An Educational Scenario for Teaching Cyber Security Using low-cost Equipment and Open Source Software

Antonios Andreatos

Hellenic Air Force Academy, Division of Computer Engineering and Information Science, Dekeleia Air Force Base, Dekeleia, Attica, Greece

antonios.andreatos@hafa.haf.gr, aandreatos@gmail.com

Abstract: This work presents a set of hands-on educational activities designed to teach some cyber security concepts in the classroom. The experimental configuration used an ad-hoc wireless and wired network, and a Raspberry Pi implementing a Web and an SSH server. Students were connected using their own devices (laptops or tablets). Initially the students tested DoS attacks to the Web server using various tools. Next, the students had to create SSH accounts to the server and a pair of RSA keys; using their SSH accounts, the students had to transfer their public keys to the server. Finally, students had to attack the SSH service from Kali Linux running on virtual machines in teams, each team using a different tool. The scenario was implemented in parts during a series of lessons and was positively accepted and evaluated by the students, who got familiar with a number of concepts and tools of computer networking and network security. In the end, the students informally assessed the Kali Linux SSH attack tools. Ways to assess the students qualitatively and quantitatively based on their participation are also presented. These lab exercises used a series of open source software, as well as low-cost equipment.

Keywords: SSH Server, Web server, DoS attacks, SSH attacks, Kali Linux, Virtual Machines, Raspberry Pi, Network Security, Cyber Security Education.

1. Introduction - Computer networks and network security courses at the Hellenic Air Force Academy

The Hellenic Air Force Academy (HAFA) offers an undergraduate programme on Telecommunications and Electronics Engineering (TEE). This specialisation is equivalent to a Bachelor's degree in Electrical Engineering. At the fourth year of studies, the Division of Computer Engineering and Information Science offers the following courses to TEE students:

- Computer Networks I is offered during the 7th semester.
- Computer Networks II is offered during the 8th (last) semester
- Network Security (in essence, Cyber Security) is offered during the 8th semester.

Cyber Security requires a strong and wide background of computer engineering and information science courses ranging from computer networks, web technologies, database management systems, programming languages, software engineering, cryptography, operating systems and computer architecture, but also mathematics, probability and statistics, psychology, etc. (Andreatos, 2017). All of these courses are offered by our institution. However, academic Cyber Security textbooks emphasise on theory and underlying principles, rarely focusing on particular systems and practical issues (Yurcik and Doss, 2000). For this reason, several lab exercises complete the theoretical education.

During the 3rd year of studies a background course of Internet technologies using the LAMP stack is taught. (LAMP stack is a bundle of four different software technologies used to build websites and web applications. LAMP is an acronym for the Linux operating system, the Apache web server, the MySQL database management system and the PHP programming language.) Procedural and object-oriented programming courses are offered in the 1st and 2nd years respectively. Operating Systems are taught at the 3rd year of studies. All these and other courses offered by other divisions are prerequisite courses for Cyber Security.

In our Network Security course the material is offered in lectures, class demonstrations, assignments, lab exercises, case studies and other activities such as videos and movies (**Andreatos, 2020).** Junior and senior students also participate in annual national and international cyber defence exercises.

2. Related works

Teaching cyber security is very different from teaching regular courses; therefore, a wide variety of teaching methodologies have been implemented during the past 15 years. Some common methodologies are: demonstrations (capture of network traffic, network simulation, video clips, movies), hands-on techniques including exercises in real and virtual labs (Prvan and Ožegović, 2020; Surma, 2003), serious games (Hwang and

Helser, 2022), and case studies (Cai, 2018). Two of the most recent surveys on the subject are: the research on Teaching Computer Networks by Prvan and Ožegović (2020) which included 196 references from ACM Digital Library and IEEE Xplore Digital Library; and the research on Teaching Cyber Security Course in the Classrooms by Churi and Rao (2021) which included 35 quality papers on innovative pedagogy on Cyber Security and similar courses from IEEE, Springer, Elsevier, and some other quality journals.

Churi and Rao (2021) support that Cyber Security is a practical subject which requires:

- Hands-on simulations of attacks and countermeasures;
- Case studies on current trends of Cyber Security;
- Use of open source software (OSS) and tools.

Yu (2007) presented a security lab setup, rules to avoid potential illegal activities for security considerations, the grading policy and the description of a term project including several successive exercises. The need for hands on laboratory exercises is emphasised by Erickson and Kim (2021), which support that "the ethical challenges of teaching students how to hack systems is real, but so is the need for them to see what is happening from both sides of the table to be able to better defend the attacks when they are in the role". One way to achieve this is to teach hacking techniques to students. Teaching students attack methods and tools in a controlled lab environment, enables them to learn what hackers are targeting and therefore find ways to defend their organisation against such attacks more easily than if they were just working on cyber defence techniques (Erickson and Kim, 2021).

Reports are indispensable in this type of lab work. The students should provide a report on what attacks were attempted, how likely they believe a skilled administrator would have detected their attack, and how the attack could have been prevented (Yu, 2007).

3. The educational scenario

3.1 Educational objectives

During the 2021-22 academic year, in an effort to promote hands-on Cyber Security education, the teacher of Computer Networks and Network Security designed a 10-12 class hours project including several successive hands-on exercises (hereafter called "scenario"). The scenario used OSS, low-cost equipment and student devices. The educational objectives of the scenario were:

a) To teach the following Computer Networking principles in practice:

- How to set up an ad-hoc LAN;
- How to monitor LAN users and network traffic;
- How to connect to a remote machine using SSH. ‘SSH’ stands for "Secure Shell", a protocol designed as a secure alternative to unsecured remote shell protocols (SSH, 2023);
- How to use virtualisation; how to connect a virtual machine (VM) to a LAN.

b) To teach the following Network Security principles in practice:

- How to generate a pair of RSA keys for public-key encryption;
- How to copy a user’s public key to a server and disable username/password authentication;
- What are the configuration files of the SSH server (sshd_config, known_hosts) and how to access them;
- How to launch a DoS attack against a web server (Williams, 2021);
- How to prepare a dictionary for a brute-force attack;
- How to brute-force attack an SSH server using a dictionary.

