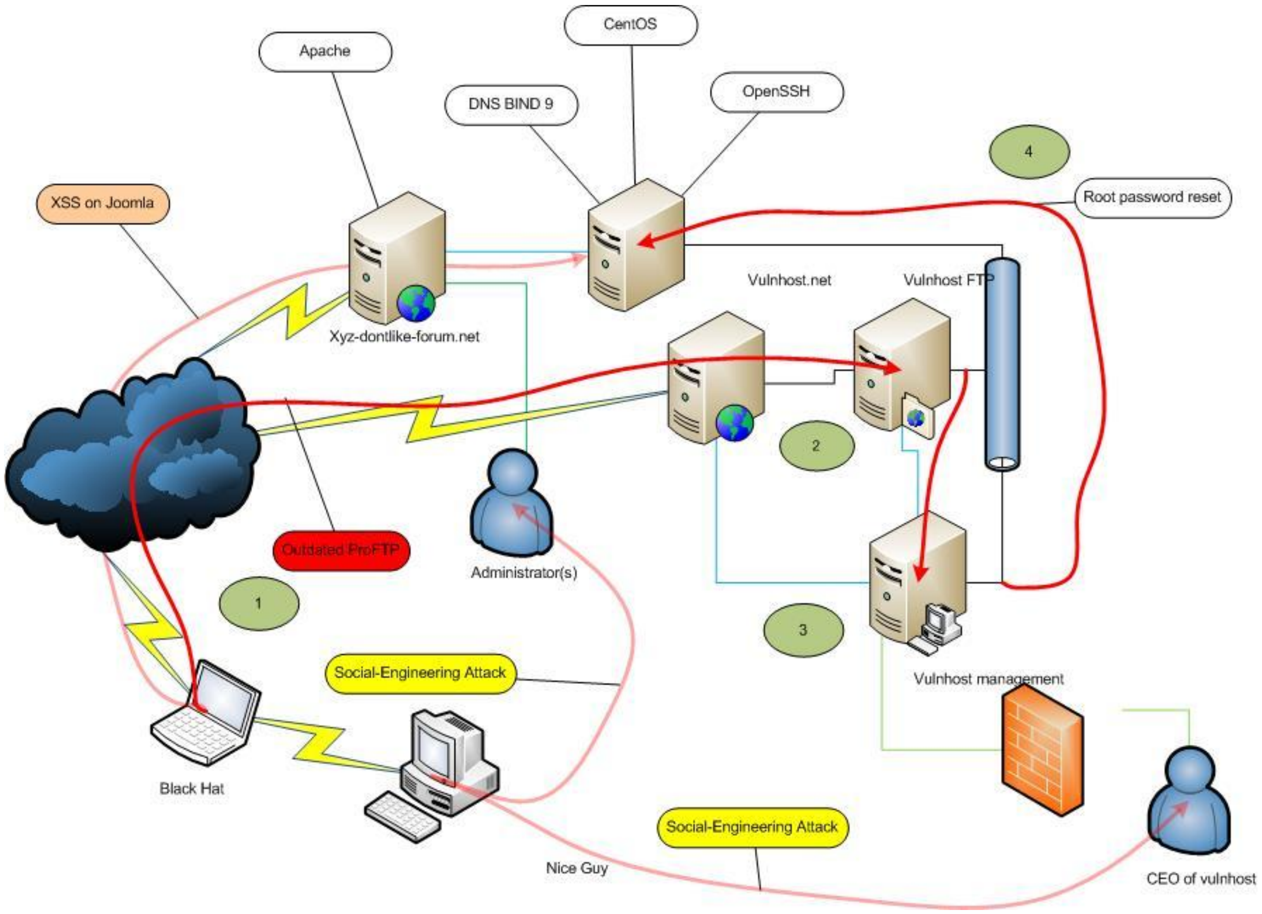
3.2 The second vector is the server/software-sided one. It's simple as running an nmap scan and grabbing the banners, searching for public exploits/PoCs but this fails. The administrator has only a web server with OpenSSH and DNS BIND 9 which doesn't give us, the black hat, much chance of getting in. We have to either use one of our zero-days (if we are getting paid worth the exploit) or simply accept that this vector is of no use to us… EXCEPT the unmasked OpenSSH and Apache information (let's say CentOS).

Let's see the diagram what do we have so far



3.3 The third vector would be the social engineering one – it's the most widely used method. Gathering all the information we can from the interwebs, their forum and people who know the administrator, we find various holes which we can exploit in order to gain his trust… pretending we are "Nice Guy" and then compromise his site. Now here comes a major difference in experienced and "un-experienced" black hats. The elite ones will save this as a backup plan as it requires human interaction (again) and things might go wrong like being exposed which will lead to the administrator(s) being even more alert and maybe securing his/their server even more. Furthermore the success rate is lower than the XSS so we have a backup plan via the third vector.

