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 GiovÉnni 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 Cialdini's Six 'Weapons of Influence'



* + 1. Reciprocation



|  |
| --- |
|  |
| "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. |

* + 1. Commitment and consistency
    2. Social proof

Liking

* 1. Authority
  2. Sca rcity

## Social Engineering TTPs

|  |
| --- |
| Spear phishing |

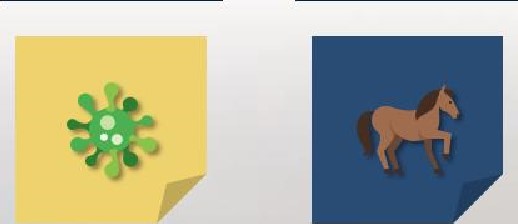
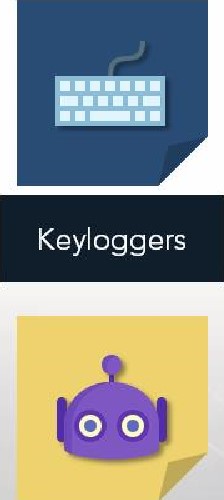
Tailgating

Phishing Smishing 

# 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

 Spyiuare 



Steal

login

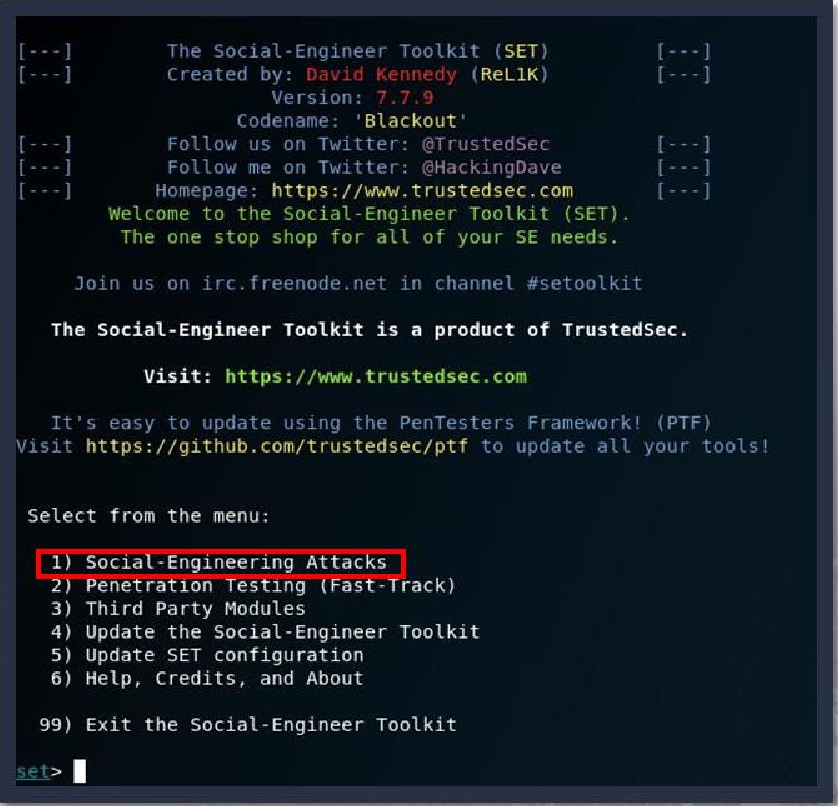
credentials

 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 a Created by TrustedSec  Python-based

* Open-source
* Penetration testing framework
* Social engineering attacks  Phishing Emails

 Various custom attack vectors

Select from the menu:

|  |  |  |
| --- | --- | --- |
| Spear-Phishing Attack Steps | Spear-Phishing Attack Vectors  Infect ious Media Generator  4) Create a Payload and Listener |  |
| Choose Spear Phishing | Mass mailer Attack  Arduino•Based Attack Vector  7) Wireless Access Point Attack Vector |  |
| Attack Vectors | 8) QRCode Generator Attack Vector  Powers heI I Attack Vectors  19) SMS Spoofing Attack Vector |  |
| Perform a Mass Email Attack | Third Party Modules  99) Return back to the main menu. |  |
|  | The sets | (SET' |

