

ERSC

ENGENHARIA DE REDES E
SISTEMAS DE COMPUTADORES
ESTG-IPVC

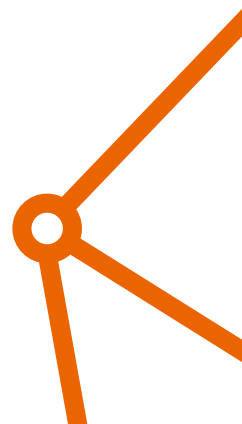
Relatório Trab. no.3 - SIEM / Security Tests

Realizado por por
Romilson Monteiro nº28891
Francisco Oliveira nº 22252
Marco Da Luz nº26476

Supervisionado por
Prof. Hugo Almeida (ESTG-IPVC)



1 May, 2023



Abstract

Índice

1	Introdução	2
1.1	Objetivos do Trabalho	2
1.2	Organização do relatório	2
2	Estado da arte	2
2.1	Arquivo .ova	2
2.2	Interface loopback	3
2.3	SSH	3
2.4	Syscheck	3
2.5	Ataque de Shellshock	3
2.6	File Integrity Monitoring	3
2.7	O ficheiro "ossec.conf"	4
3	WAZUH - HIDS	4
3.1	Instalação do Wazuh	4
3.2	Criação dos agentes wazuh	4
3.2.1	Configuração do agente windows.	5
3.2.2	Configuração do agente ubuntu	5
3.3	Eventos e Alertas	5
3.3.1	Falhas de login	5
3.3.2	Tentativas de acesso não conseguida via ssh	7
3.4	Funcionalidades avançadas- FIM	7
3.5	Detectando um ataque Shellshock	9
3.5.1	Emulação de ataque	9
3.5.2	Visualizar os alertas	9
4	HoneyPots	12
4.1	Implementacao de um honeyPot para posterior monitorização	12
4.2	Idealização e teste de ataque ao IDS-honeypot	12
5	Investigação	13
5.1	Alternativa ao Wazuh	13

1 Introdução

Na disciplina de Criptografia e Segurança nas Comunicações, recebemos uma tarefa do professor Hugo Almeida que consiste na instalação do Wazuh Manager e na configuração de dois agentes, um em Linux e outro em Windows. Além disso, é necessário implementar HoneyPots nas máquinas para monitorar possíveis ataques. Para concluir, devemos apresentar alternativas ao Wazuh e justificar uma comparação mais completa.

1.1 Objetivos do Trabalho

Aqui, apresentaremos os objetivos deste trabalho, que consistem em:

- WAZUH - HIDS:
 1. Instalar o Wazuh Manager em uma máquina com Ubuntu Server 20 LTS e configurar agentes de arquiteturas diversas.
 2. Criar uma sequência de eventos de vários graus de criticidade aplicados ao agente em Linux, que permita recolher alertas no Wazuh Manager. Explicar esses alertas.
 3. Configurar e ativar a funcionalidade FIM (File Integrity Monitoring) e criar um cenário no agente Windows onde possa recolher dados sobre eventos efetuados aos objetos de monitorização.
- HoneyPots:
 1. Implementar um HoneyPot para posterior monitorização, colocando um agente nessa máquina virtual.
 2. Idealizar e testar soluções de ataque ao IDS-HoneyPot anterior.
- Investigação:
 1. Apresentar uma alternativa ao Wazuh, fazendo uma comparação devidamente justificada entre a solução apresentada pelo grupo e a aquela aqui referida.

Este trabalho visa, portanto, explorar diferentes ferramentas de segurança, como Wazuh e HoneyPots, além de avaliar as soluções disponíveis no mercado, a fim de contribuir para a segurança de sistemas de informação.

1.2 Organização do relatório

2 Estado da arte

2.1 Arquivo .ova

Um arquivo com a extensão .ova é usado para disponibilizar uma máquina virtual pré-configurada, no nosso caso o Wazuh, já instalado e pronto para uso. Essa abordagem simplifica e acelera o processo de configuração do Wazuh para os utilizadores, pois não é necessário se preocupar com a instalação e configuração do sistema operativo e do software separadamente.