3.4 Nothing new so far… now let me introduce you to the fourth vector of black hat hackers methodology of penetration – via the hosting. Issuing a quick traceroute (http://just-traceroute.com/), maybe ask http://www.whoishostingthis.com/ plus a whois (http://who.is/) gives us just enough information to identify our victims hosting (e.g. vulnhost). What is next? All those vectors which were above written about can be applied here. There are big chances that you will gain access very quickly via this method which is quite common. The unawareness for security in terms of private companies is still enormous and vastly exploited by hackers. It is as simple as exploit (e.g. outdated proftp), gain support/administrator access and reset the password of **xyz-dontlike-forum.net** . How would this look like?



In this case scenario we exploit the outdated proftp vulnerability, gain access to the FTP server, afterwards escalate ourselves to root/administrator/staff and finally as step 4 – reset the root password on our victims machine. To not look suspicious we chose perfect timing when our victim is asleep/away and email him via the support system of vulnhost that there has been a malfunction on his server and that the root password has been reset to "xyzsystemcrash" without him knowing about our secret backdoor… Now you have his personal data(payment details from vulnhost), his IP and access to his server, what more could you want? Our job is completed and we have received our money.
What if this fails ? Well, you can do the same for the hosting and see if they are resellers, then targeting the "big fish".

3.5 No5 vector

A few months after our attack we are hired once more but this time everything is much more secure and nothing seems to be vulnerable/exploitable. If the fourth vector fails (which is not much likely) we move on to the fifth which is attacking "the third-party" like DNS, SSL certificates etc. Compromising the DNS is sometimes easy, others it needs to be sophisticated attack in order to succeed (compromising host of DNS provider etc.). Such an attack occurred on a well-known carder market.

3.6 The sixth vector I am going to cover, used by black hats, is attacking the repositories of the country in which the server is in. It's simple as it sounds. The technique and vectors can all be applied here as well but what we are really looking for is a serious vulnerability in some application like Apache which will give us access to the repository before it's patched. This requires much patience, luck and fast actions.

3.7 The seventh vector is using DDoS to our evil advantage. Underground hackers have been more than creative and have come up with the simple idea *Big downtime -> Change of host/big expenses.* Changing host means giving the attacker new opportunities(victim moves to another hosting company) but it can also mean big expenses for both sides.

3.8 No8 - Hell

Last but not least attacking the ISP of your victim is always worth the shot. A high level of skill, precision, timing and resources would be needed to attack but singles are the black hats who have managed and successfully completed compromise.

III. Counter-Measures

We have talked about how they "do it" but how can we protect ourselves? Anyone can draw conclusions on their own but I'm going to give some advice how to defend against most of the attacks.

1. Never use shared hosting if it is a company/shop/forum site.
2. Always update your web applications/monitor for updates. (*tip: apply mod_security*)
3. Update your applications such as Apache, OpenSSH, FTP etc.
4. Hide/mask versions of your applications.
5. Always do a background check on your hosting. Ask what do they do to maintain strong security. Check if they are vulnerable.
6. Check your DNS servers if they are vulnerable. If they are, alert your DNS provider.
7. Configure proper IPtables and/or physical firewall.
8. Do not use the same password over and over again.
9. Never trust people on 100% - they are either your true friends or experienced social-engineers.
10. Your security depends on the choices you have made on your own!

IV. Underground business

1. Personal data and a cup of malware

The business around credit cards/dumps/bank logins hasn't changed much but it has surely became easier for cyber criminals to steal personal data and even more for black hats to steal it.

1.1 Compromising C&Cs

The idea behind this paper is NOT to show you how to "pwn" bank trojan control and command(C&C) centers and get what it has stolen but to give out a clear message – if someone wants to make your illegal business simply stop, they will. I do hope this paper will quit those who steal what others have achieved through their life time and get a proper job. Understand that if you are doing something illegal, in the end, you get jailed/owned – this paper gives a relatively easy method for it. Furthermore I am sure that anyone who is interested in fighting cyber crime on their own can benefit – compromising the box, deleting all gathered personal information, getting the IP of the owner and reporting it.