Third Party Modules

Other options for spear phishing 99) Return back to the main menu. attack include: se-t> 1

The spearphishing module al lows you to specially craft email messages and send

* Create a FileFormat Payload them payloads, to a targe If you (or want small) to spoof number your of email peopte address. With attached be sure titeformat "Sendmail" maliciousis in

stalled (apt-get install sendmaiO and change the config/set\_config SENDMAIL—OF

* Create Social-Engineering flag to SENDMAtu=ON.

Template 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!

Perform a Mass Email Attack

* 1. Create a FI eFormat Pay oa
  2. Create a Social-Engineering Template

Return to Main Menu

# 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

us r/ f ramewo rk/

Select the file format explOit you want.

The default is the PDF embedded EXE

SET Custom Written DLL Hijacking Attack Vector (RAR, Zlm 2) SET Custom written Document UNC LM SMB Capture Attack

1. Microsoft Windows media center MCL vulnerability
2. MS14-017 Microsoft Word RTF Object Confusion (2614-04-01)
3. Microsoft windows C reateSizedDIBSECTION Stack Buffer overflow
4. Microsoft Word RTF pFragments Stack Buffer Overflow (MSIO-087)
5. Adobe Flash Player "Button" Remote code Execution
6. Adobe COOL Type SING Table •uniquetqame•• overflow
7. Adobe Flash Player "newfunction" Invalid Pointer use
8. Adobe collab .coIIectEmaiUnfo Buffer overflow
9. Adobe Collab egetlcon Buffer Overflow
10. Adobe JBIG2Decode Memory corruption Exploit
11. Adobe PDF Embedded EXE Social Engineering
12. Adobe util. printf() Buffer Overflow
13. custom EXE to VBA (sent via RAN) (RAR required)
14. Adobe '\_J3D CLODProgressiveMeshDecIaration Array Overrun
15. Adobe PDF Embedded EXE social Engineering (NODS)
16. Foxit PDF Reader v4.1.1 Title Stack Buffer Overflow ouot
17. Apple QuickTime PICT pnSize Buffer overflow
18. Nuance PDF Reader v6,o Launch Stack Buffer Overflow
19. Adobe Reader u3D Memory Corruption Vulnerability
20. MSCOMCTL Activex Buffer overtrow ("1512-027)

# Spear-Phishing Attack Steps

|  |  |
| --- | --- |
| * Hacker IP 10.1.1.1 * Meterpreter   Memory Injection  Listener Port 443   * Windows   Meterpreter  Reverse Shell   * Payload via   Shellcode Injection | Enter the iP address for the payload (reverse) :lö.l.l.i  What payload do you want to generate:  Name : Description  1 ) Meterpreter Memory Injection (DEFAULT) This will drop a meterpreter payload through powershell injection  3 ) SE Toolkit Interactive Shell Custom interactive reverse toolkit designed for SET  SE Toolkit HTTP Reverse Shell Purely native HTTP shell with AES encryption support   1. ) RATTE HTTP Tunneling payload Security bypass payload that tunnel all comms over HTTP 2. ) Shet tCodeExec Alphanum Shettcode This witt drop a meterpreter payload through sheUcodeexec Import your own executable Specify a path for your executable   8 ) Import your own commands. txt Specify payloads ta be sent via command tine  PORT of the listener :  Select the payload you want to deliver via she LLcode inj ection  Windows Meterpreter TCP   1. Windows Meterpreter (Reflective Injection), Reverse HTTPS Stager 2. Windows Meterpreter (Ref Lective Injection > Reverse HTTP Stager 3. Windows Meterpreter (ALL PORTS) Reverse TCP   Enter the number for the payload [meterpreter reverse httpsl : 1  J Preppi ng |

The DLL Hijacker vulnerability file to can total (or remote) .dtt files that can then catt your payload or executable, In this scenario it; compact the attack in a zip file and when the user opens the tile extension, trigger the dll then ultimately Our payload. During the time of this release. Of these file extensions were tested and appear to work and are not patched. This

