CS 473: Network Security – A4

Total Marks: 115

Deadline : 26th April 2022 11:55 pm

Guidelines:

You will have to submit a zipped folder on LMS, containing a pdf with all the answers, code snippets explanations and respective screenshots.

You can do this assignment is pairs.

Submit your file with the naming convention **rollnumber1_rollnumber2_PA4.pdf**

Section 1

Read the following research paper, Resilience of Deployed TCP to Blind Attacks, to explore how resilient the deployed TCP is to some of the attacks: Links to the paper: **[15 Marks]**
https://www.caida.org/~mjl/pubs/blind.pdf
https://drive.google.com/file/d/1MMhblHGJ5Jo__r0A8laZlwTDQYaLG0C_/view?usp=sharing
You are supposed to write around a half-page (12 font, Times New Roman) summary of this paper. The summary should be structured as follows:

- ❖ Goal(s) of the paper
- ❖ Methods used
- ❖ Findings of the paper

Do not simply copy paste sentences from the paragraph.
Ensure that you write in your own words as plagiarism will be taken into account.

Section 2

You will be performing the following tasks on the VMs which you need to setup using instructions in ***setup.pdf***

In this task, you will be performing attacks on DNS. When a user enters http://www.example.net in the browser, the machine will issue a DNS query to find out the IP address of the website. Your goal as the attacker is to fool the machine with a fake DNS reply through which you will be directing them to a malicious IP address. In this section, you will be launching a series of DNS attacks on the example.net domain.

Task 1: Modifying the Host File **[10 Marks]**

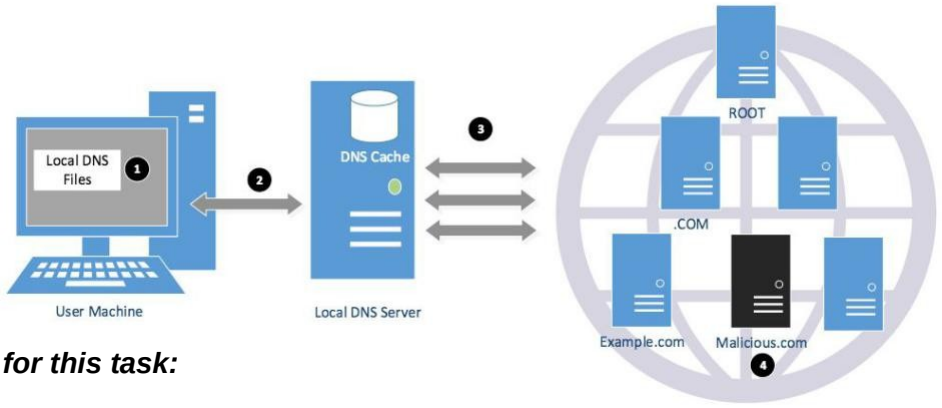
With the assumption that you can compromise the victim's machine (you need to do this), try to redirect www.randomurl.comto any IP address of your choice.

A few things to note:

1. The host name and IP address pairs in the hosts file [/etc/hosts] are used for local lookup.

2. The host file is ignored by the dig command, but will take effect on the ping command and web browser.

Here's a visual representation of this attack:



Submission for this task:

- Compare the results of redirection both before and after the attack
- Provide screenshots of the edited host file.
- Provide before and after attack screenshots of ping www.randomurl.com.
- Please also list the important code snippets followed by explanation. Simply attaching code without any explanation will not receive credits.

Task 2: Directly Spoofing Response to User **[15 Marks]**

In this attack, the victim's machine has not been compromised so you cannot directly change the DNS query process on the victim's machine. However, as you might already know, if the attacker is on the same local area network as the victim, they can still cause problems.