Step-by-step instructions, bibliography and the objectives of the lab exercises were communicated to the students in advance in two assignments (in November 2021 for Computer Networking I and in March 2022 for Network Security). The students were also advised to take notes and screenshots during the lab to put them in their reports. Figure 1 presents the steps of the scenario.

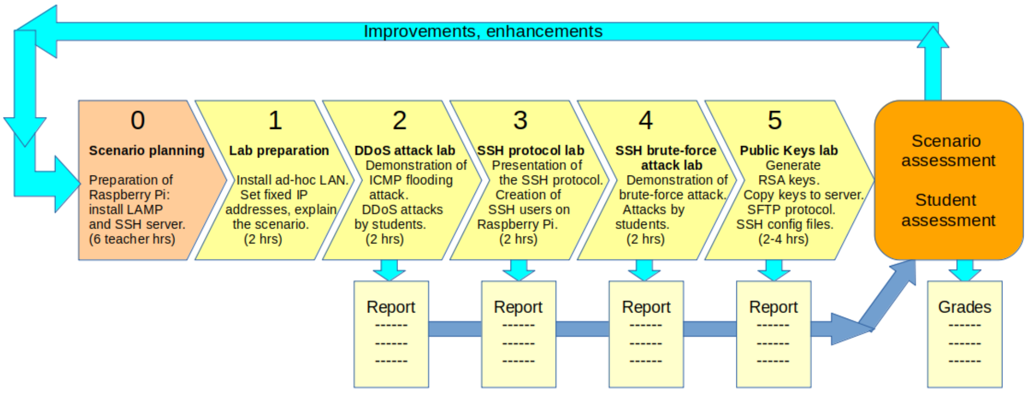

Improvements, enhancements
0
Scenario planning
Preparation of Raspberry Pi: install LAMP and SSH server. (6 teacher hrs)
1
Lab preparation
Install ad-hoc LAN. Set fixed IP addresses, explain the scenario. (2 hrs)
2
DDoS attack lab
Demonstration of ICMP flooding attack. DDoS attacks by students. (2 hrs)
3
SSH protocol lab
Presentation of the SSH protocol. Creation of SSH users on Raspberry Pi. (2 hrs)
4
SSH brute-force attack lab
Demonstration of brute-force attack. Attacks by students. (2 hrs)
5
Public Keys lab
Generate RSA keys. Copy keys to server. SFTP protocol. SSH config files. (2-4 hrs)
Scenario assessment
Student assessment
Report
Report
Report
Report
Grades

Figure 1: The educational scenario step-by-step

The whole activity was implemented during lecture hours, approximately two hours per week, in parallel with Computer Networking and Network Security theoretical classes, so that the students had enough time to get familiar with the subject. Several freely available software tools were used in these exercises, including Angry IP Scanner (for Linux), Advanced IP Scanner (for Windows), ssh-keygen, PuTTY (for Windows), VirtualBox, etc. Wireshark open-source packet analyser was used to capture network traffic in order to monitor students' activity (Ghafarian, 2014). Patator, Medusa and Metasploit were the Kali Linux tools used to attack the SSH server.

During the lab exercises the instructor provided guidance and technical support; he used tools and ways to objectively assess students based on their participation, which are also presented in this paper. The students assessed the scenario positively; in addition, it was found that, in contrast to theoretical lectures, such alternative educational activities support a variety of learning styles.

Finally, it should be noted that the planning of the scenario, the preparation of each lab, as well as the students' assessment, required many hours of work on the part of the teacher.

This paper describes the educational scenario in details in order to facilitate colleagues who may want to try it in their classroom.

3.2 Scenario planning

Due to its long duration, the activity was implemented in parts and spanned several weeks from both the Fall 2020 and Spring 2021 semesters. For this reason, the equipment had to be minimal, portable and fast to set up.

In the Fall 2020 semester the scenario was executed during the **Computer Networks** I hours; in Spring 2021 it was executed during the **Computer Networks** II and Network Security hours, in parallel with theoretical lectures, so that the students had enough time to get familiar with the prerequisite theoretical background. The three above courses are taught by the same teacher, so he had the flexibility to set the background, avoid overlays and gaps, and synchronise the lab exercises between classes. Table 1 summarises the scenario activities and the tools required in each step.

Table 1: Scenario activities and tools

No.	Activity	Tools
1	Create an account on Raspberry Pi	Terminal & ssh command
2	Perform a DoS attack on Raspberry Pi	LOIC and HOIC, hping3, Python scripts
3	Check site availability	Browser
4	Detect and present the specific attacks	Wireshark, tcpdump, netstat
5	SSH Brute Force attack on Raspberry Pi	Patator, THC Hydra, Medusa, Metasploit
6	Detect, sniff, record and present the above attack	Wireshark, tcpdump, netstat, nmap
7	Create a pair of RSA keys	ssh-keygen
8	Upload the public key to the server	ssh-copy-id, sftp, PuTTY
9	Configure the ssh-server to require keys for connection, and prevent root login	sshd_config

Activities 1 to 6 were implemented in December 2021. Students had to submit a report with their activities. Activities 7 to 9 were implemented in March 2022 (in the 2nd semester, Network Security course) after teaching the section about asymmetric encryption; students had to submit another report. Table 2 presents most tools used in the proposed scenario organised in categories.

