BackTrack 5 tutorial: Part 3 – More on exploitation frameworks

Karthik R, Contributor

You can read the original story here, on SearchSecurity.in.

BackTrack 5, the much-awaited penetration testing framework, was released in May 2011. This third installment of our BackTrack 5 tutorial explores tools for browser exploitation such as theft of credentials, Web privilege escalation and password recovery. This part of our BackTrack 5 tutorial also provides an insight into automated SQL injection using DarkMySQLi.

Stealing browser credentials

Previous instalments of the BackTrack 5 tutorial explained ways to exploit the target using various payloads. Now, we shall use the Windows attack modules of the Metasploit framework to steal the browser credentials stored in Mozilla Firefox running on Windows XP. A third-party tool called Firepassword will retrieve all the stored passwords from the Mozilla Firefox browser on the target.

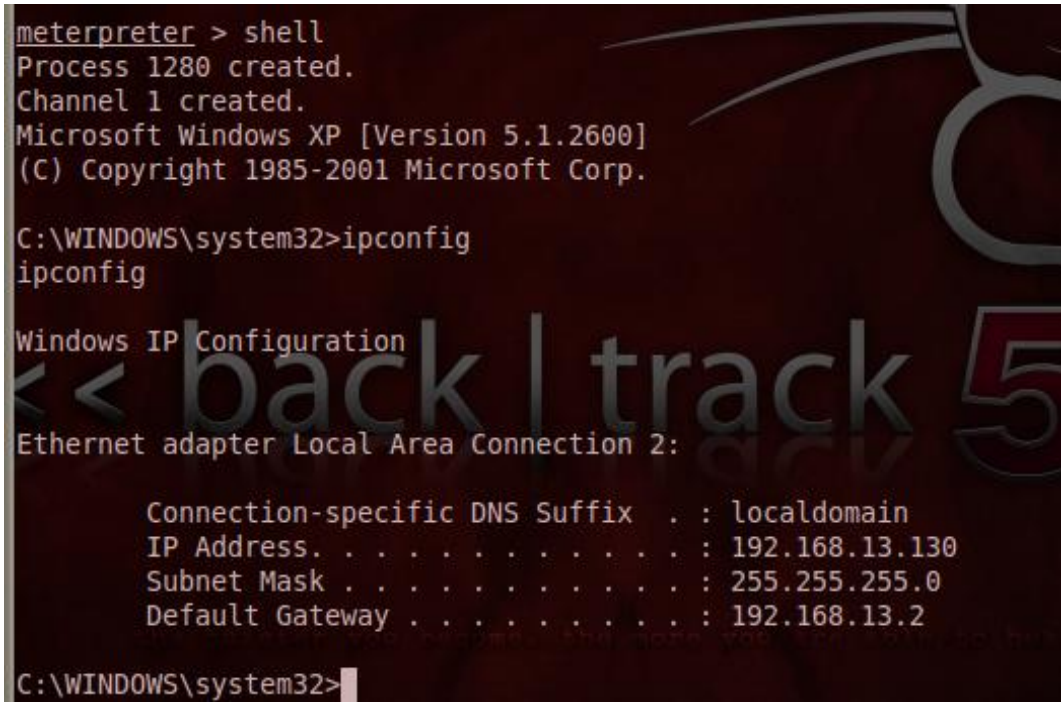

Figure 1: *Compromised system, Windows XP*

We shall use the famous WinXP RPC DCOM exploit to compromise the system, spawn a Metasploit shell and carry out the post-exploitation activity. If there is a master password for Firefox, it's important that we retrieve that first, in order to view the other passwords. Usually no master password exists, hence this enables us to retrieve the stored credentials.

Pen- tester's perspective on stealing data

The goal of a pen-tester as well as a black hat hacker is the same, namely, to infiltrate the network and surreptitiously steal data. However, while a black hat sells the data or uses it for malicious intent, a pen-tester reports the stolen data to the organization for which he is carrying out the pen-test, with utmost confidentiality, integrity and accountability.

Information that can be tracked by data theft includes personal information that can be used for social engineering attacks; credit card or other financial details; and, receipts and bills or sensitive company information in the email inbox.

Thus, checking for any data that can be stolen is an important phase in pen-testing, to give a complete and honest report to the organization. Figure 1 shows the compromised target. Here, we upload firepassword.exe to steal the stored Firefox passwords.

Figure 2: *Uploaded firepassword.exe to the target*

Use the *upload* command to execute the task in the meterpreter shell.

Once the Firepassword is uploaded (Figure 2), the data is as seen in Figure 3.

Figure 3: *Saved usernames and passwords, using Firepassword.*

Running firepassword.exe shows the passwords in the system. But there is a catch here. It's useful to check your user-level access, once you gain access to a system. In the example explained for this BackTrack 5 tutorial, access to the compromised Windows XP box is with the 'system' privilege, but for Firepassword to run one needs to have 'administrator' privilege. Hence, change the user level to administrator by the following method.

1. Use the *ps* command in meterpreter to list the processes with their PIDs, and look for explorer.exe or a process that has administrator-level access.
2. Now copy this PID and use the *steal_token* command to change the user level to administrator.
3. To ascertain your current user access level, type the *getuid* command in the meterpreter shell.

Once you are the administrator, run firepassword.exe by opening a Windows shell in meterpreter and check out the saved password as shown in Figure 3.

