

Penetration Testing on FTP Server

Mohammed F. Abdulqader

Kirkuk University/ College of Engineering–Electrical Engineering Dept.

ABSTRACT

This project is focused to perform penetration testing on the FTP server. First the Penetration test, Penetration tests are a great way to identify vulnerabilities that exists in a system or network that has an existing security measures in place. A penetration test usually involves the use of attacking methods conducted by trusted individuals that are similarly used by hostile intruders or hackers. FTP or File Transfer Protocol refers to the standardized network protocol used to transfers files and data from one host to another over the internet or TCP based network such as your internet server to host network. FTP is ideal for those who want to be able to transfer large files quickly across a network using a program such as CUTE FTP, which is a free FTP application you can download. This project focuses on the FTP accounts, in the year which allows us to perform brute force attacks.

1. INTRODUCTION

This project is focused to perform penetration testing on FTP Server. Penetration testing is often done for two reasons[1]. This is either to increase upper management awareness of security issues or to test intrusion detection and response capabilities. It also helps in assisting the higher management in decisionmaking processes[2]. The management of an organization might not want to address all the vulnerabilities that are found in a vulnerability assessment but might want to address its system weaknesses that are found through a penetration test[3]. We will perform all the phases of penetration testing to check the scope of attacks that can be performed on FTP Server. We will start by Information Gathering, where we will try to find as much information as we can about the target website, followed by performing a port scanning, to confirm about the open ports specifically, port 21[4]. In last phase of penetration testing, we will perform brute force attack on ftp account of a website which doesn't block user, when he attempts different combination of usernames and passwords[5]. We take the advantage of this kind of vulnerability which doesn't limit the number of attempts [6]. This project will be focused on FTP accounts, which in general allow us to perform brute force attacks.

2. PLANNING AND PENETRATION

This project focuses on performing brute force attack to break the username and password. In general, websites are administered via ftp accounts, so it becomes important to perform security assessment on FTP Accounts. Limitations with these ftp accounts is that; they don't block the access after some numbers of attempts are tried. Taking advantage of this vulnerability, we will use HYDRA software, which is part of password cracking online attacks in backtrack, penetration testing distribution. We have the option of using default wordlist present in backtrack for usernames & passwords or else as per policy, we can get maximum combination of usernames & passwords which uses alphabets, numbers as well as special characters. Security Consultants will also get to know, how their company FTP and other protocols can be remotely accessed through unauthorized process.

Assessment Agreement

The assessment agreement will include:

Scope

We had to follow external approach as we need to find the chances of breaking usernames & passwords with the given wordlist. So we follow Black Box approach as this has to be done stealthily but at the same time with pre-approved permission.

Table 1: Penetration Tests Scope

Penetration Testing Scope	
In Scope	Out of Scope
1. Router 2. Web Server 3. Host Server 4. FTP Accounts	1. VoIP 2. Mobile Device 3. DMZ 4. Zigbee

Table 2: Penetration Testing Tools Scope

Penetration Testing Tools Scope	
In Scope	Out of Scope
1. Hydra 2. NMAP 3. Backtrack 5R 4. Virtual Box	1. Metasploit 2. W3AF 3. Core Impact 4. SQL map

Deliverables

Table 3: Deliverables

Deliverable	Description	Acceptance Criteria
Presentation	Electronic Document	As defined in scope, vetted by Team Lead, approved by Project Manager
Report	Electronic Document & Presentation	As defined in scope, vetted by Team Lead, approved by Project Manager

Team Members

Table 4: Team Members

Penetration Team Project Members	
Role	Responsibility Description
Project Manager	Gregory Funk – Manage team, ultimately responsible for success of project.
Project Sponsor	Anthony Barba – Handles escalated personnel issues, represents project and team to third parties.
Team Members	Name.
Stakeholders	Wilmington University, IT Department Heads

Penetration Testing Team Members

Table 5: Penetration Testing Team Members

Engineer	Specialty	Duty	Email	Phone Number	Alternate
Gregory Funk	Project Management, Wireless Penetration	Project Manager	gregoryfunk@wilmu.edu	1-800-943-225	Anthony, Barba
Nanda Kishore	Database, Email, Web Server Penetration	Engineer	vundecoden@wilmu.edu	203-400-5829	Gutlapally, Srikanth
Srikanth	Network admin	Engineer	Sri.1852@wilmu.edu	2016065349.	Peter, Haynes
Dhanunjay	SQL database specialist	Engineer	Dhanu@wilmu.edu	201-224-1253	Patrick, John
Vaishnavi	Additional support team	Engineer	vaishnavi@wilmu.edu	201-3333-5829	Will, turner
Syed	Addl. Team support	Engineer	syedmohammed@wilmu.edu	201-777-8253	Kirk, Patrick

Escalation Path All the problems and unethical data would be reported to our manager Mr. Gregory Funk and to the team leaders at participating teams.