Continiously be updated as tine 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.o.1
* Firefox 3.6.O
* EnCase
* IBM License Key Admin

Microsoft RDP

The DLL Hijacker vulnerability will allow normal file extenstions 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 continiously 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 2037
5. . Microsoft Group Converter
6. . safari V5.G.1
7. . Firefox 3.6.8
8. , Microsoft powerpoint 231€
9. . Microsoft PowerPoint 2007
10. . Microsoft Visio 2018
11. . Microsoft Word 2007
12. . Microsoft powerpoint 20€7
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

> rar : 2

This may take a few to load NSF.. .

L •J If you are using GMAIL • you need to need to Create an application password;

[-1 As an added bonus, use the file-format creator in SET to create your attachment ,

* Choose the file's name Right now the attachment will be imported with filename of 'template .whatever•

Do you want to rename the file?

* Select Single Email Attack example Enter the new filename: moo , pdf

2. Rename the file, I want to be cool

: QhXfdnmng>2

Filename ,

Social Engineer Toolkit Hass 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

ass e

99. Return to main menu.

# Spear-Phishing Attack Steps

* Use Pre-Defined Template
* Select 'Computer Issue'
* Send email to:

'123click@vulnerable.com'

## • Send from

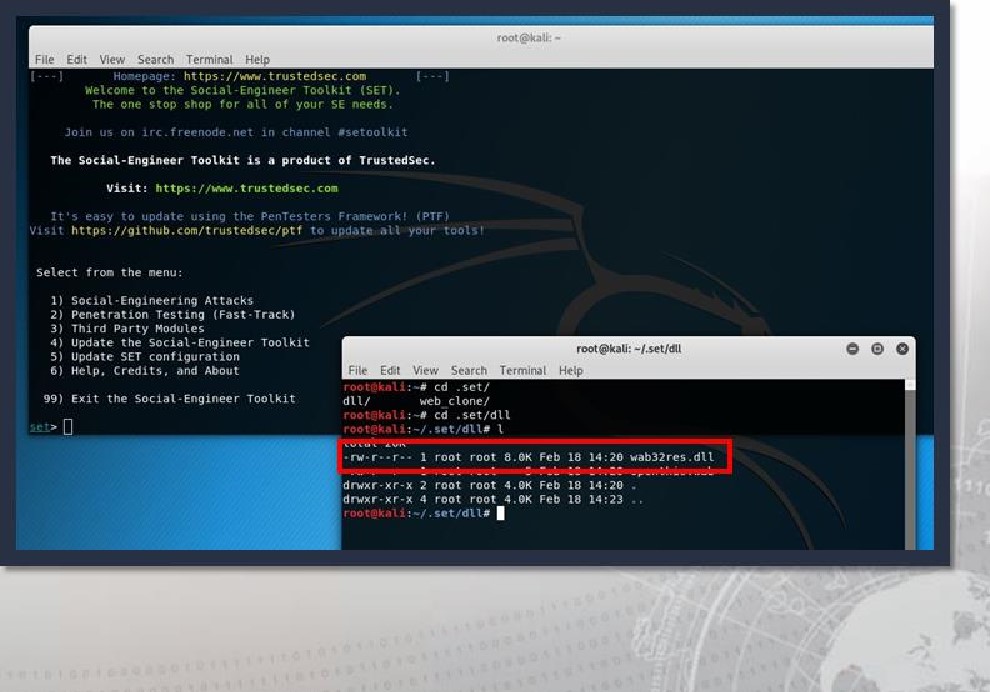
'hack2hack@spectre.com'

• From name user will see:

'Poppins, Mary'

I

# Spear-Phishing Attack Steps

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

I

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.

## 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?

I

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?

