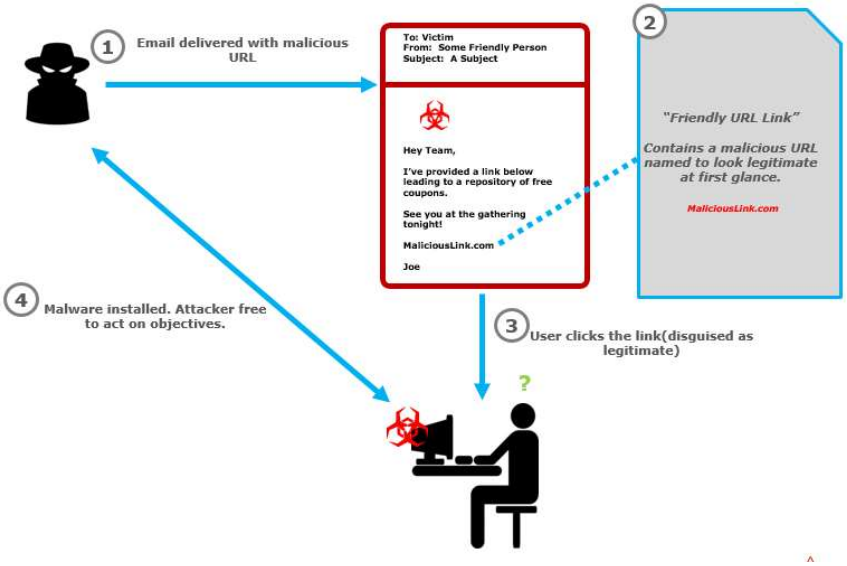
Threat Hunting with RSA: Heads up and Hands On

ACTIVITY GUIDE QUESTIONS

For help during the 72 hours after the webinar, please email hunters@rsa.com. The threat hunting team will respond to questions during normal business hours. For an instructional video on phishing which will guide you through the interface, please review: a pre-recorded video of Use Case #1. https://youtu.be/UrN3XHfbnyM