Date of the test 1st December, 2014.

Start time 09:00am.

Miscellaneous Points of Contact

- Law Enforcement (City, State, County): Wilmington State Police, Delaware – 19702, USA. Ph# 919-564-5656.
- Internet Service Provider: Comcast Services, 2nd Floor, Patrick Avenue, Newark, Delaware.
- Consultants: Rosie Johnson Consultants, Dover, Wilmington.
- Subject Matter Experts: Panel of heads of departments, Wilmington University.
- Lawyers: Andrew Augustine advocates services, Newyork.

Retest Policy A total of 3 recurring tests are performed to maintain accuracy and to decrease errors.

Working conditions Wilmington University using Dell personal computers.


Non-disclosure Agreement

Liability Insurance or Approval in Writing ISO insurance company New York.

Assessment This phase emphasize on performing penetration testing on FTP Accounts using Black Box Testing Approach.

Information Gathering

As this is black box testing we will perform passive information gathering on target website. We will be using net craft, which is one of the free utility to display what services are running on the web server running our target website. By performing information gathering, we come to know that demo.wftpserver.com is hosted on Windows Server 2003 and is using Wing FTP Server.

Site	http://demo.wftpserver.com	Netblock Owner	WebNX, Inc.
Domain	wftpserver.com	Nameserver	ns3.pairnic.com
IP address	216.18.195.46	DNS admin	root@pair.com
IPv6 address	Not Present	Reverse DNS	216-18-195-46.vps.rashost.com
Domain registrar	pairnic.com	Nameserver organisation	whois.pairnic.com
Organisation	Ftp Server, Hang Zhou, Hang Zhou, Zhe Jiang, 310018, China	Hosting company	WebNX.com
Top Level Domain	Commercial entities (.com)	DNS Security Extensions	unknown
Hosting country	 US		

☐ Hosting History

Netblock owner	IP address	OS	Web server	Last seen Refresh
WebNX 530 W. 6th St Suite 701 Los Angeles CA US 90017	216.18.195.58	Windows Server 2003	Wing FTP Server/3.4.3wftpserver.com	16-Apr-2010
WebNX 530 W. 6th St Suite 701 Los Angeles CA US 90017	216.18.195.58	Windows Server 2003	Wing FTP Server/3.4.2wftpserver.com	14-Apr-2010

Figure 1: Black Box Testing

Active Information Gathering using Metasploit Auxiliary Module, We will use Metasploit auxiliary/scanner/ftp/ftp_version to detect the FTP version of software.

```
msf auxiliary(ftp_login) > use auxiliary/scanner/ftp/ftp_version
msf auxiliary(ftp_version) > set RHOSTS demo.wftpserver.com
RHOSTS => demo.wftpserver.com
msf auxiliary(ftp_version) > run

[*] 216.18.195.46:21 FTP Banner: '220 Wing FTP Server ready...\x0d\x0a'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(ftp_version) >
```

Figure 2: Metasploit Auxiliary Module

Network Mapping

Alternately, we can perform nmap scan on our target website and find out, whether FTP service is running or not, also we can check whether port 21, default port is open or not.

```
RX bytes:2035000 (2.0 MB) TX bytes:2035000 (2.0 MB)
root@bt:~# nmap demo.wftpsrv.com

Starting Nmap 6.01 ( http://nmap.org ) at 2013-11-19 01:11 EST
Nmap scan report for demo.wftpsrv.com (216.18.195.46)
Host is up (0.27s latency).
rDNS record for 216.18.195.46: 216-18-195-46.vps.rashost.com
Not shown: 946 filtered ports, 49 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
25/tcp    open  smtp
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 278.77 seconds
```

Figure 3: NMAP port scanning shows us that, port 21 is open and running ftp service

Vulnerability Analysis

We will do Vulnerability Scanning with Nessus to find out what are the vulnerabilities associated with FTP Server.

[illegible]