Table 2: A taxonomy of tools used according to their function

Monitoring tools	Connection tools	DDoS tools	SSH attack tools	Discovery/ Network traffic	Support tools
Angry IP Scanner	ssh	ddos.py	THC Hydra	nmap	VirtualBox with extension pack
Advanced IP Scanner	PuTTY	LOIC and HOIC	Patator, Medusa, Metasploit	Wireshark	kali Linux image for VirtualBox
Bash commands	sftp	hping3	Dictionary tools	tcpdump	ssh-keygen

4. Lab execution

4.1 Equipment and infrastructure

Raspberry Pi is a tiny, low-cost but powerful computer board, based on a 'system on a chip'; it was first released in February 2012 (https://www.raspberrypi.org). Figure 2 shows a Raspberry Pi 4 Model B (2019). To date the Raspberry Pi Foundation has produced several generations of boards with several models which cover a wide range of open-source projects. Raspberry Pi can run several operating systems which are offered as ready-made images for downloading, with preinstalled software which converts Pi to a Print Server, Media Server, Game Sever, LAMP Web Server with WordPress, etc. In this work the Raspbian operating system has been used. Raspbian is a free version of Debian optimised for the Raspberry Pi hardware (https://www.raspbian.org). Raspberry Pi's use an SD card in order to store the operating system, applications and additional software installed.

Figure 2: Raspberry Pi model 4

A Raspberry Pi model 3B was used in these lab exercises. An ad-hoc wireless Local Area Network (LAN) was set-up to support the whole scenario. The Raspberry Pi was used as a 'headless' server (i.e., without keyboard and monitor); its software was prepared by the teacher. The web server was Apache and it hosted a site from 3rd year's course "Internet Technologies", familiar to the students. Because this device does not avail a Wi-Fi port, it was connected via wire (Ethernet port) to a Wi-Fi range extender used in access point mode. Students' and instructor's laptops were connected via Wi-Fi to the ad-hoc LAN. The Wi-Fi Range extender device was a TP-Link AC750. It operates at 2.4 GHz and offers a data exchange rate of 300 Mbps.

The recommended operating system for students was Kali Linux, either installed on bare hardware or in a virtual machine. Figure 3 presents a photograph from the lab setup.

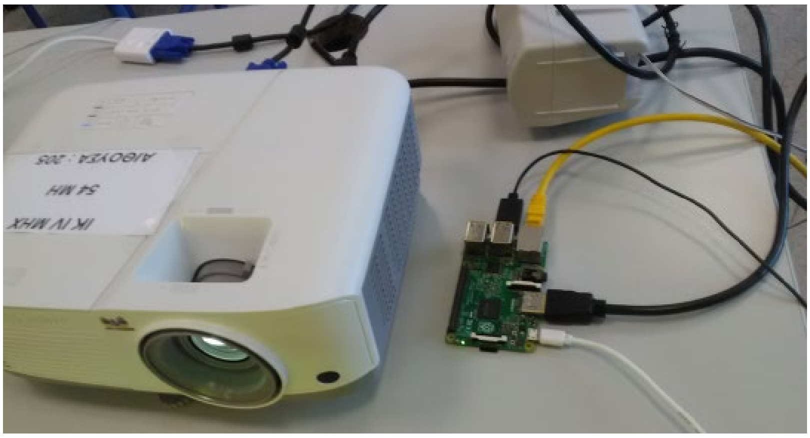


Figure 3: A photograph from the lab showing the Raspberry Pi and the projector

4.2 Instructor's role

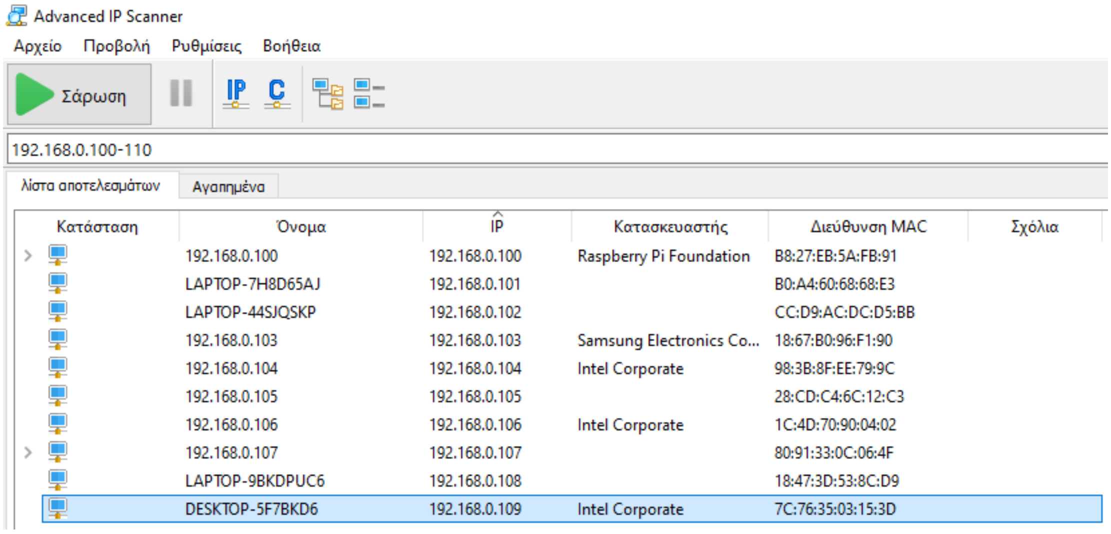
The whole experiment consumed a lot of the teacher’s time and effort in the design, implementation, student support and assessment. The instructor was guiding the students through the scenario, demonstrating the steps, offering technical support, as well as displaying the big picture through a projector (for instance, the results of the students’ activities on the Raspberry Pi or on the network traffic).