Table of Contents

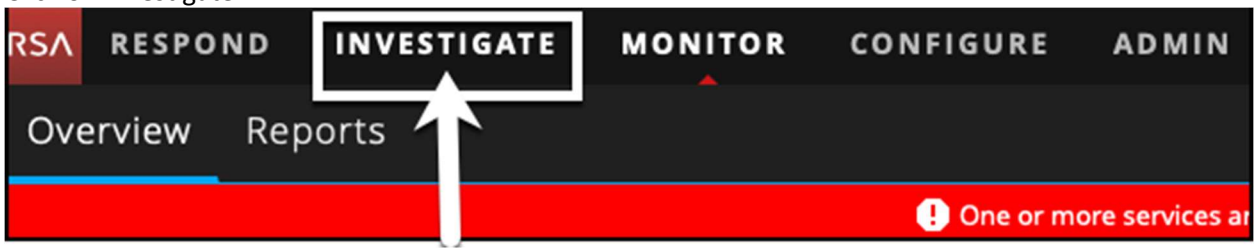
ACTIVITY QUESTION #1: Phishing Email



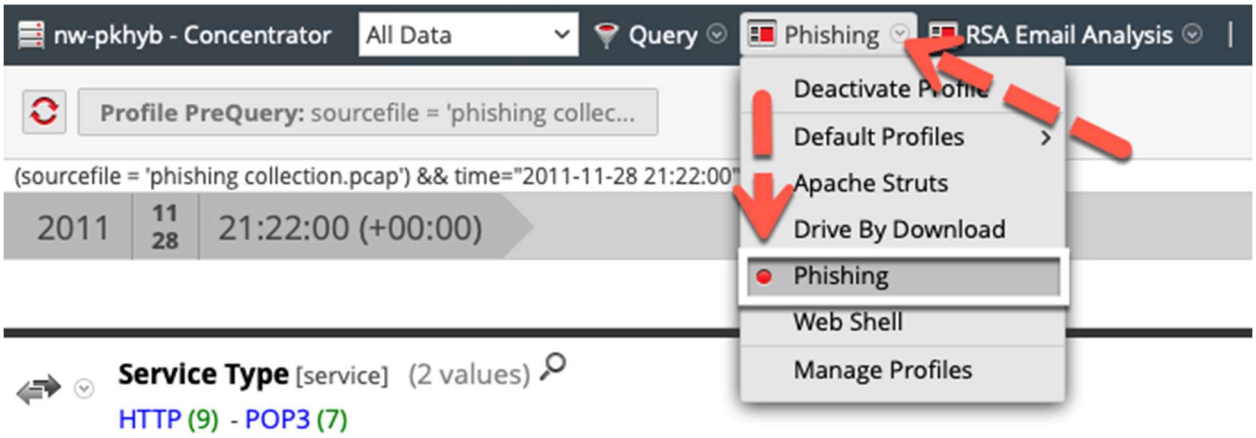
Overview:
Phishing refers to an attack that uses email or a messaging service (like those on social media sites) that tricks or fools you into taking an action, such as clicking on a link or opening an attachment. By falling victim to such an attack, you risk having your highly sensitive information stolen and/or your computer infected. Attackers work hard to make their phishing emails convincing. For example, they will make their email look like it came from someone or something you know, such as a friend or a trusted company you frequently use. They will even add logos of your bank or forge the email address so the message appears more legitimate. Then the attackers send these phishing emails to millions of people. They do not know who will fall victim, all they know is the more emails they send, the greater the chance for success. Phishing is similar to using a net to catch fish; you do not know what you will catch, but the bigger the net, the more fish you will find.
Reference: https://www.sans.org/security-awareness-training/ouch-newsletter/2015/phishing

Objective: A phishing email was sent to users at Prymida. Investigate and determine the scope of this phishing attack.

Getting started: Open a browser and head to https://nw#.titan-net.work

- The # will be written on the board or communicated to you.
- Login Credentials: USERNAME: student# PASSWORD: NetWitness!
  - The # in the username will be provided to you.
- Click on Investigate
- 

- and use the drop down from the profile tab to select Phishing



-

Before you begin think about the following:

- What is your methodology for investigating a phishing attack?
- What do you look for?
- How do you confirm a phishing email?

INVESTIGATION VIEW:

1. What is the subject of the email sent to Prymida users?
2. Who/What is the sender of the email?
3. What is the source IP associated with the phishing email?
4. To how many destination IPs did the source IP communicate?

EMAIL VIEW:

5. Right click on the green number next to one of the email sessions and select “View Sessions in New Tab”. What is suspicious about this email?

TEXT VIEW:

6. What is suspicious about the link in the email www.facebook.com?
7. Is this a legitimate IP address from Facebook?
8. How many users actually clicked the link www.facebook.com?

META VIEW:

9. From the same query ‘ip.dst = 41.140.181.156’ in the Investigation View - Right click on the number 3 next to “exe” from the meta category ‘Extension’ and select “View Sessions in New Tab”.
    a. What is the name of the exe file?
    b. What client (user agent) was used for this get request?
    c. What is the destination country and city for this session?

****Bonus Question*****

What emails were compromised?

Tip: Match IPs to email addresses from the Source IP Address category.

FURTHER ACTIONS:

After investigating and determining the scope of the phishing attack, what other actions can be taken to further ensure or validate the scope of the attack?