In this task, you will spoof a fake DNS response. The criteria the DNS response must follow in order to be accepted by the user's computer is as follows:

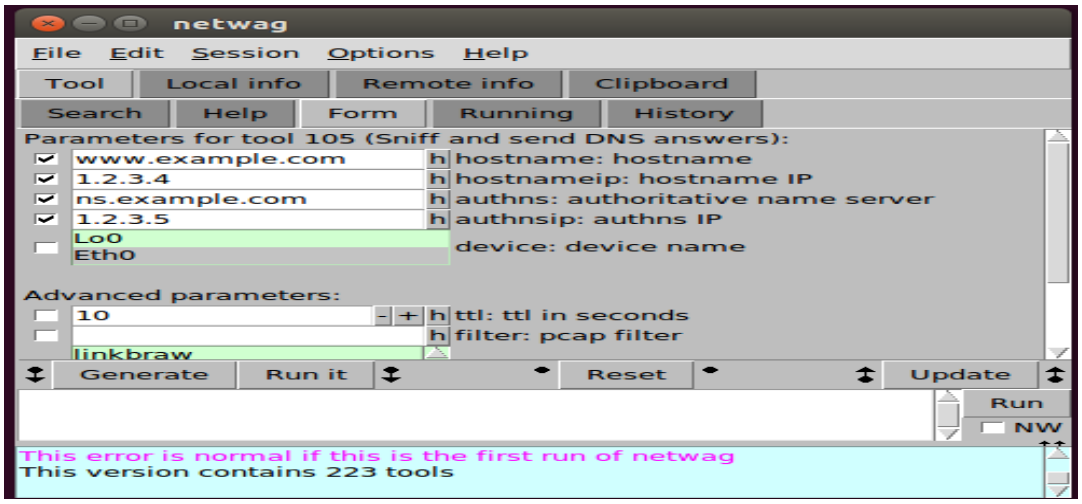
- The source IP address must match the IP address of the DNS server
- The destination IP address must match the IP address of the user's machine
- The source port number, which is also known as the UDP port, must match the port number that the DNS request was sent to [this is usually port 53]
- The destination port number must match the port number the DNS request was sent from
- The UDP checksum must be correct
- The transaction ID must match the transaction ID in the DNS request
- The domain name in the question section of the response must match the domain name in the question section of the request
- The domain name in the answer section must match the domain name in the question section of the DNS request
- The user's computer must receive the fake DNS reply before it receives the legitimate DNS response

Netwox tool 105 *or* ***Netwag tool 105*** lets you conduct the type of sniffing and responding required in this case. You can limit the scope of your sniffing to packets only from a particular host by

setting respective flags of these tools. **Netwag tool 105** is a gui version of Netwox tool. The manual of the Netwox tool is:

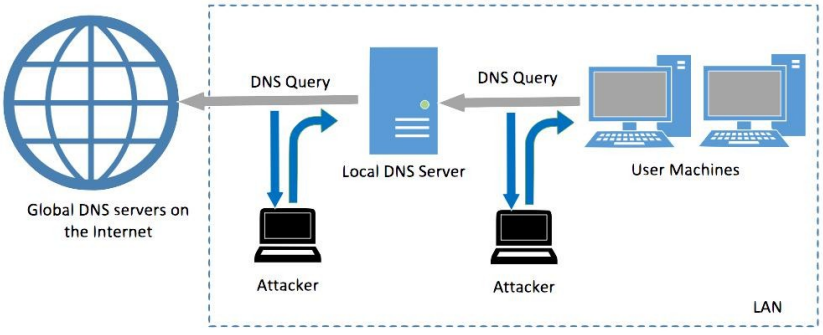
```
Title: Sniff and send DNS answers
    Usage: netwox 105 -h data -H ip -a data -A ip [-d device]
                      [-T uint32] [-f filter] [-s spoofip]
    Parameters:
    -h|--hostname data    hostname
    -H|--hostnameip ip    IP address
    -a|--authns data      authoritative nameserver
    -A|--authnsip ip      authns IP
    -d|--device device    device name
    -T|--ttl uint32       ttl in seconds
    -f|--filter filter    pcap filter
    -s|--spoofip spoofip  IP spoof initialization type
```

The interface of **Netwag 105** is as follows:



Additional Question: why is this attack not efficient?