2.2 Interface loopback

A interface loopback é uma interface de rede virtual presente em todos os sistemas operativos que suportam o protocolo TCP/IP. Ela é usada para permitir que um computador se comunique com seus próprios serviços e processos através da rede, mesmo que não esteja conectado a nenhuma outra rede física.

A interface loopback é geralmente identificada pelo endereço IP 127.0.0.1, que é reservado para uso da interface loopback, é útil para testar e depurar serviços e aplicativos em um computador, sem precisar se conectar a uma rede externa. Por exemplo, um desenvolvedor pode testar um servidor web em seu próprio computador usando a interface loopback, sem precisar implantar o servidor em um servidor externo.

2.3 SSH

SSH (Secure Shell) é um protocolo de rede que permite uma conexão segura e criptografada entre dois dispositivos, geralmente um cliente e um servidor. Ele é usado para gerenciar remotamente dispositivos como servidores, roteadores, switches, entre outros.

2.4 Syscheck

O Syscheck é um componente do sistema de detecção de intrusão Wazuh que realiza a verificação de integridade do sistema operativo e dos arquivos do sistema. Ele compara o estado atual dos arquivos do sistema com uma referência conhecida, ou seja, uma base de dados de integridade. Qualquer alteração nos arquivos do sistema que não esteja de acordo com a referência é considerada uma anomalia e pode indicar uma violação de segurança.

2.5 Ataque de Shellshock

O Shellshock é um tipo de vulnerabilidade de segurança que afeta muitos sistemas operativos baseados em Unix e Linux. O ataque de Shellshock é uma exploração dessa vulnerabilidade, que permite a um invasor executar comandos maliciosos em um sistema afetado.

A vulnerabilidade do Shellshock está relacionada a um recurso do Bash (Bourne-Again SHell), que é um shell de linha de comando comum em sistemas operacionais Unix e Linux. O Bash usa variáveis de ambiente para armazenar informações importantes, como as configurações do sistema e as credenciais de login do usuário. A vulnerabilidade do Shellshock permite que um invasor execute comandos maliciosos através dessas variáveis de ambiente, explorando uma falha de segurança no Bash.

2.6 File Integrity Monitoring

O File Integrity Monitoring (FIM) é uma funcionalidade do Wazuh que monitora a integridade de arquivos em um sistema operativo. O objetivo do FIM é detectar alterações não autorizadas em arquivos críticos do sistema, como arquivos de configuração, executáveis do sistema e arquivos de log.

O FIM funciona comparando periodicamente o estado atual dos arquivos monitorados com um estado previamente registrado em um banco de dados. Se uma alteração é detectada, o Wazuh envia um alerta ao servidor e ao agente correspondente para investigação e possível ação.

Deploy a new agent Close

1 Choose the operating system

Red Hat Enterpris...

CentOS

Ubuntu

Windows

macOS

> Show more

2 Choose the version

Windows XP

Windows Server 2...

Windows 7 +

3 Choose the architecture

i386/x86_64

4 Wazuh server address

This is the address the agent uses to communicate with the Wazuh server. It can be an IP address or a fully qualified domain name (FQDN).

192.168.1.13

Figure 1: configuração de um agente na interface gráfica do wazuh

2.7 O ficheiro "ossec.conf"

O ficheiro "ossec.conf" contém as configurações principais do Wazuh, como as regras de detecção de ameaças, as configurações de integração com outras ferramentas de segurança, as configurações de log e as configurações do agente.

3 WAZUH - HIDS

3.1 Instalação do Wazuh

Para a instalação do wazuh baixamos o arquivo wazuh.ova[1] , que é usado para distribuir máquinas virtuais prontas para uso com o Wazuh já instalado e configurado. Isso torna o processo de configuração do Wazuh mais rápido e fácil, pois não precisamos de preocupar com a instalação e configuração do sistema operativo e do software.

3.2 Criação dos agentes wazuh

Foi necessário criar dois agentes wazuh, um ubuntu e outro windows. Para a criação dos agentes temos que acessar a interface web do wazuh, e na seção "agent" temos que adicionar um no agente, indicando o sistema operativo, a versão do sistema operativo, entre outros parâmetros, como mostra as imagens (1) e (2) . Este processo é idêntico para qualquer sistema operativo.