The instructor had also to keep track of students’ activities in order to make sure that no one was left behind, so that all students would be able to finish the activity. Special attention was paid to synchronising the activities with the background and skills of the students.

4.3 Procedure

The students were instructed to install the required software which included:

- Network monitoring tools (Advanced IP Scanner, Angry IP Scanner, nmap)
- Network traffic / packet capture tools (
- DoS attack tools (LOIC, HOIC and hping3)
- Virtualisation tools and a Kali Linux image (VirtualBox)
- SSH brute force attack tools (embedded in Kali).



192.168.0.100-110

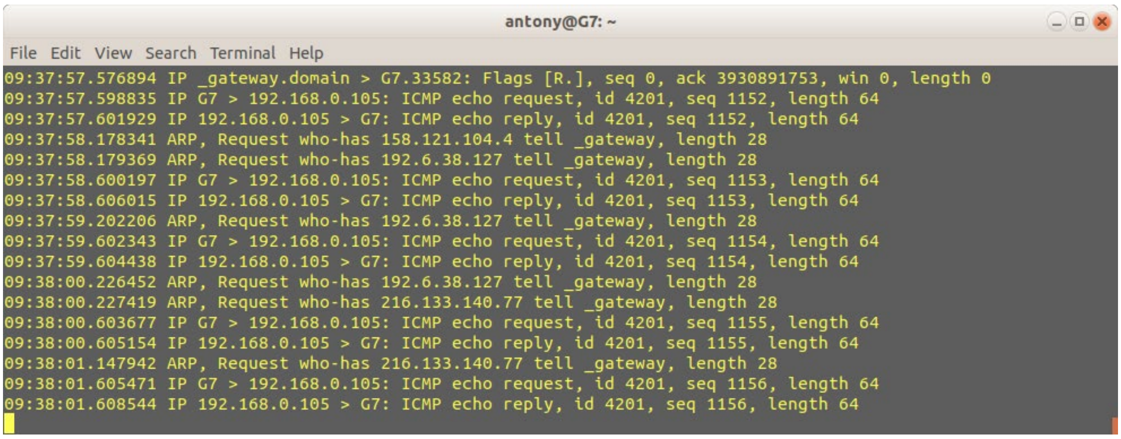
Κατάσταση	Όνομα	IP	Κατασκευαστής	Διεύθυνση MAC	Σχόλια
	192.168.0.100	192.168.0.100	Raspberry Pi Foundation	B8:27:EB:5A:FB:91	
	LAPTOP-7H8D65AJ	192.168.0.101		B0:A4:60:68:68:E3	
	LAPTOP-44SJQSKP	192.168.0.102		CC:D9:AC:DC:D5:BB	
	192.168.0.103	192.168.0.103	Samsung Electronics Co...	18:67:B0:96:F1:90	
	192.168.0.104	192.168.0.104	Intel Corporate	98:3B:8F:EE:79:9C	
	192.168.0.105	192.168.0.105		28:CD:C4:6C:12:C3	
	192.168.0.106	192.168.0.106	Intel Corporate	1C:4D:70:90:04:02	
	192.168.0.107	192.168.0.107		80:91:33:0C:06:4F	
	LAPTOP-9BKDPUC6	192.168.0.108		18:47:3D:53:8C:D9	
	DESKTOP-5F7BKD6	192.168.0.109	Intel Corporate	7C:76:35:03:15:3D	

Figure 4: A screenshot from Advanced IP Scanner

The teacher used a Linux laptop to connect to the Raspberry Pi via SSH. From this laptop the teacher was also monitoring and recording students’ activities using proper software (Angry IP scanner, Advanced IP Scanner, Wireshark and tcpdump). Figure 4 presents a screenshot from Advanced IP scanner.