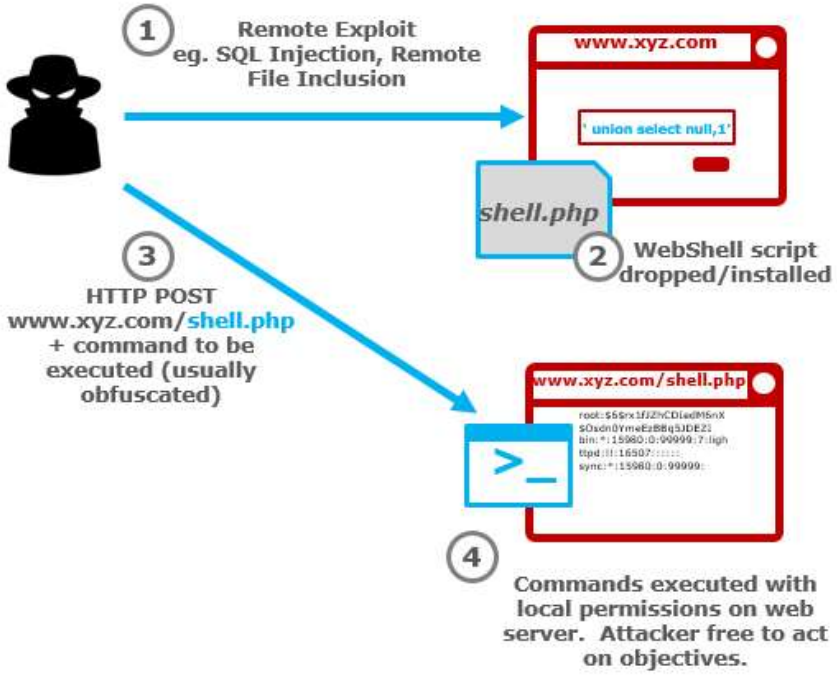
a. Scan machines with an EDR tool to see if there is further compromise on the host machine.
b. Look for suspicious or anomalous activity on the host.
c. Document and capture any artifacts and IOCs to add to your threat intelligence feeds you can also deploy to other systems
d. Remediate host machine – quarantine, block, or wipe

Examples of real-world Phishing attacks:

https://community.rsa.com/community/products/netwitness/blog/2017/08/04/targeted-malspam-delivers-chthonic-and-dimnie-8-2-2017

https://community.rsa.com/community/products/netwitness/blog/2018/02/14/malspam-delivers-isr-stealer-2-13-2017

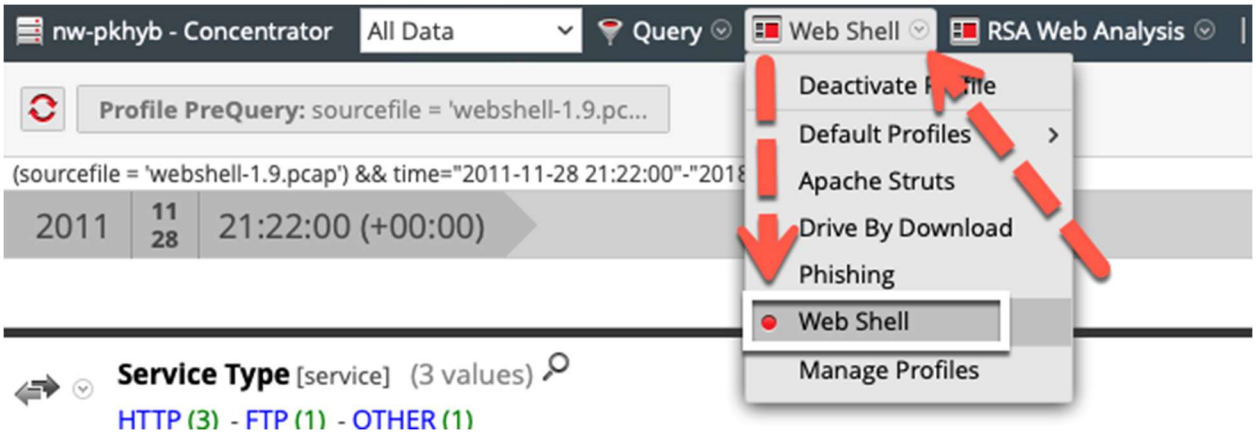
ACTIVITY QUESTION #2: WebShell



Overview:
A WebShell is a piece of code or a script running on a server that enables remote administration. While often used for legitimate administration purposes, it is also a favorite tactic used by malicious actors in order to gain remote control of internet-facing web servers. Once interaction with a WebShell is established, an attacker is free to act on any number of objectives such as disrupting services, moving laterally, or exfiltrating data.