Here's a visual representation of this attack:



Submission for this task:

- Compare the results of the dig command obtained both before and after the attack.
- Provide screenshots throughout along with explanation of what you are doing
- Answer the additional question
- Please also list the important code snippets followed by explanation. Simply attaching code without any explanation will not receive credits.

Task 3: DNS Cache Poisoning Attack **[15 Marks]**

When a DNS server X receives a query, it checks its cache; if the hostname is there, the server will simply reply with the information from its cache. If not, the server will ask another DNS server for the information. Once it gets the answer from another DNS server, it stores the answer in the cache for future queries.

In this task, you will be exploiting this and performing DNS cache poisoning. You will spoof the response from the other DNS servers so the DNS server X will keep the spoofed response in its cache for a certain time period. Next time, when a user's machine wishes to resolve the same hostname, DNS server X will use the spoofed response present in the cache to reply.

You can use the same tool **Netwox 105 or Netwag 105** for this task. However, before attacking, please make sure the DNS cache is empty. You can flush the cache using this command: **sudo rndc flush**

A few things to note:

1. Select raw in the spoofip field or else Netwox 105 will try to also spoof the MAC address for the spoofed IP address and your attack might not work.
2. You can determine if the DNS server is poisoned or not by observing the DNS traffic using wireshark when you run the dig command on the target hostname.

Submission for this task:

- Compare the results obtained both before and after the attack
- Provide screenshots throughout along with explanation of what you are doing
- Please also list the important code snippets followed by explanation. Simply attaching code without any explanation will not receive credits.

Section 3

Guidelines:

Please download the zip folder for this section from the link given below:
https://drive.google.com/file/d/1jqRhgIvQa7sFFZrkfOr1TahpDCEYrnnF/view

---

Question 3.1

[20 Marks]

For this question, you need tools that are part of Kali Linux. You can download the VM image from the following link:

https://www.osboxes.org/kali-linux/#kali-linux-2020-4-vbox

Please download Kali Linux 2018.4

Username: root
Password: osboxes.org

SketchyCorp employees connect to the wireless network using WPA2-PSK security. Our goal is to break into their network. We have managed to find a capture of their WiFi authentication handshake, which can be found as wpa2.pcap (in the zip file). We have also managed to determine that the password is in the form of either cos432-XYZ or COS432-XYZ (X, Y, and Z are alphanumeric characters [a-z, A-Z, 0-9])

Answer the following questions:

- How many possible Wi-Fi passwords are there that fulfills the password format?
- What is the actual Wi-Fi password used?
- How did you obtain that password?Make sure you add a detailed description of all the steps you took and the reason for doing so. Additionally, also add screenshots.

The following links will be helpful:

3. https://null-byte.wonderhowto.com/how-to/hack-like-pro-crack-passwords-part-4-creating-custom-wordlist-with-crunch-0156817/
4. https://tools.kali.org/wireless-attacks/aircrack-ng

Question 3.2

[40 Marks]

The goals of this question are to build up your familiarity with both how real network attacks manifest and how to effectively employ some widely available tools for analyzing network activity. The forensic questions are designed to not require exhaustive manual analysis to answer. You need to use Wireshark to carry out your investigations. You can read about Wireshark from relevant section of the document given in the following link:
https://drive.google.com/file/d/1KtpOf1Oas0ux8wR5wr6fWN86dHJEE9Vi/view

Further, some questions require the knowledge of specific header fields (which we might not have talked about in the class) to locate a "needle in the haystack." We recommend that you spend some time thinking about your analysis plan before diving into a question, i.e., how you can efficiently explore the logs. This process might benefit from some (often light) web surfing to get ideas about how to locate particular features. In general, we anticipate that the biggest pitfall for completing this question effectively is the temptation to poke through the logs "blindly" rather than thoughtfully. That often won't work effectively here — and in actual practice will work even less well because the logs you'll encounter in real life will be much larger than those here.