DoS/DDoS attacks

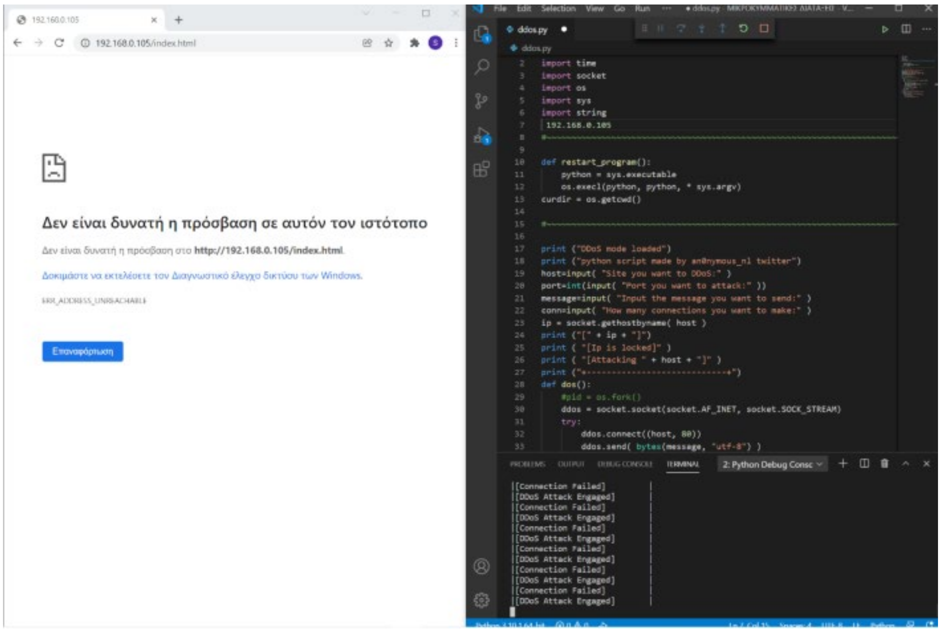
The teacher launched an ICMP flooding attack with endless ping and displayed the traffic on screen using tcpdump (Figure 5). Afterwards he displayed the students' traffic from Wireshark on the projector.



```
09:37:57.576894 IP _gateway.domain > G7.33582: Flags [R.], seq 0, ack 3930891753, win 0, length 0
09:37:57.598835 IP G7 > 192.168.0.105: ICMP echo request, id 4201, seq 1152, length 64
09:37:57.601929 IP 192.168.0.105 > G7: ICMP echo reply, id 4201, seq 1152, length 64
09:37:58.178341 ARP, Request who-has 158.121.104.4 tell _gateway, length 28
09:37:58.179369 ARP, Request who-has 192.6.38.127 tell _gateway, length 28
09:37:58.600197 IP G7 > 192.168.0.105: ICMP echo request, id 4201, seq 1153, length 64
09:37:58.606015 IP 192.168.0.105 > G7: ICMP echo reply, id 4201, seq 1153, length 64
09:37:59.202206 ARP, Request who-has 192.6.38.127 tell _gateway, length 28
09:37:59.602343 IP G7 > 192.168.0.105: ICMP echo request, id 4201, seq 1154, length 64
09:37:59.604438 IP 192.168.0.105 > G7: ICMP echo reply, id 4201, seq 1154, length 64
09:38:00.226452 ARP, Request who-has 192.6.38.127 tell _gateway, length 28
09:38:00.227419 ARP, Request who-has 216.133.140.77 tell _gateway, length 28
09:38:00.603677 IP G7 > 192.168.0.105: ICMP echo request, id 4201, seq 1155, length 64
09:38:00.605154 IP 192.168.0.105 > G7: ICMP echo reply, id 4201, seq 1155, length 64
09:38:01.147942 ARP, Request who-has 216.133.140.77 tell _gateway, length 28
09:38:01.605471 IP G7 > 192.168.0.105: ICMP echo request, id 4201, seq 1156, length 64
09:38:01.608544 IP 192.168.0.105 > G7: ICMP echo reply, id 4201, seq 1156, length 64
```

Figure 5: Screenshot from an ICMP flooding attack demonstrated by the teacher

LOIC and HOIC tools were proposed for DoS attacks on the Raspberry Pi's web server. However, a student had some Python script tools which shared with his classmates. Next, the students started the DDoS attack from their devices. Figure 6 demonstrates a screenshot from a student's report demonstrating a DoS attack via 'ddos.py'. The message on the left writes that 'access to this site is not possible' in Greek.



Δεν είναι δυνατή η πρόσβαση σε αυτόν τον ιστότοπο

Δεν είναι δυνατή η πρόσβαση στο **http://192.168.0.105/index.html**.

Δοκιμάστε να εκτελέσετε τον Διαγνωστικό έλεγχο δικτύου των Windows.

ERR_ADDRESS_UNREACHABLE

```
import time
import socket
import os
import sys
import string
 192.168.0.105
#------------------------------------------------------------------------

def restart_program():
    python = sys.executable
    os.execl(python, python, * sys.argv)
curdir = os.getcwd()

#------------------------------------------------------------------------

print ("DDoS mode loaded")
print ("python script made by an0nymous_nl twitter")
host=input( "Site you want to DDoS:" )
port=int(input( "Port you want to attack:" ))
message=input( "Input the message you want to send:" )
conn=input( "How many connections you want to make:" )
ip = socket.gethostbyname( host )
print ("[" + ip + "]")
print ( "[Ip is locked]" )
print ( "[Attacking " + host + "]" )
print ("+----------------------------+")
def dos():
    #pid = os.fork()
    ddos = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    try:
        ddos.connect((host, 80))
        ddos.send( bytes(message, "utf-8") )
```

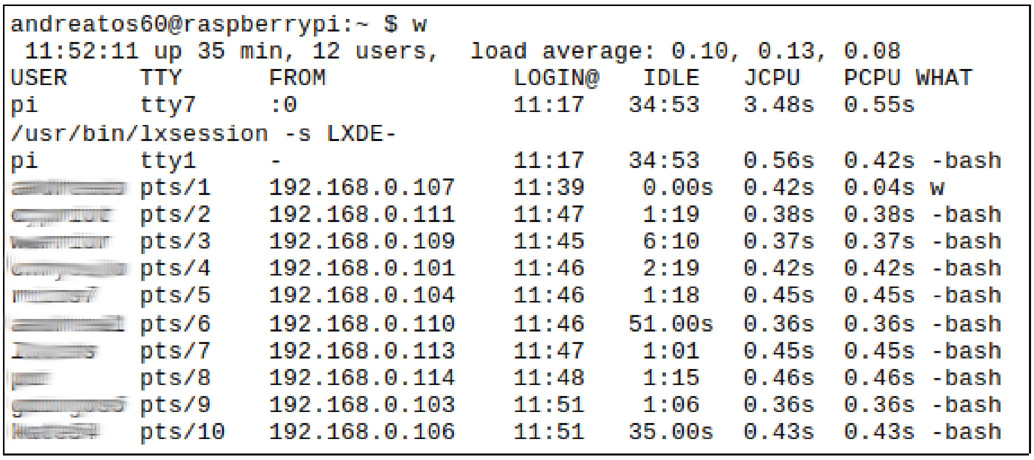
```
|[Connection Failed]
|[DDoS Attack Engaged]
|[Connection Failed]
|[DDoS Attack Engaged]
|[Connection Failed]
|[DDoS Attack Engaged]
|[Connection Failed]
|[DDoS Attack Engaged]
|[Connection Failed]
|[DDoS Attack Engaged]
|[Connection Failed]
|[DDoS Attack Engaged]
```

Figure 6: Screenshot from a student's report demonstrating DoS attack via 'ddos.py'

Creation of SSH users

The teacher demonstrated how to connect to Raspberry Pi as root and how to create a new SSH user with username and password. Then, the students created personal SSH accounts using usernames related to their lastname. Next, the students connected to Raspberry Pi using the username and password they created and explored their home directory.