Before you begin:

- use the drop down from the profile tab to select webshell

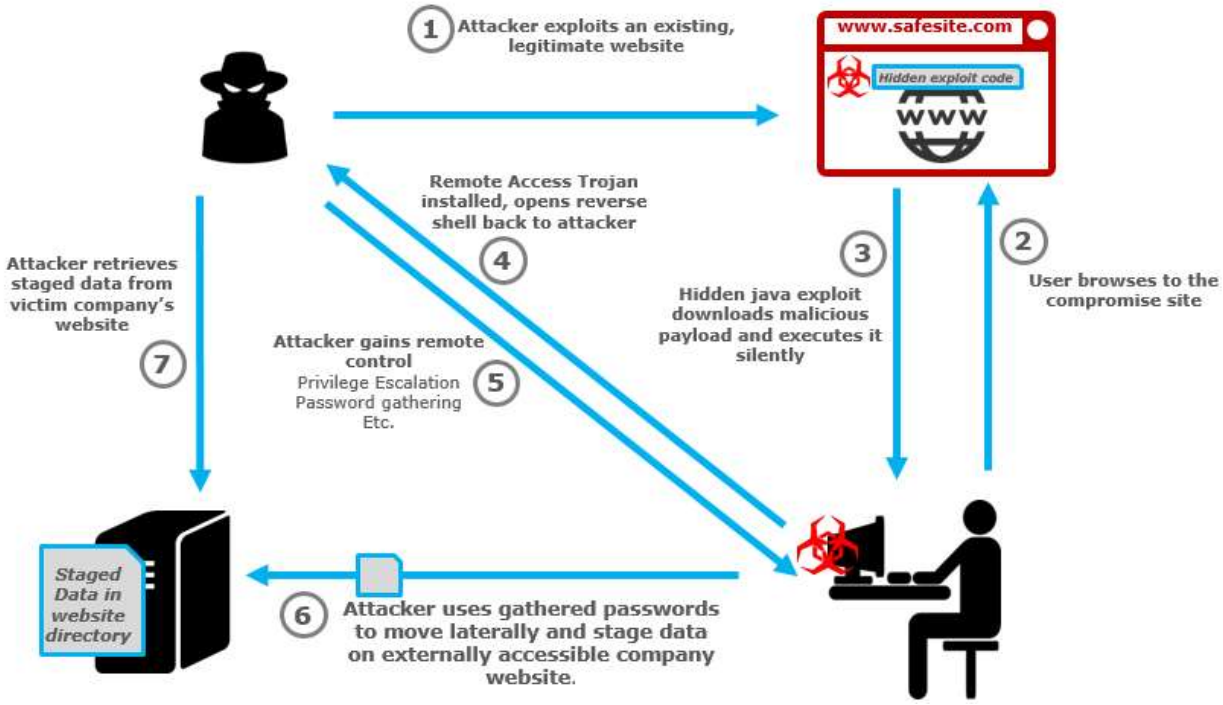


Objective:

You have received an event notification from your tier 1 analyst notifying you of a potential WebShell. Your tier 1 analyst has already done some preliminary work and notices that it appears to have occurred through a 'POST; command without a preceding 'GET.' The referrer also appears to be uncommon. Investigate and determine the scope of this WebShell.

1. Based on the above information, what are the two meta keys that serve as pivot points for http post traffic?
2. Are there any other suspicious service types?
3. What is the malicious actor's IP address?
4. What is the name of the file that is used as a setting to allow commands to be posted?
5. What was the first command used?
6. What was the second command used?
7. What is the variable used to launch commands?
8. Was this a successful campaign?
9. What is the referrer and why might it be an important pivot point in any proactive hunting investigation?