Submission Instructions (for this question):

You will be examining a different scenario in each problem. For each scenario, you will submit a summary of your forensic analysis. Use the questions in each problem as a road map to present your case. We expect you to provide as strong a case as you can by including the relevant information from the log files formatted according to the following skeleton:

- For scenarios 1 and 5: Answer the questions listed in the scenario.
- For scenario 3 and 4: List the following.

1. Name of the attack
2. Attacker: IP address and domain (if relevant)
3. Victim: User account, document, IP address
4. The action of the attacker: description supported by evidence from the relevant log files.

   For scenarios involving vulnerability:

   Vulnerability: description of the vulnerability

   IPs of vulnerable hosts supported by evidence (e.g., a successful attack)

Scenarios and Traces:

This forensic investigation relates to Huge Big Dairy, a farming and poultry conglomerate runout in Madison, Wisconsin. They pride themselves on their yogurts, brie cheeses, and

buffalo wings (made out of Real Buffalo). Huge Big's CEO, Chuck "Mondo" Cheeze, brashly trumpets his company's expertise, not only in all things dairy, but their e-marketing prowess and home-grown Internet security savvy. Synonymous decides to humiliate HBDairy, exposing their secrets and incompetence, and disrupting the activity of their employees. In a series of Internet attacks that HBDairy finds itself powerless to counter, Synonymous deeply embarrasses the company. Eventually, HBDairy must admit they have been out-matched, and in desperation, they turn to experts outside help: you. They commission your team to analyze how Synonymous Achieved Their Exploits. Luckily, the one facet of computer security they managed not to screw up is logging: they have full packet traces of all of the systems in question.

The traces have been shared with you in the zip file and numbered according to the following scenarios.

- **Wi-fi Connect Capture**

  Investigate the s1 trace using Wireshark. The trace captures the Authentication and Association Phase of a station connecting to a wireless access point.

  1. Why doesn't the trace contain any IP packets?

  2. What is the authentication type used by the Wireless Access Point? What are the security risks of this authentication mechanism?

  Here is a useful resource to understand the steps involved:

  https://www.packet6.com/802-11-state-machine/

- **The vulnerable DNS clients**

  Recall that most DNS clients now select a random UDP source port when making DNS queries to help defend against the Kaminsky attack. When you mention this threat to the HBDairy IT staff, they reply, "The K-huh-what attack?" Thus, you view it as prudent to assess whether any of their clients making DNS queries lack UDP source port randomization. Analyze the s2 trace to assess the sequence of source ports seen for each resolver that makes more than one query. If you find they all appear to be okay, then list the resolvers you analyzed. If you find some that appear to not use randomization, list those and the corresponding evidence.

- **The Mysterious wall post.**

  One fine morning, an HBDairy employee noticed that a secret message he had sent last night to his colleague Fro Yo using Facebook messaging (i.e., sent to his friend's inbox) was subsequently posted using his account on his friend's wall. Examine the web traffic in the s3 trace to find evidence of the attack used for the wall post. Sketch the steps of the attacker.

- **YouTube becomes NoTube.**

  One of the competitive benefits that HBDairy provides to its employees is on-the-job access to YouTube. Lately, many disgruntled employees have complained that they have lost this benefit because their browser's report page could not be loaded when they try to access YouTube. Analyze the web traffic in the s4 trace to find out how Synonymous disrupted the YouTube access. How much downtime did this result in?

- **Emails in the clear**

  The POP protocol is used for Email. Seems like one of the employees at HBDairy was taking a security course, as his email exchanges indicate. Investigate the s5 trace, and find out:

  - What is the POP username and password?
  - How many emails are in the user's mailbox?
  - Give the contents of from, to, subject, and date for each email.