Figure 4: Vulnerability Scanning with Nessus

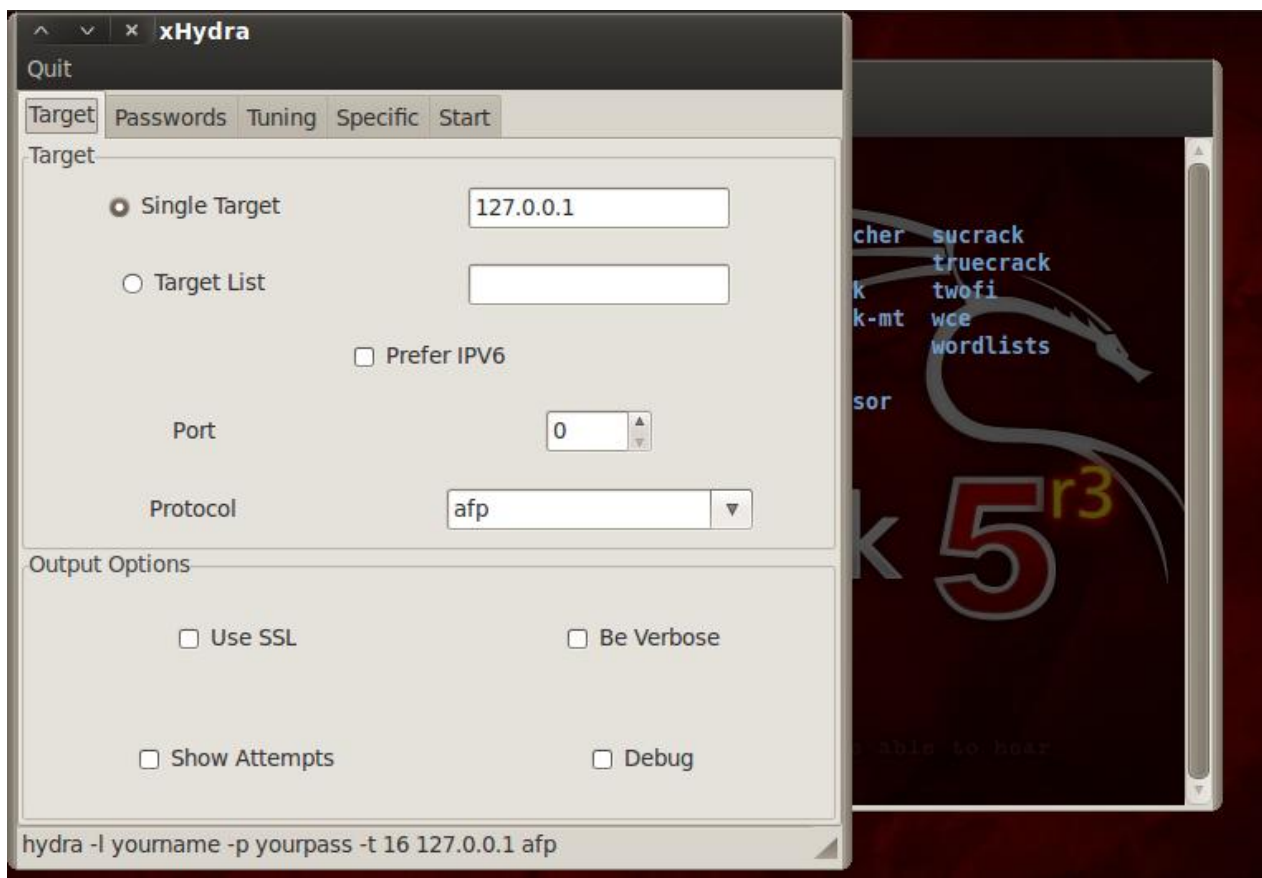
Table 6: Vulnerability Details

System	Vulnerabilities	Exploit	Exploit Description	Exploit Source	Ranking
Wing FTP Server running on Windows Server 2003	Vulnerability in Wing FTP Server, which allows performing number of attempts to FTP Login.	Auxiliary/scanner/ftp/ftp_login_enum - Brute Force attack using HYDRA- GTK	This HYDRA software will help us to attack to perform brute force attack until we get the actual username. We Will also use Metasploit auxiliary – scanner/ftp/ftp_login	Password Cracking Directory in Backtrack and Metasploit Auxiliary Modules	Good