ACTIVITY QUESTIONS #3: Drive by Download

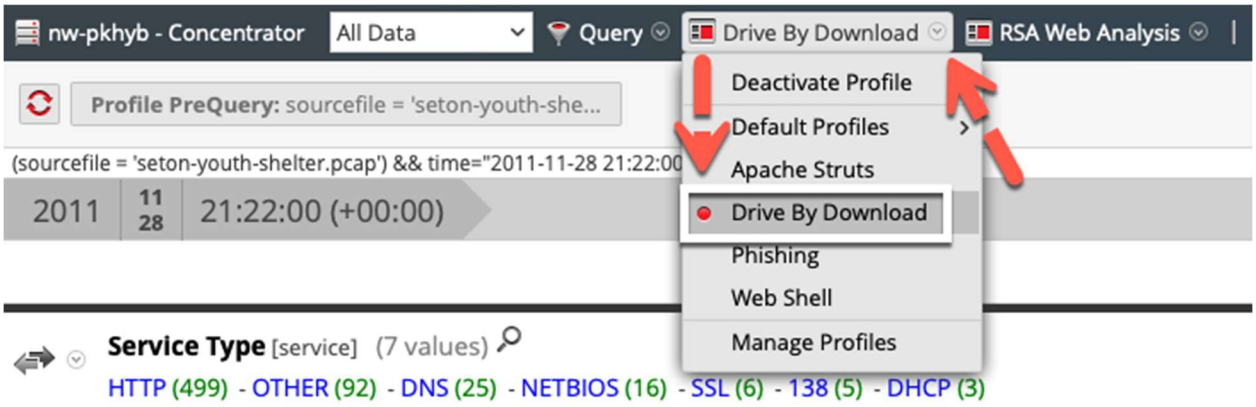


Overview:
Drive by Downloads are a common technique used by attackers to silently install malware on a victim computer. Once a target website has been weaponized with some form of exploit (typically browser or plugin exploits, hidden iframes, javascript, among other techniques), the attacker may lure, or wait for, their target to browse to the webpage. The compromised page will typically look completely normal to the end user, while the exploit executes and installs malware on the victim computer silently in the background. Once the malware makes its way onto the target's computer, the attacker can act on their objectives.

Objective: A user has unknowingly come across a malicious site and has downloaded something bad. Investigate and determine the scope of this Drive by Download.

Before you begin:

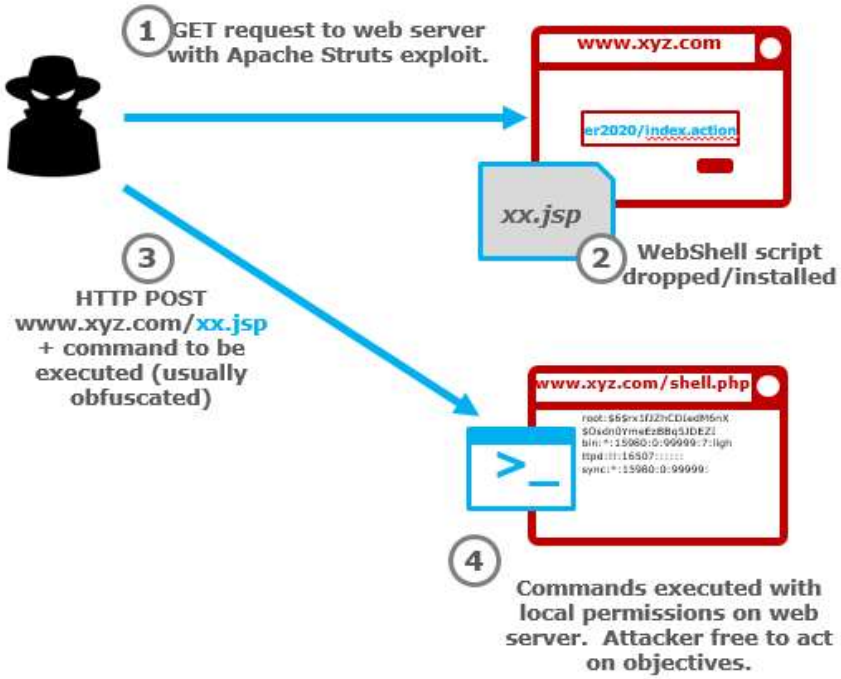
- use the drop down from the profile tab to select Drive By Download



Let's get started. After the exercise is completed you will be able to describe what happened.

1. Look around the data to familiarize yourself with what's in the Pcap.
2. What do you notice? Does anything stand out as unusual?
    a. File Types
    b. Hostnames - Do they all look like valid domain names?
    c. Services
    d. Referer
    e. DNS queries
3. Is there a large number of sessions for one service type over the other?
4. If you click on one of the .ms domain names what do you find?
    a. What files are associated with it?
5. Does the Count13.php file behave the way you could expect?
    a. Describe what you see
6. There was some activity on the user's workstation around this time?
    a. What domain did this belong to?
    b. What site was the user browsing?
    c. Was the user initiating this action?
7. After this activity, what files were downloaded?
    a. Were they normal files or is anything odd?
    b. What types of files were downloaded?
8. Were any mismatched files downloaded?
9. What was the originator of the infection?
10. What was it in #9 that started the infection?
11. How could you look for this type of behavior in the future in an automated fashion?