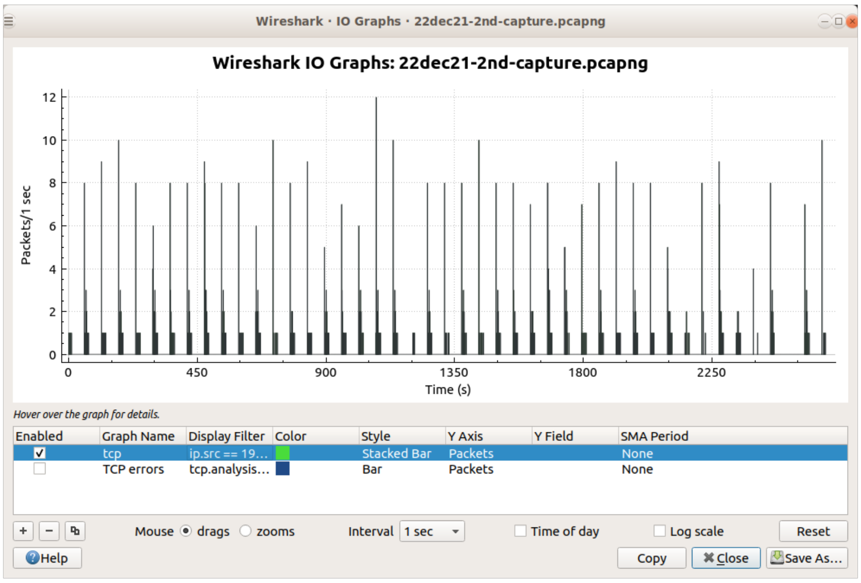
The teacher checked their connection via the 'w' command. The 'w' command is a Linux terminal built-in tool that allows administrators to view information about currently logged in users. This includes their username, where they are logged in from (IP address in our case), log-in time, what they are currently doing, etc. This is a milestone used in quantitative assessment. Figure 7 demonstrates a representative screenshot.



```
andreatos60@raspberrypi:~ $ w
 11:52:11 up 35 min, 12 users,  load average: 0.10, 0.13, 0.08
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
pi       tty7     :0               11:17   34:53   3.48s  0.55s
/usr/bin/lxsession -s LXDE-
pi       tty1     -                11:17   34:53   0.56s  0.42s -bash
[redacted] pts/1    192.168.0.107    11:39    0.00s  0.42s  0.04s w
[redacted] pts/2    192.168.0.111    11:47    1:19   0.38s  0.38s -bash
[redacted] pts/3    192.168.0.109    11:45    6:10   0.37s  0.37s -bash
[redacted] pts/4    192.168.0.101    11:46    2:19   0.42s  0.42s -bash
[redacted] pts/5    192.168.0.104    11:46    1:18   0.45s  0.45s -bash
[redacted] pts/6    192.168.0.110    11:46   51.00s  0.36s  0.36s -bash
[redacted] pts/7    192.168.0.113    11:47    1:01   0.45s  0.45s -bash
[redacted] pts/8    192.168.0.114    11:48    1:15   0.46s  0.46s -bash
[redacted] pts/9    192.168.0.103    11:51    1:06   0.36s  0.36s -bash
[redacted] pts/10   192.168.0.106    11:51   35.00s  0.43s  0.43s -bash
```

Figure 7: A screenshot from ‘w’ command demonstrating students connected to Raspberry Pi

The teacher recorded the network traffic with Wireshark (Figure 8). From the Wireshark Statistics menu the teacher could identify their activity (based on the student’s MAC and IP addresses). This was another milestone for quantitative assessment.



Wireshark · IO Graphs · 22dec21-2nd-capture.pcapng
Wireshark IO Graphs: 22dec21-2nd-capture.pcapng
Packets/1 sec
0
2
4
6
8
10
12
0
450
900
1350
1800
2250
Time (s)
Hover over the graph for details.
+
−
Help
Reset
Copy
Close
Save As…

Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Field	SMA Period
☑	tcp	ip.src == 19…	🟩	Stacked Bar	Packets		None
□	TCP errors	tcp.analysis…	🟦	Bar	Packets		None