I

## Web Shell Defined

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 5-314A

• 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

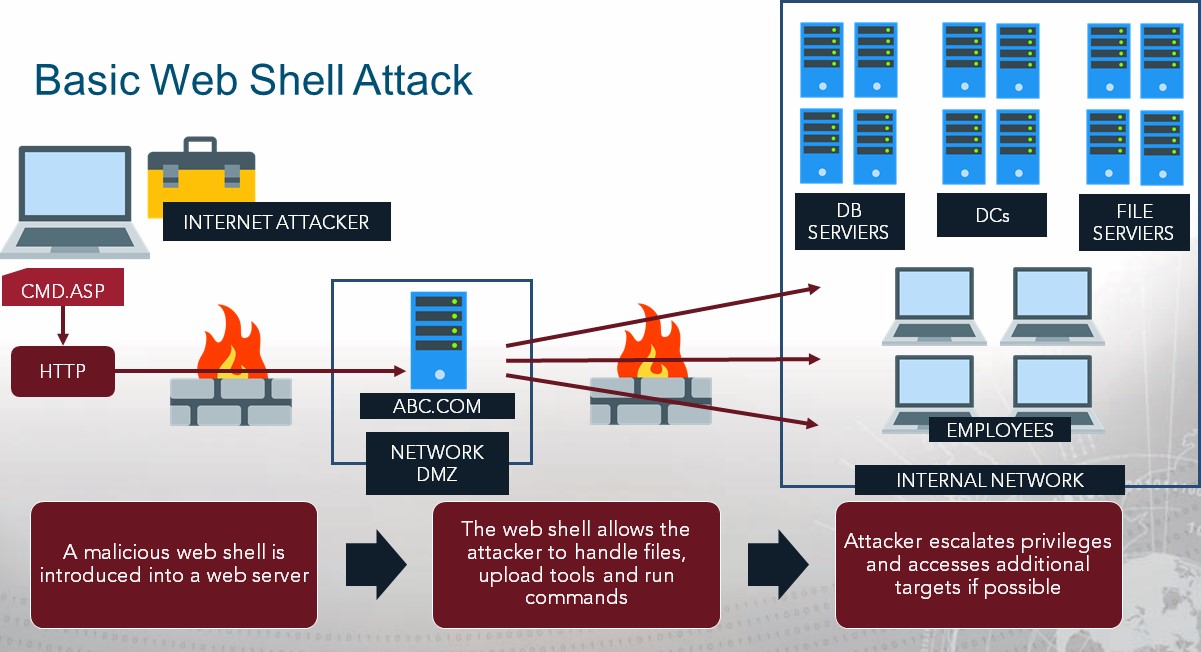
I

## Delivery Tactics

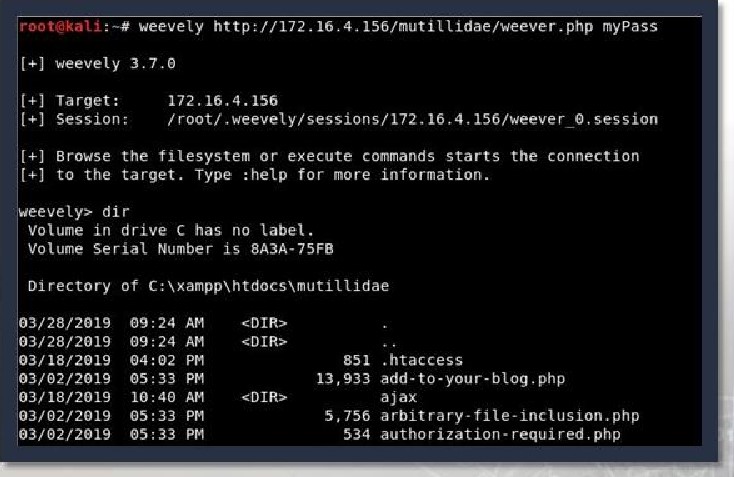
* SQL Injection
* Web App / Service

Vulnerabilities (CMS)

* Remote File Include (RFI)
* Local File Include (LFI)



## Web Shell Example: weeveIy3

There are many types of web shells but we will focus on weevely3

* 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

# 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?

I

## Lesson Summary

In this lesson we learned about:

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

I

|  |
| --- |
| End of Module 2, Lesson 3 |