Penetration Testing

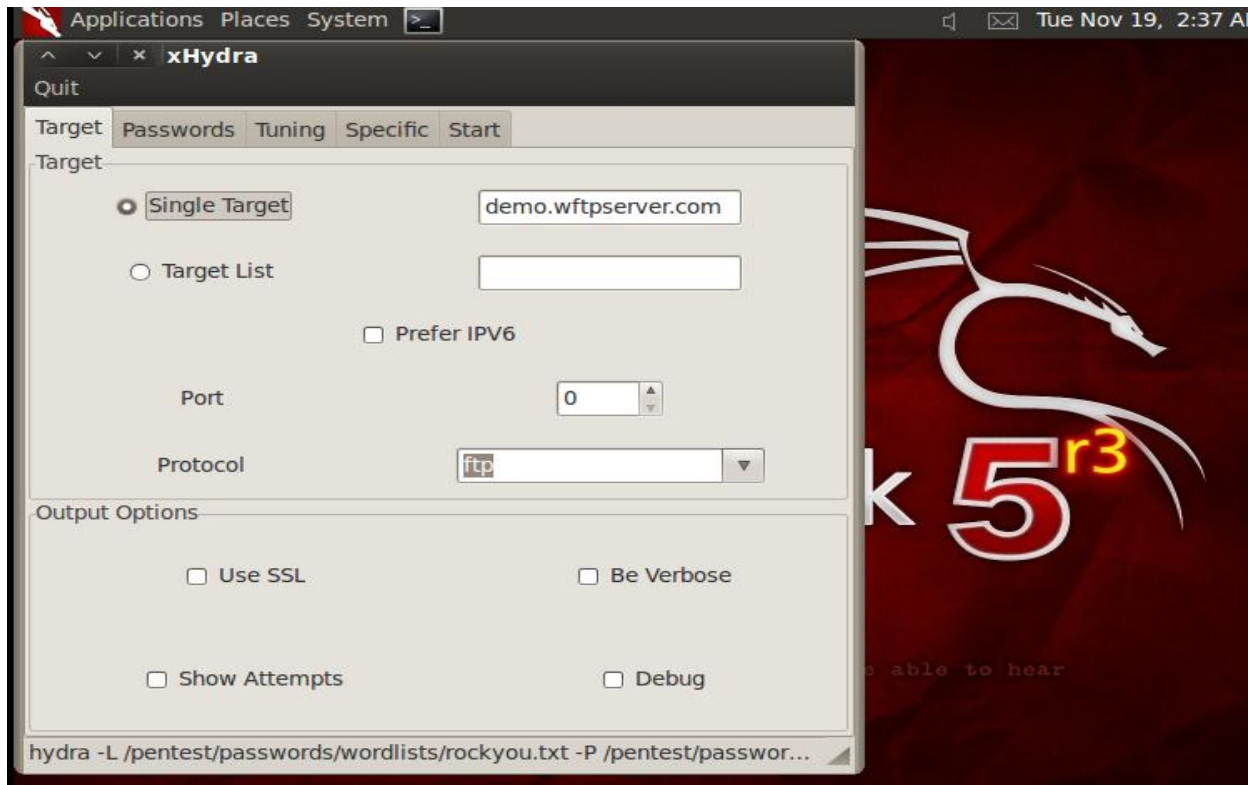
We will start using GUI version of HYDRA for breaking usernames & passwords of FTP Account and to confirm the results what we get will also use Metasploit Auxiliary Module-scanner/ftp/ftp_login.

Step 1: Opening Hydra-GUI, we have 2 options of opening this software, one from Menu other from command line terminal.