For this BackTrack 5 tutorial, note that this procedure works only if you know the master password for the Firefox browser. Nine times out of ten the master password won't be set, and credentials can be extracted. But, luck may not always favor the brave.

There are similar third-party tools for extracting passwords from other browsers as well as chat clients.

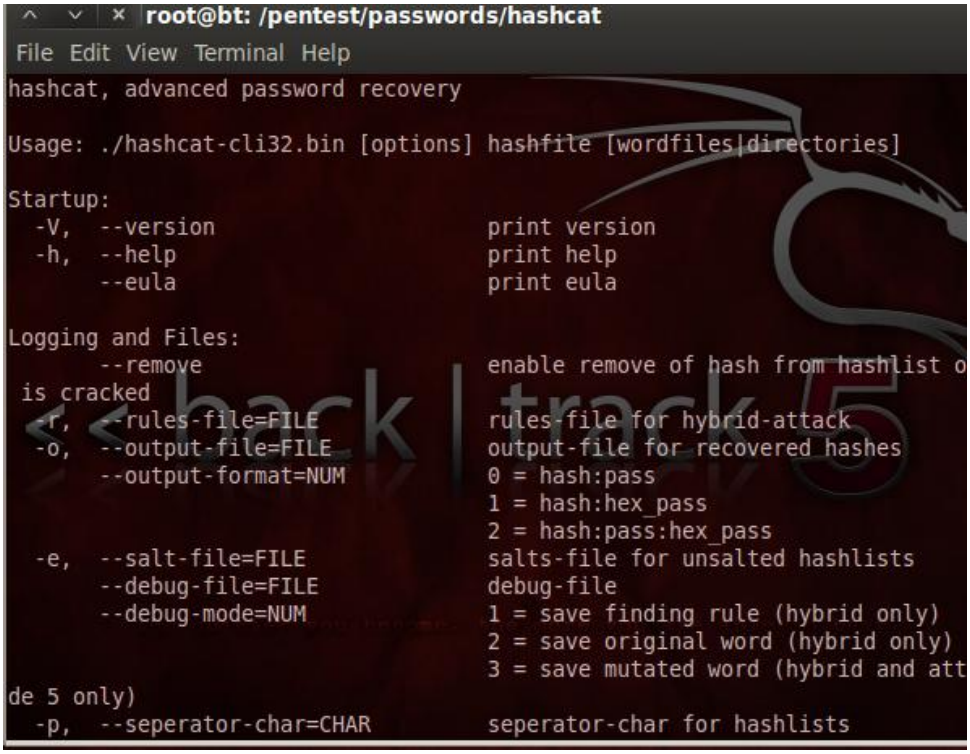

Figure 4: *Hashcat commands on BackTrack 5*

Hashcat on BackTrack 5

Hashcat is a free, advanced, multi-platform, multi-OS password recovery tool. The platforms supported include CUDA, OpenCL and CPU, among others.

In this BackTrack 5 tutorial, Figure 4 shows the usage syntax for Hashcat with an explanation for each option. The options are classified as follows:

- Startup operations.
- Logging and file operations.
- Managing system resources.
- Types of attacks, including brute force, table lookups and permutations.

Pen-tester's perspective on escalating privileges

A penetration tester mostly gains access at a lower access level. Subsequently, it's the tester's job to uncover local vulnerabilities, and gain a higher level of privilege as administrator. This is critical for obtaining rights required to perform the required security assessment. The tools under "Backtrack > Privilege escalation > Online attacks/Offline attacks" have been developed keeping this aspect in mind.

Most operations in Windows can be carried out as 'administrator', but for a few, the higher 'system' privilege is required. BackTrack 5 has tools such as meterpreter to facilitate such escalation of privileges.

BackTrack 5 for SQL injection

SQL injection ranks number one in the OWASP Top 10 Web application vulnerabilities. It can be performed either manually or with automated tools. The manual method is tedious and time consuming, whereas automated methods are faster, user friendly and more effective. Havij is one such tool for automated SQL injection.

BackTrack comes with DarkmySqli that performs automated SQL injection on the target.

The syntax is as follows:
```
python DarkMySQLi.py –u http:// <target website>
```

A full scan facilitates extracting the username and password of the target, using the above command in the console. The path to access it in BackTrack 5 is
`/pentest/web/DarkMySQLi`

Truth behind automated pen-testing

Many vendors sell automated pen-testing products using the "cheaper, faster, more accurate" pitch. Given cost and time constraints, such offerings are of course desirable. But there is also a view that automated pen-tests provide a false sense of security, as their scope is narrow and excludes reviews of IT architecture and security policy. Each individual needs to evaluate the pros and cons of either approach, based on the specific needs of the organization.

In this BackTrack 5 tutorial we have seen Web exploitation frameworks, stealing of browser credentials using third party tools, and uploading them to the remote system under compromise. Future BackTrack 5 tutorial installments will cover other aspects of the information security domain, including forensics and reverse engineering.

Do not miss Part 4 of our BackTrack 5 tutorial which details how to perform stealth actions.

About the author: ***Karthik R*** *is a member of the NULL community. Karthik completed his training for EC-council CEH in December 2010, and is at present pursuing his final year of B.Tech. in Information Technology, from National Institute of Technology, Surathkal. Karthik can be contacted on rkarthik.poojary@gmail.com. He blogs at http://www.epsilonlambda.wordpress.com*

You can subscribe to our twitter feed at @SearchSecIN. You can read the original story here, on SearchSecurity.in.