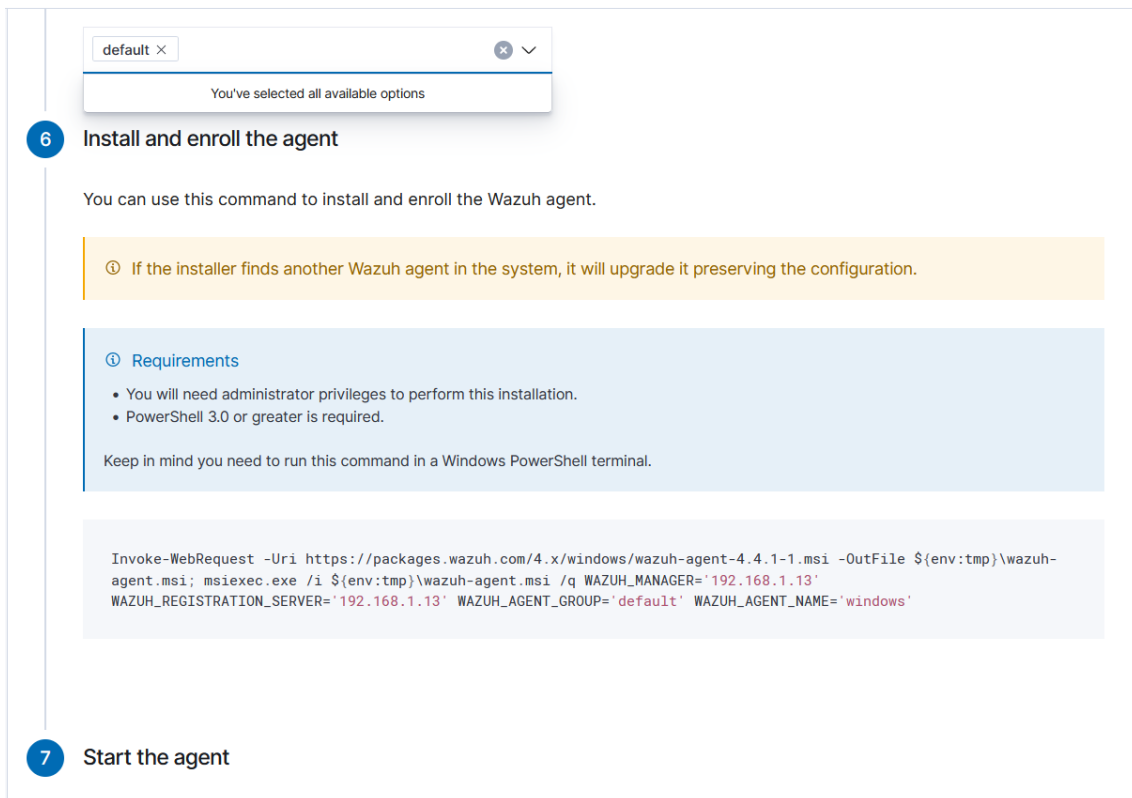


Figure 2: configuração de um agente na interface gráfica do wazuh

3.2.1 Configuração do agente windows.

Com privilégios de administrador, é possível editar o arquivo de configuração do agente Wazuh, denominado ossec.conf, no diretório de instalação correspondente. Como o nosso pc tem uma arquitetura de 64 bits, portanto o caminho completo para o arquivo é: C:\Program Files (x86)\ossec-agent\ossec.conf. No arquivo "ossec.conf" temos que adicionar o ip do wazuh manager, como mostra a figura (3) .