1.2 Materials needed

* One computer
* Good Internet connectivity
* A browser
* One SpyEye 1.2.X or 1.3.X control and command(C&C) center
* Sqlmap (python installed)
* A brain

1.3 The compromise

1.3.1 Identification

First we need to find a command center, right? To do that you can go to carding/black market forums and see who is selling credit cards, bank information etc. and/or SpyEye builder/bins. The social engineering attack can be different from making yourself their/his/hers partner to offering spreading service (this way you gain his BIN and reverse engineer it to see where it's connecting to). Or you can go to https://spyeyetracker.abuse.ch and start pwn'in!

Additional information: SpyEye 1.2.X costed $2,000 with all modules & plugins whereas now it costs much more.

1.3. The attack itself

After we have identified the SpyEye C&C (e.g. **image-hosttter.com/spyeye/**) we need to start pwning it. If you look thorough SpyEye 1.2.X or 1.3.X you will notice multiple vulnerabilities including XSS, CSRF, SQL etc. I will use a vulnerability on frm_findrep_sub2.php (**image-hosttter.com/spyeye/panel/frm_findrep_sub2.php**).
If we go to

image-hosttter.com/spyeye/panel/frm_findrep_sub2.php?id=
we get an error… interesting! But if we try

image-hosttter.com/spyeye/panel/frm_findrep_sub2.php?id=1
it returns "Not found". Next we will launch SQLmap (if you are lazy doing the SQL manually)

```
root@ninjashell:~$ ./sqlmap.py -u http://image-hosttter.com/spyeye/panel/frm_findrep_sub2.php?id=1
```

After it has finished we launch a second attack but this time guessing the path (can be easily guessed by identifying server OS or bruteforcing)

```
root@ninjashell:~$ ./sqlmap.py -u http://image-hosttter.com/spyeye/panel/frm_findrep_sub2.php?id=1 –file
read=/var/www/spyeye/panel/config.php
```

Now check the directory in which the sqlmap.py is in… owned. Now you have the botnets' MySQL creditentials but in order to compromise the box we must upload a shell/get a reverse connection.

1.3.3. Gaining access – uploading a shell

To upload a shell we can either check for the phpMyAdmin or phpmyadmin directory or try logging in by connecting to the port in config.php (3306 by default for MySQL). If you are good at SQL injections you can do it manually and even exposing the current directory (like pwd command). After we have connected in preferred method we issue this query:

```
SELECT *
"PHP SHELL SOURCE HERE" INTO OUTFILE '/var/www/spyeye/panel/ninjashell.php';
```

Now go to **image-hosttter.com/spyeye/panel/ninjashell.php** and see your PHP shell uploaded.

2. Malware business.

As banking trojans get more and more sophisticated their security starts to lack more and more as well. A perfect example is the exploited SpyEye C&C. Authors of exploit packs are also living the big life since many people are buying their "products". What is an exploit pack? A collection of "best" public (rarely 0-days) exploits for Adobe, Firefox, Chrome, IE, Flash etc. which attack your browser and try to infect it with the malware that has been uploaded in the C&C of the exploit pack(e.g. SpyEye bin). A great paper and PoC of how such exploit packs lack any kind of security has been written by Maxe, "Hacking the Skiddies", check it out.
Recently there has been a leak of the latest ZeuS source code which leads us all to the idea that we should be expecting modifications/skids versions of it very soon.

3. Black Hats and their business

Many would ask the question "How do black hats make money?" – well there are quite a lot actually. From hacking e-shops and stealing its credit card database to dealing with private underground contracts for various assignments. Yes, such things do exist. A black hat would usually charge you around $2,500 to even $10,000 per job(depending on the job) – is it worth it? You are the contractor, you decide.
To build up a "strong" image of a black hat you either compromise the biggest underground markets one by one, merge their database into one and build your own market… or you can simply alert the administrators by asking something in return. Afterwards, well, you can only dream for bigger reputation.

To summarize where the bad guys can be used anywhere even
hacking websites to inject iframes => exploit packs => visitors infection => banking Trojan => identity theft

VI. About the author

- Ethical hacker;
- Freelance security consultant/penetration tester;
- Security researcher in the spare time;
- Over 12 years of experience;

You can always email me - ninjashellmail@gmail.com or follow me on twitter **@ninjashell1337**

V. Reference/Interesting

Reverse IP - http://www.domaintools.com/research/reverse-ip/
Who is hosting this? - http://www.whoishostingthis.com/
Who is? - http://who.is/
Traceroute from four different locations - http://just-traceroute.com/
Joomla! 1.6 XSS - http://seclists.org/fulldisclosure/2011/Mar/157
SpyEye tracker – https://spyeyetracker.abuse.ch
Hacking the Skiddies - http://www.exploit-db.com/download_pdf/17067