Mouse ● drags ○ zooms   Interval 1 sec   □ Time of day   □ Log scale

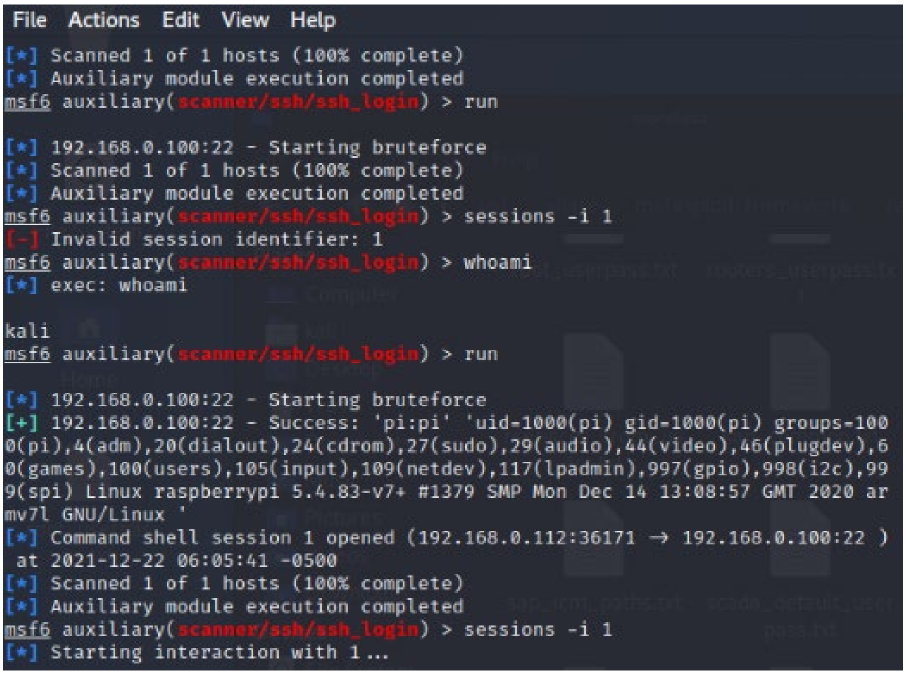
Figure 8: Screenshot from Wireshark demonstrating the SSH brute force attack

Brute force attack on the SSH server

The SSH brute force attack (CMU, 2023) took place in December 2021. Initially the teacher demonstrated an attack using Hydra and then he asked the students to do the same using their own tool (Patator, Medusa, Metasploit) in teams. Three teams were formed from the eleven students. Each team had to find instructions on how to use their tool. Finally, each team should assess the usability of their tool. SSH brute force attack tools usually include a default dictionary with common usernames and passwords. The teams had to add their classmates’ usernames and possible passwords related to their personalities (i.e., use social engineering). Finally, the SSH brute force attacks succeeded. Figure 9 presents a screenshot from the SSH brute force attack using Metasploit.

4.4 Evaluation of the SSH brute force tools

The teams, after using their assigned tool, commented on its efficiency and usability. Medusa and Metasploit got a satisfactory assessment; Patator disappointed their users.



```
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) > run

[*] 192.168.0.100:22 - Starting bruteforce
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) > sessions -i 1
[-] Invalid session identifier: 1
msf6 auxiliary(scanner/ssh/ssh_login) > whoami
[*] exec: whoami

kali
msf6 auxiliary(scanner/ssh/ssh_login) > run

[*] 192.168.0.100:22 - Starting bruteforce
[+] 192.168.0.100:22 - Success: 'pi:pi' 'uid=1000(pi) gid=1000(pi) groups=100
0(pi),4(adm),20(dialout),24(cdrom),27(sudo),29(audio),44(video),46(plugdev),6
0(games),100(users),105(input),109(netdev),117(lpadmin),997(gpio),998(i2c),99
9(spi) Linux raspberrypi 5.4.83-v7+ #1379 SMP Mon Dec 14 13:08:57 GMT 2020 ar
mv7l GNU/Linux '
[*] Command shell session 1 opened (192.168.0.112:36171 → 192.168.0.100:22 )
 at 2021-12-22 06:05:41 -0500
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) > sessions -i 1
[*] Starting interaction with 1 ...
```

Figure 9: Screenshot from the SSH brute force attack using Metasploit

4.5 Use of public keys

After this date followed the Christmas holidays and the final exams of the Fall semester. The scenario continued in the Spring 22 semester, during the Computer Networks II and Network Security courses.

Asymmetric cryptography was taught in Network Security and after that, the corresponding lab exercise (RSA key generation) was implemented in March 2022. The students had to transfer their public keys to the SSH server in order to enable automatic connection and disable username and password login in an effort to reduce the attack surface and make the SSH server immune to brute force attacks.

5. Discussion

5.1 Achieving the learning objectives

In this series of hands-on lab exercises students had the opportunity to interact with real networking hardware and use a variety of tools and methods. The students had to prepare their own devices (laptops and tablets) by installing software. They had the opportunity to try a lot of tools in practice and get valuable practical experience; they also had the chance to see the results of their activities in real time on screen. The scenario kept the students interested till the end; they cooperated harmoniously both with the teacher and among themselves, since some activities were implemented in teams.

From their reports we evaluated the students' achievements which are listed below:

- The students were able to set their IP address, as well as find the IP addresses of the Raspberry Pi and the other users.
- They were able to create a username και password for connecting to the Raspberry Pi.
- They performed a DoS attack on the Raspberry Pi's web server using several tools.
- They performed a brute force attack on the Raspberry Pi's SSH server in teams.
- They found instructions on how to use their tool and assessed the usability of their tool in the end.
- They created a pair of RSA keys and copied their public key to the Raspberry Pi's SSH server.
- Only one out of eleven students managed to verify that his public key was there, as well as, viewed the configuration files of the SSH server using the sftp protocol.

Students' comments were positive; an interview with the aforementioned student who prepared the best report revealed that he gained valuable practical experience and enjoyed the scenario much more than theory. Hence, we conclude the success and the effectiveness of this educational activity.

5.2 Evaluating the students

Ways to assess students both qualitatively and quantitatively, based on their participation and achievements, are presented here. We begin with the quantitative metrics. The following milestones were assessed:

1) Assessment of DoS attacks: each student had to use one of the suggested DoS attack tools against the Web server of Raspberry Pi, until a proper message showing that the page was not available appeared on their screen. The instructor could observe the packet floods in the packet capture (given the students' IP and MAC addresses).
2) The creation of SSH user accounts in the Raspberry Pi SSH server was verified by exploring the students' home directories.
3) The brute-force attacks on the SSH server were verified through the Wireshark packet capture files.
4) The students had to submit a report with their activities as an assignment in the Computer Networks course, describing their activities and supporting them with screenshots.
5) Generating an RSA key pair and uploading the public key to the server was verified by exploring the students' home directories in Raspberry Pi.
6) The students had to submit another report as an assignment in the Network Security course.