3.2.2 Configuração do agente ubuntu

No agente ubuntu configuramos o ficheiro "/var/ossec/etc/ossec.conf", adicionando o ip do wazuh manager e depois fizemos restart ao agente ubuntu, como mostra a figura (4)

3.3 Eventos e Alertas

Para criar uma sequência de eventos de vários graus de criticidade no agente Linux que permita recolher alertas no manager Wazuh, podemos considerar os seguintes exemplos:

- Falhas de login;
- Falhas no acesso ssh;

3.3.1 Falhas de login

Neste exemplo básico uma tentativa mal conseguida de entrar no sistema por parte de um utilizador, que possivelmente não acertou o seu username ou a sua password, foi reportado pelo agente wazuh, como mostra a figura (5)

```

<!--
Wazuh - Agent - Default configuration for Windows
More info at: https://documentation.wazuh.com
Mailing list: https://groups.google.com/forum/#!forum/wazuh
-->

<ossec_config>

  <client>
    <server>
      <address>192.168.1.13</address>
      <port>1514</port>
      <protocol>tcp</protocol>
    </server>
    <config-profile>windows, windows10</config-profile>
    <crypto_method>aes</crypto_method>
    <notify_time>10</notify_time>
    <time-reconnect>60</time-reconnect>
    <auto_restart>yes</auto_restart>
    <enrollment>

```

Figure 3: Adicionar o ip do wazuh manager no ficheiro ossec.conf do agente windows

```

GNU nano 6.4 ossec.conf
<!--
Wazuh - Agent - Default configuration for ubuntu 22.10
More info at: https://documentation.wazuh.com
Mailing list: https://groups.google.com/forum/#!forum/wazuh
-->

<ossec_config>
  <client>
    <server>
      <address>192.168.1.13</address>
      <port>1514</port>

```

Figure 4: Adicionar o ip do wazuh manager no ficheiro ossec.conf do agente ubuntu

Password Guessing

> Technique details

✓ Recent events

19 hits

DQL

Today
Show dates

 Refresh

+ Add filter

Time ↓	Technique(s)	Tactic(s)	Level	Rule ID	Description
Apr 30, 2023 @ 16:01:18.45 3	T1110.001	Credential Access	5	5503	PAM: User login failed.
Apr 30, 2023 @ 16:01:06.46 2	T1110.001	Credential Access	5	5503	PAM: User login failed.

Figure 5: Tentativa falhada de login

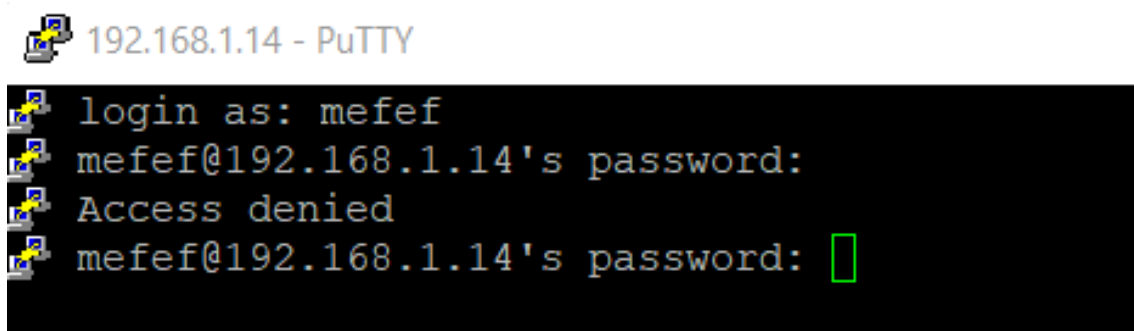


Figure 6: tentativa de acesso via ssh com o putty

3.3.2 Tentativas de acesso não conseguida via ssh

A seguinte imagem mostra a tentativa de login via ssh de um utilizador não registado com o username "mefef" como mostra a figura (6), que foi prontamente reportada pelo agente wazuh, indicando o username e o seu respetivo ip do suposto utilizador como podemos observar na figura (7)

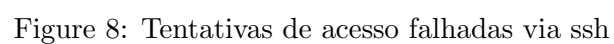
Na seguinte figura (8) podemos observar de forma mais geral algumas tentativas de acesso via ssh falhadas.