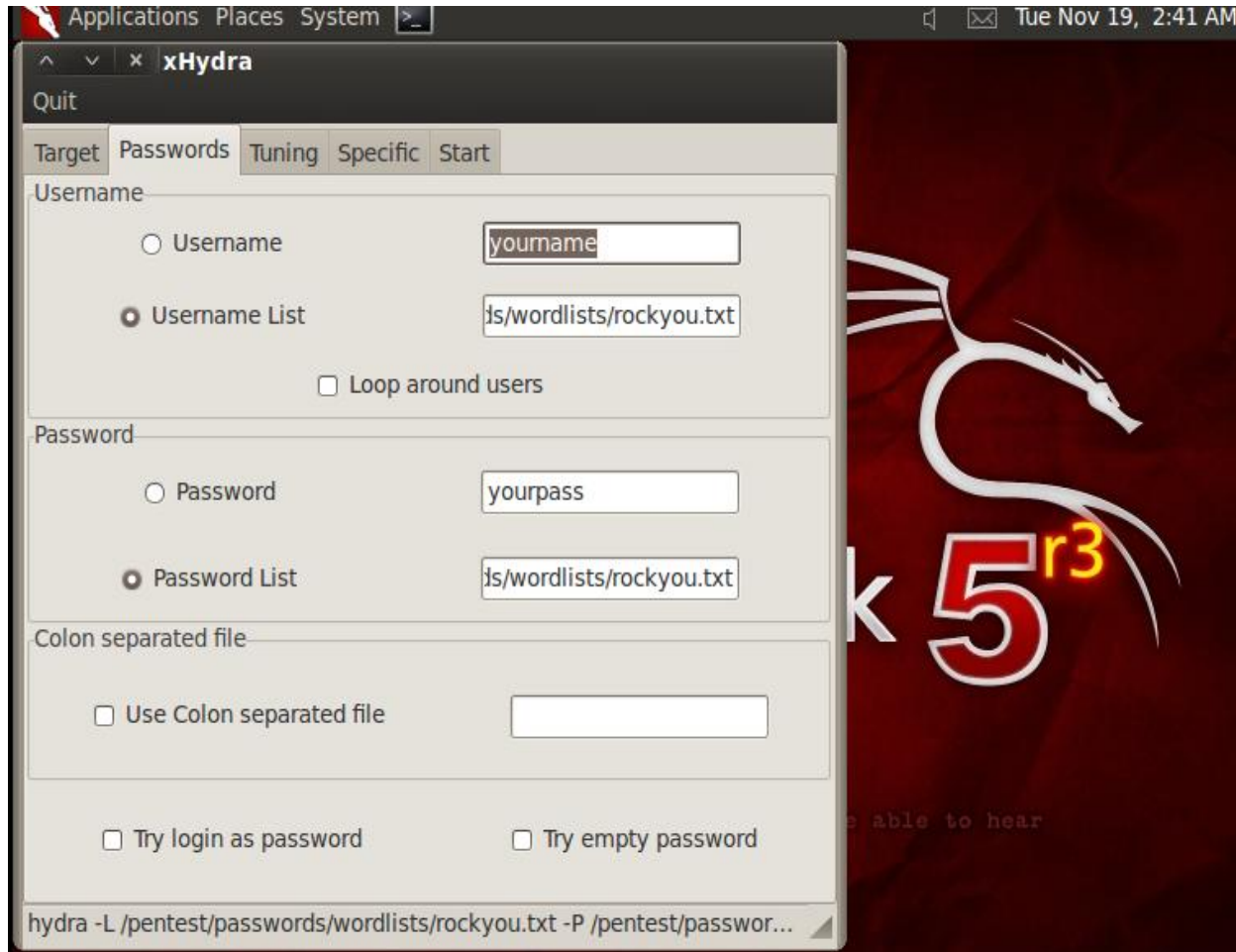


Step 2: We can also run HYDRA via command line terminal: `hydra -l username -p password -t 16 192.168.2.2 ftp.`

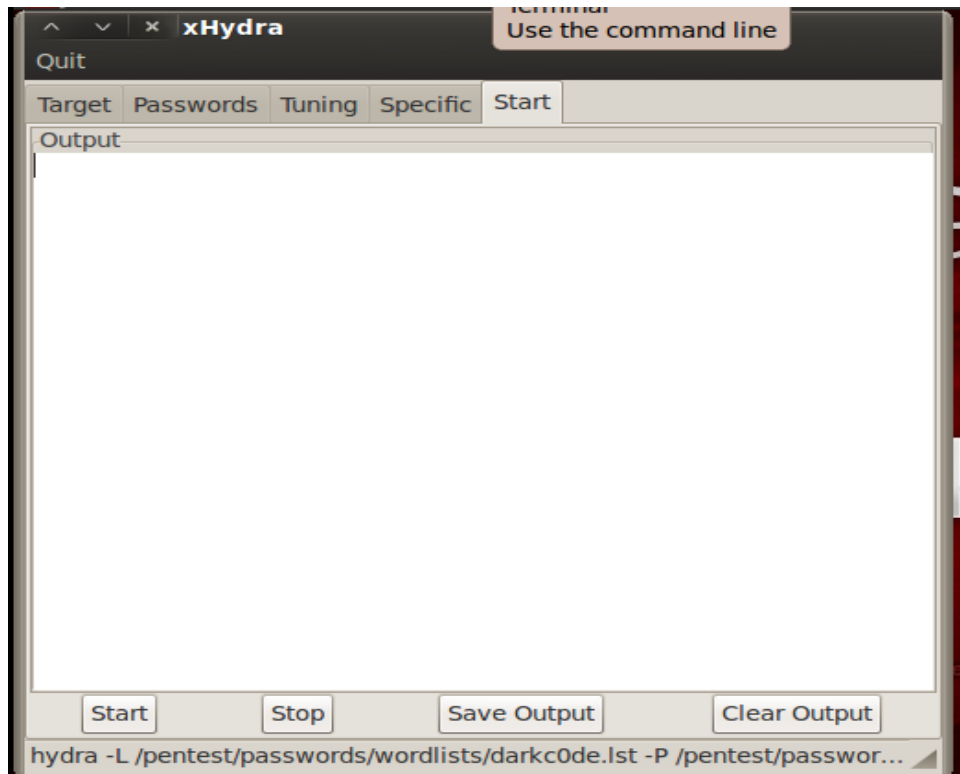
Step 3: Specifying FTP account details:



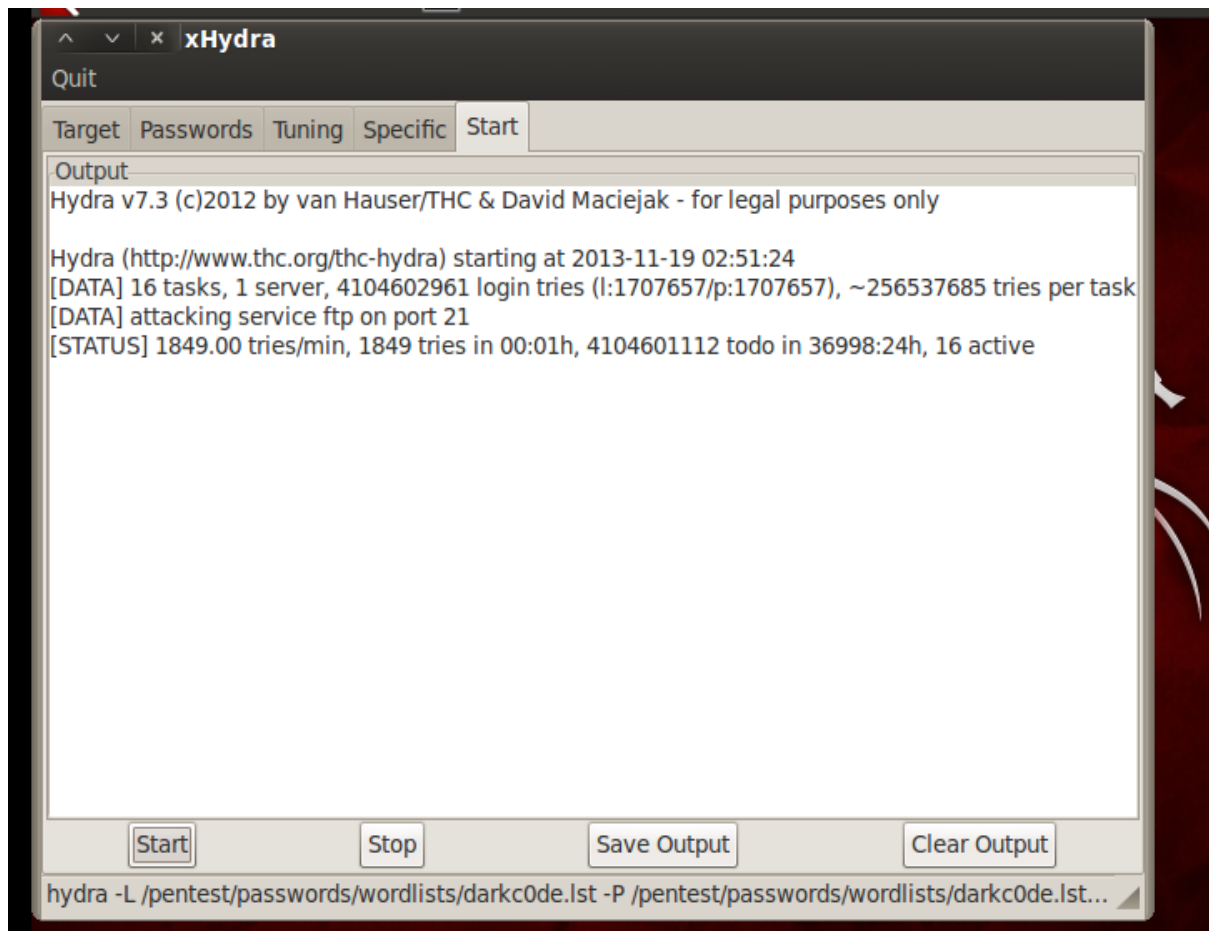
Step 4: We will specify the location of usernames and passwords files location, here we are using default wordlist present in backtrack - /pentest/passwords/wordlists/rockyou.txt. Although we can create or download wordlist dictionary as per requirement, which includes alphabets, numbers and special characters:



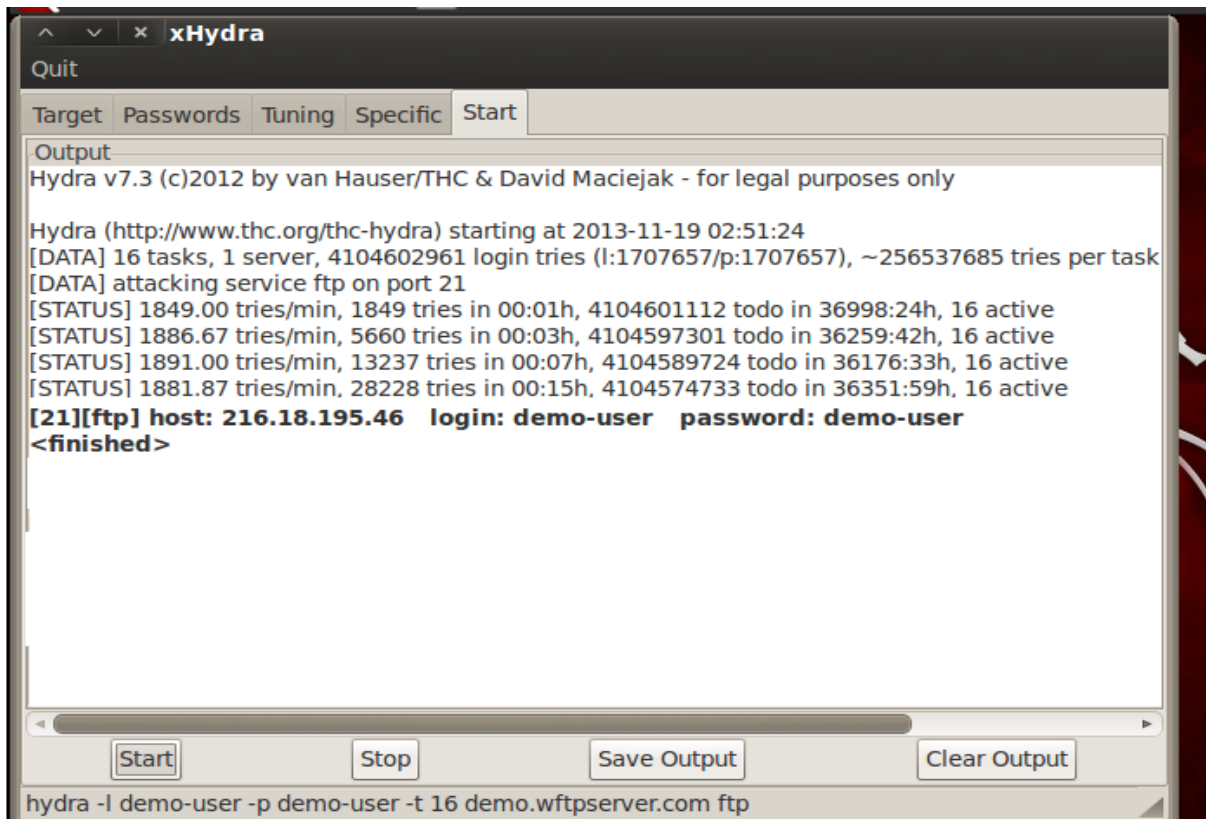
Step 5: After specifying the password and username file, we will move to the last section- start which will start performing brute force attack:



Step 6: HYDRA Attempting to Crack the combination of usernames & passwords:



Step 7: HDYRA-gtk successfully breaks the username & password:



Penetration Testing on FTP Account using Metasploit Auxiliary Module to check whether the FTP Credential we got through Hydra is valid or not.