The teacher could check student activity during the various steps of the scenario in real time using a variety of tools and methods including monitoring tools (Angry IP Scanner or Advanced IP Scanner), packet captures and Linux terminal commands.

Qualitative assessment was based on the teacher's observations on student participation and interest, as well as their roles in the team activities (leaders, followers or observers).

5.3 Future work

In the future we intend to improve and extend the scenario including additional activities such as:

1) The use of Wireshark, tcpdump and netstat by the students for recording and documenting their attacks.
2) The use of Firewall (iptables, ufw) on Raspberry Pi.
3) The use of Fail2Ban and Snort (**Ghafarian, 2014**) on Raspberry Pi.

We also plan to add more questions to the assignment.

6. Conclusion

This paper presented a cyber security scenario implemented in class using OSS, low-cost infrastructure and students' devices. The students saw how to create an ad hoc Wi-Fi LAN, connect a Raspberry Pi, launch DoS attacks using various tools, monitor the user activities using various tools, capture, monitor and analyse the network traffic, etc. The students got familiar with the Kali Linux platform and virtualisation, created a pair of keys and uploaded the public key to the SSH server so that they could login without username and password; they used three brute force attack tools against the SSH server, as well as assessed these tools.

This educational scenario gave practical lab experience and inspiration to the students, one of which completed the Massive Open Online Course (MOOC) "Networking Essentials" after graduation. Students with practice-oriented learning styles had the opportunity to learn in their own way. So this scenario was used as an alternative assessment activity, instead of exams and tests (**Andreatos and Leros, 2023**). The advantages of the scenario presented are:

- It uses low-cost, off-the-shelf equipment.
- It uses OSS and a variety of tools.
- The experimental infrastructure is inexpensive, portable and fast to install.

The current study verified that to teach technologically advanced topics such as cyber security, innovative teaching and assessment methods need to be applied (**Churi and Rao, 2021).** In the future we plan to improve the scenario in order to include more activities and tools.

Acknowledgements

The author wishes to thank the reviewers for their constructive feedback.

References

Andreatos, A.S. (2017) “Designing educational scenarios to teach network security”, IEEE Global Engineering Education Conference (EDUCON), pp 1606-1610. https://ieeexplore.ieee.org/document/7943063

Andreatos, A. (2020) “Movies as an Aid to Teach Principles of Cybersecurity and Cybercrime in Higher Education”, International Journal of Education and Information Technologies, Vol 14, 2020, pp 76-82.

http://www.naun.org/main/NAUN/educationinformation/2020/a202008-010(2020).pdf, http://doi.org/10.46300/9109.2020.14.10

Andreatos, A. and Leros, A. (2023) “Can Oral Grades Predict Final Examination Scores? Case Study in a Higher Education Military Academy”, accepted for publication in MDPI Analytics.

Cai, Y. (2018) "Using Case Studies To Teach Cybersecurity Courses", Journal of Cybersecurity Education, Research and Practice, Vol 2018, No. 2, Article 3. https://digitalcommons.kennesaw.edu/jcerp/vol2018/iss2/3

Churi, P. and Rao, N.T. (2021) “Teaching Cyber Security Course in the Classrooms of NMIMS University”, International Journal of Modern Education and Computer Science (IJMECS), Vol 13, No. 4, pp 1-15. https://www.mecs-press.net/ijmecs/ijmecs-v13-n4/IJMECS-V13-N4-1.pdf

Ghafarian, A. (2014) "An Empirical Study of network forensics analysis tools", Proceedings of the 9th International Conf. on Cyber Warfare and Security, West Lafayette, Indiana, USA, pp 366-370.

Erickson, M. and Kim, P. (2021) “Designing cybersecurity curriculum: Exploring the need for industry certifications and experiential learning”, Issues in Information Systems, Vol 22, Issue 4, pp 9-20. DOI: https://doi.org/10.48009/4_iis_2021_9-21

Hwang, M.I. and Helser, S. (2022) "Cybersecurity educational games: a theoretical framework", Information and Computer Security, Vol 30 No. 2, pp 225-242. https://doi.org/10.1108/ICS-10-2020-0173

CMU Information Security Office, Protect Against Brute-force/Dictionary SSH Attacks,
https://www.cmu.edu/iso/aware/be-aware/brute-force_ssh_attack.html

Prvan, M. and Ožegović, J. (2020) “Methods in Teaching Computer Networks”, ACM Transactions on Computing Education (TOCE) 20, pp 1–35. https://dl.acm.org/doi/10.1145/3394963

Surma, D. R. (2003) "Lab exercises and learning activities for courses in computer networks", 33rd Annual Frontiers in Education, FIE 2003, Westminster, CO, USA, 2003, pp T2C-21, doi: 10.1109/FIE.2003.1263297.

What is SSH? (2023) [Online]. Available at https://phoenixnap.com/kb/what-is-ssh [accessed 7 March 2023].

Williams, L. (2021) “10 Best FREE DDoS Attack Tool Online (2023)”, Updated January 7, 2023 [Online]. Available at https://www.guru99.com/ddos-attack-tools.html [accessed 7 March 2023].

Yurcik, W. and Doss, D. (2000) “Information Security Educational Initiatives to Protect E-Commerce and Critical National Infrastructures”, Information Systems Education Conference (ISECON), Philadelphia, PA, USA.

Yu, Y. (2007) “Designing hands-on lab exercises in the network security course”, J. Comput. Sci. Coll. 22, 5, pp 105–110.