3.4 Funcionalidades avançadas- FIM

No nosso caso queremos monitorizar um diretório em específico (integridade), para isso temos de adicionar o caminho, dizer que queremos que ele seja monitorizado o tempo todo e que queremos que as alterações sejam reportadas, essas informações devem ser adicionadas no ficheiro de configuração "ossec.conf" mais precisamente na seção do Syscheck, como mostra a figura(9). O ficheiro de configuração "ossec.conf" contém as configurações principais do Wazuh, como as regras de detecção de ameaças, as configurações de integração com outras ferramentas de segurança, as configurações de log e as configurações do

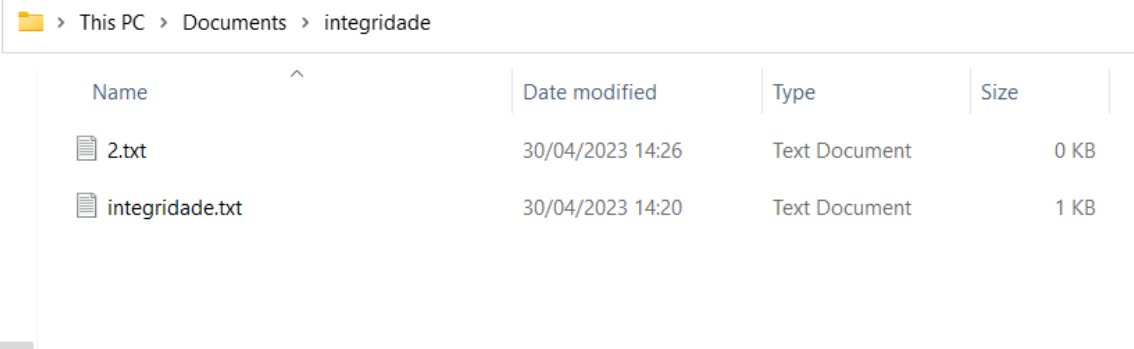
×

Figure 7: Detalhes da tentativa de acesso falhada via ssh



```
<directories check_all="yes" realtime="yes" report_change="yes">C:\Users\Marco da luz\Documents\integridade</directories>
```

Figure 9: adicionar o diretório integridade no ficheiro ossec



Name	Date modified	Type	Size
2.txt	30/04/2023 14:26	Text Document	0 KB
integridade.txt	30/04/2023 14:20	Text Document	1 KB

Figure 10: Diretório integridade

agente. A seguinte figura (10) mostra os ficheiros que estão contidos no diretório "integridade" com os respetivos ficheiros criados para fazer alguns teste relativos a integridade do ficheiro.

Todos as alterações feitas no diretório "integridade" vão ser reportadas, ou seja, se apagarmos um ficheiro, se adicionarmos um ficheiro ou até mesmo uma simples modificação em ficheiro mesmo que adicionando apenas um carácter vão ser reportadas pelo agente wazuh, como mostra as figuras(11) e (12).

3.5 Detectando um ataque Shellshock

Utilizando o Wazuh, é possível identificar a ocorrência de um ataque Shellshock por meio da análise dos registos do servidor da Web, que são coletados a partir de um endpoint monitorado. Em um cenário prático, é possível configurar um servidor web Apache em um endpoint Ubuntu e realizar uma simulação de ataque Shellshock. Fizemos um ataque Shellshock, mas primeiro instalamos um servidor apache no nosso agente ubuntu, como mostra a figura (15). Depois de instalado configuramos o agente Wazuh para monitorar os logs de acesso do seu servidor Apache, para isso temos que fazer algumas modificações no ficheiro `"/var/ossec/etc/ossec.conf"`, como mostra a figura (16), assim sendo o agente Wazuh passa a supervisionar os registos de acesso do nosso servidor Apache.

3.5.1 Emulação de ataque

O seguinte comando (que podemos observar na figura(13)) simula um ataque de Shellshock no nosso próprio servidor apache, um vez que utilizamos o ip `"127.0.0.1"` (ip da interface loopback).

3.5.2 Visualizar os alertas

Podemos visualizar os dados de alerta na interface web do Wazuh. Para isso, temos de aceder o módulo `"security events"`. Como podemos observar na figura (14)).