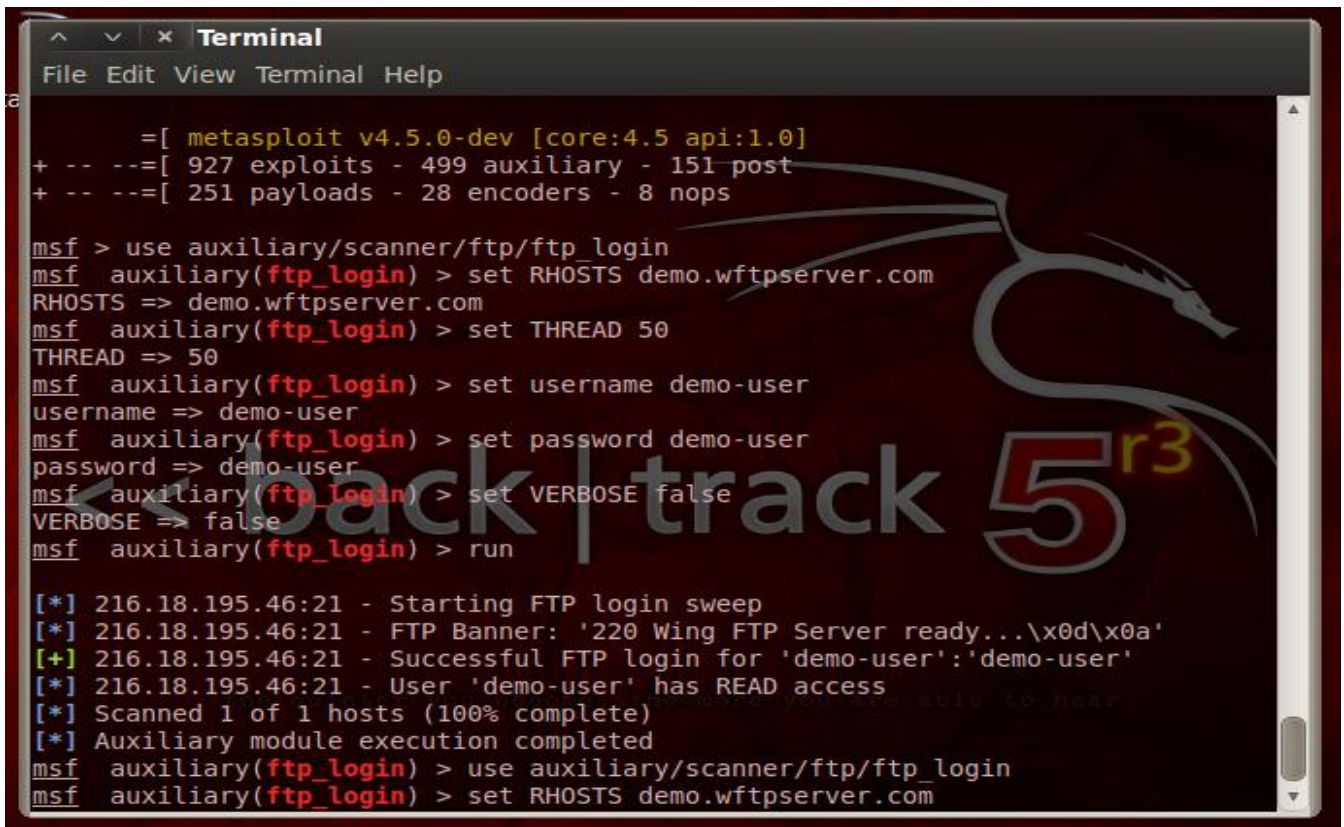


Figure 5: Result shows us that, username & password have been successfully cracked

3. CLOSING ACTIVITIES

Reporting

The report attached has the detailed procedure with all the screen shots in sequential order detailing the procedure. The method we used is very effective and accurate; this method employed by is what which separates us from other companies.

Follow-on Actions

The entire data was cleaned up, systems were wiped off. We also notified law enforcement and the Internet Service Provider and stakeholders that the penetration test is concluded. Also we destroyed the information and data gathered during the process. We are also happy to inform that no unethical incidents, physical or cyber happened during the pentest process.

Archiving

The procedure and final results would be stored with us for future analysis.

REFERENCES

- [1] P. Engebretson, "The Basics of Hacking and Penetration Testing", 2011. (GoogleBooks, General Internet site)
- [2] D. Maynor, "Metasploit Toolkit" for Penetration Testing, Exploit Development, and Vulnerability Research, 1st Edition, 18 Sep. 2007, pp. 350. (Book style)
- [3] R. Baloch, "Ethical Hacking and Penetration Testing Guide", Paperback – Import, 28 Jul 2014, kindle edition with free application, pp.94-164. (Book style)
- [4] J. Scambray, S. McClure and G. Kurtz, "Hacking Exposed 2nd Edition", 20 Nov. 2001, pp. 25-29. (Book style)
- [5] M. Sutton, A. Grenne and P. Amini, "Fuzzing: brute force vulnerability discovery", Paperback – Import, 29 Jun. 2007, pp. 32-40. (Book style)
- [6] J. O'Gorman, D. Kearns, D. Kennedy and M. Aharoni "Metasploit - The Penetration Tester's Guide", July 2011, pp. 328, ISBN: 978-59327-288-3. (Book style)
- [7] S. Kiyota, "Creating an Integrated Internal and E-Business Information Security Architecture", 2001, pp. 66-68. (Book style)
- [8] R. E. Haeni, "Firewall Penetration Testing", the George Washington University, 1997, pp. 77-80.
- [9] W. Pritchett and D. D. Smet, "Backtrack 5 Cookbook", Paperback, 21 Dec. 2012, pp. 45-47. (Book style)
- [10] E. S. Schetina, K. Green and J. Carlson, "Internet Site Security", 2002, pp. 400-417. (Book style)
- [11] Russell Square, Ltd 2015, 44 London, WC1B 4JP, +44 (0) 20 7307 5001. (PDF, General Internet site)
- [12] <https://www.thc.org/thc-hydra/>. [Accessed: Sept. 12, 2015]. (General Internet site)
- [13] http://www.backtrack-linux.org/wiki/index.php/Basic_Usage. [Accessed: Nov. 22, 2015].
- [14] <http://www.backtrack-linux.org/forums/showthread.php?t=18072>. [Accessed: Jul. 9, 2015].

AUTHOR

1. Mohammed Fakhruddin Abdulqader:



Mohammed Fakhruddin Abdulqader: Received B.Sc. in Computer Software Engineering from Technical Faculty Kirkuk / Kirkuk-Iraq in 2003 and M.S. degrees in Computer Engineering from Sam Higginbottom Institute / Allahabad-India, in 2014. During 2004-2006, he worked as an engineer in Ministry of Kirkuk University, then in 2006 joined to the Engineering College / Kirkuk University. He now lecturer in Engineering College / Kirkuk University / Kirkuk-Iraq and, the responsible of the Internet & Computer Centre in the College.