COMPETITION: Apache Struts



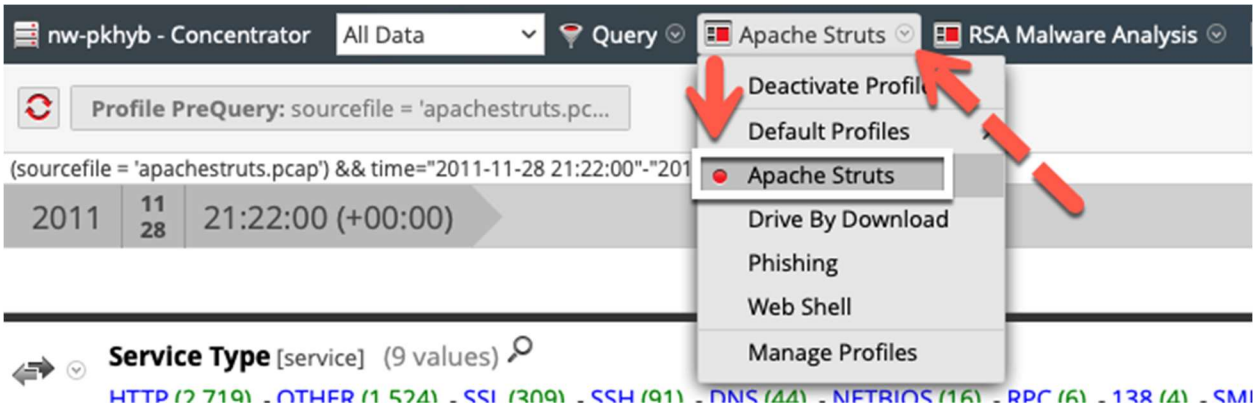
You have 45 mins to complete this exercise. The person with the most correct answers wins.

Overview:
Apache Struts is vulnerable to remote command injection attacks through incorrectly parsing an attacker's invalid Content-Type HTTP header. The Struts vulnerability allows these commands to be executed under the privileges of the Web server. This is full remote command execution and has been actively exploited in the wild since the initial disclosure.
Source: https://www.synopsys.com/blogs/software-security/cve-2017-5638-anatomy-apache-struts-vulnerability/

Objective:
An alert comes into your queue at 7:56 Pacific Standard Time that says "Apache Struts Exploit Attempt with Server Response for 188.225.32.103" where 188.225.32.103 is the attacker. You are receiving this alert in Houston, Texas. Investigate and determine the scope of this Struts attack.

Before you begin:

- SUBMIT Answers to below questions @ https://www.surveymonkey.com/r/9LJP995
- use the drop down from the profile tab to select Apache Struts



1. What is the name of the website which is exploited by the Apache Struts vulnerability?
2. What is the IP of the victim host?
3. What is the IP of the attacker for the struts exploit?
4. What are the destination port and protocol used by the attacker to exploit the web server?
5. What User-Agent is being sent with the exploit attempts?
6. What time did the first exploit attempt from the attacker IP happen?
7. What OS is the victim host running?
8. What user account is the web server running under?
9. What tool (or type of tool) did the attackers install on the web server using the exploit?
10. At what time was the tool uploaded?
11. After this new 'tool' is uploaded, what is the first payload sent to it by the attacker?
12. What encoding scheme is used to obfuscate the payload from #11?
13. Once decoded, what Windows command appears to be sent to the web server this payload?
14. What is the second command string (just the first few characters are fine) that is posted to the WebShell and what command does it appear to be trying to send (once decoded) to the web server?
15. What is the attacker's purpose with the second command being sent to the web server?
16. Which IP address is the PowerShell Empire listener /C2 host sitting on?
17. List the command and control URL(s)