Time ↓	Path	Action	Rule description	Rule Le...	Rule Id
Apr 30, 2023 @ 14:27:12.282	c:\users\marco da luz\...	added	File added to the sys...	5	554
Apr 30, 2023 @ 14:27:12.019	c:\users\marco da luz\...	deleted	File deleted.	7	553
Apr 30, 2023 @ 14:27:07.812	c:\users\marco da luz\...	added	File added to the sys...	5	554
Apr 30, 2023 @ 14:20:46.873	c:\users\marco da luz\...	modified	Integrity checksum c...	7	550
Apr 30, 2023 @ 14:17:54.367	c:\users\marco da luz\...	modified	Integrity checksum c...	7	550

Figure 11: FIM - Modificações no diretório "integridade"

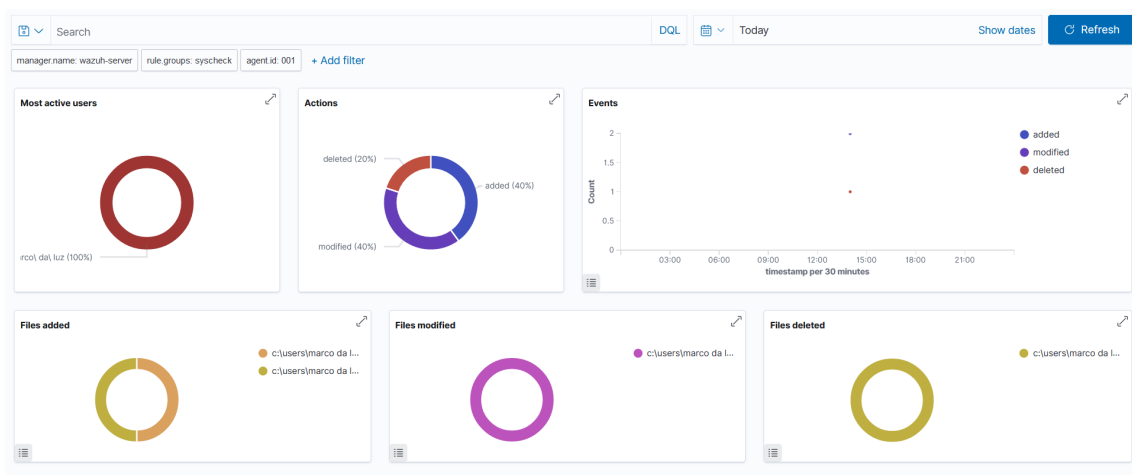


Figure 12: Gráfico com os dados das modificações no diretório "integridade"

```
root@trabalhócriptografia:~# sudo curl -H "User-Agent: () { :; }; /bin/cat /etc/passwd" 127.0.0.1
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
  <!--
    Modified from the Debian original for Ubuntu
    Last updated: 2022-03-22
    See: https://launchpad.net/bugs/1966004
  -->
  <head>
```

