Simple Web-Hacking Techniques

Written by Nikolaos Rangos / kcope / eliteb0y

With help of this paper one can get information and abilities to conduct targeted attacks against websites and networks.

Normally attacks to computers are run trough automatic hacking. This technique is also called “mass hacking”. It is quite simple and is an old way to hack into sites. One example of mass hacking is the old OpenSSL Remote Exploit which came into release including a scanner. Manual mass hacking is conducted with to glue together parts, which are: A scanner and the actual exploit (mail server exploit, HTTP server exploit etc etc), the program that attacks the site and if it succeeded for example saves the positive hacked entries into a logfile. My experience shows that a scanner like “grabbb” can be reprogrammed to use an actual exploit to not just scan but also hack into the sites (using an IP range and the actual ports).
This paper is not about how to make use of mass hacking. This paper will show you the technique to hack into a site which is taken as a target. This time one cannot use a mass hacking program or script. My experience shows that penetrating into a special site can be more challenging.
Let’s take the example that we want to hack into a dot-com site. First - of course – the sites address needs to be taken as the primary information. Then the second thing is to just ping the domain name of the dot-com site and find out its IP. After that we take a scanner like nmap and look what ports are open. Many times only HTTP and HTTP-SSL ports are open. This makes attacks done on the “infrastructure” harder, because one cannot use exploits. Only HTTP and HTTPS exploits can be used to gain access to the system then. As seen in the past there are those HTTP and HTTPS exploits in the wild. One example is the

Apache mod_jk remote exploit or several exploits against IIS, which are normally patched in the Microsoft patching cycle.

Now if we do not have access to an exploit against the particular server (in its so called “infrastructure” – means: running services) we are limited to the web applications running on top of the http server running through port 80 and 443 (SSL). So at the first stage of exploiting the system we just look at the website and try to guess what program is running as a web application on top of the web server. It is especially important to know if the code running on the web server is open source or self-made. Open Source software can be downloaded and analysed manually and locally on the attackers’ host. If it is self made it’s harder to get the source code what really helps on finding a bug to slip trough and get access.

There are also different programming languages and therefore different programming errors and bugs. There are websites relying on PHP – JAVA – DOTNET or even simple HTML sites.

So at first it’s important to look at the web application and look after bugs contained in it. Sometimes there is a bug in an Open Source application which in its’ specific version has a bug. So the attacker just looks after the exploit and runs it against the web server – as an example running the old phpBB remote exploit against it. Another approach is to use Google search service to find for example uploading scripts, where as an example a PHP, ASP or Java Servlet can be used to upload “shell backdoors“ and execute code on the target host. There are so many different bugs in different applications especially in audited Open Source software that it becomes easier to get into the targeted site.

Now for example let’s say we have a dot-com site we want to hack into, but the web application is running only HTML websites and has only static content installed. If this is true for the attacker he has to look for easier ways of hacking into the system. Here the so called “Reverse IP” technique comes into play. Many dot-com sites are running on web servers which host many sites at a time for the same IP. A good tool is the http://search.live.com search engine by Microsoft. Using this service one can see nearly all websites running on the same IP by commanding the search engine to search for that sites simply by putting a “IP:<iphere>” and click on find. So we know the domain name of the web server and its IP. We look on live search for the other sites hosted on the web server. Many times the websites are not running on “dedicated” servers. If this is the case and the web server hosts more websites, the attack vector becomes huge because of the other installed sites on the same IP. Now the only thing to do is to look after an easy target site that contains a remotely exploitable bug. The attacker clicks through the sites for this IP and pings the domains to verify that they are really running on the exact same system with the same IP. Now the different exploits and exploit-scripts against web applications are easier and more effective to use because of the huge attack surface we now got because of the sites hosted on the same system. Let’s take the example that Site 1 is the targeted site and Site 2 is running on the same IP and system. Site 2 has an upload scripts installed or something similar and easy to use to get shell access. The attacker exploits Site 2 and gets a shell, reverse shell or something similar to execute commands on the web server. By hacking with this technique often plain text passwords can be gained for e.g. SQL or maybe a running FTP server. The main goal now is to get credits to the Site 1. Site 2 will often have read access to Site 1 but no write access. Now local root exploits namely "privilege escalation" exploits come into play. Often kernel bugs on Linux or Windows hosts can be attacked with the appropriate tools and exploits. When the attacker has gained the required credits using the local root exploit he/she has complete control not only of Site 1 now, but all other sites hosted on the very same system. Now he can penetrate deeper into the network, read mails of the paying users on the site, install web application backdoors which are modified code to log login attempts, install a rootkit or a patched SSH backdoor etc etc. There are many things the attacker can do from now on. If we are confronted with a dedicated server where only one site runs on it and only HTML static content and all ports are closed we have to look for other possibilities to gain root - say "SYSTEM" - access. One thing is to guess the passwords of the administrator by hacking into a very near server to which the administrator has access. Let's take the example of a university site. Universities most times have a great IP range assigned to them. A quick look on http://www.ripe.net for example can reveal information about this IP range. This time the attackers' goal is to hack a server which is residing closely to the IP of the targeted site and the same assigned address space. If the attacker gains root access on this particular system he can for example crack the passwords of the administrator. Sometimes there are the same passwords for the closely server and the server with is actually attacked. Passwords include SQL passwords and E-Mail Passwords. What can be helpful here are Kernel Memory Disclosure exploits which often reveal sensitive information of the whole system in just only one file dumped off the running host. Armoured with this information it is easy to get close to the targeted site or even open more ways to hack into accounts which run near or even far away from the system, because the information becomes far enough to get access to other systems (hopefully also to the targeted site) and gain root access there. It is important to keep stealthy when doing these tasks. In my experience sites which are outside of the attackers' country are less sensitive than sites inside the attackers closely range and city. This is because if the administrator catches you he cannot hurdle the law of his own country and catch you in the other country. If you do things with non-legally intensions the risk is of course larger because you can be wanted internationally. With this technique we got access to a closely site of CIA.gov what shows how effective this techniques are.