Figure 13: Ataque Shellshock

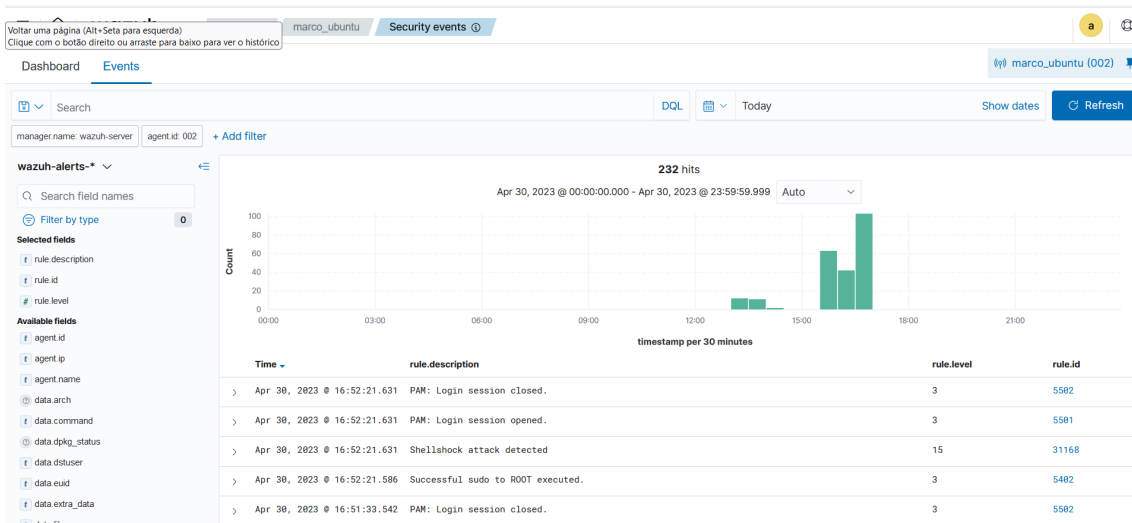


Figure 14: Shellshock ataque detetado pelo wazuh

```
marcoluz@trabalhocriptografia:~$ sudo apt update
sudo apt install apache2
```

Figure 15: Instalação do servidor apache

```
<localfile>
  <log_format>syslog</log_format>
  <location>/var/log/apache2/access.log</location>
</localfile>
```

Figure 16: Modificação do ficheiro ossec.conf

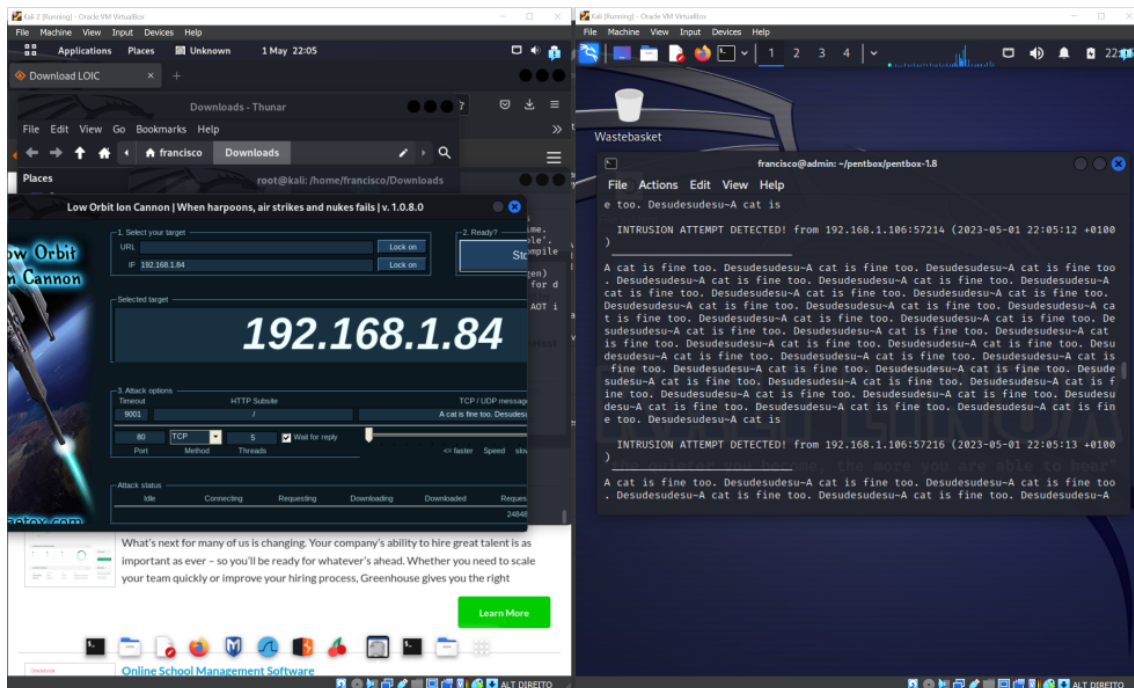


Figure 17: Ataque de DDoS

4 HoneyPots

4.1 Implementacao de um honeyPot para posterior monitorizaçãõ

A implantação de um honeypot pode parecer uma tarefa complexa . No entanto, com as ferramentas certas e um guia confiável, a instalação pode ser realizada de maneira simples e eficiente.

No nosso caso, a implementação do honeypot foi facilitada graças ao link disponibilizado pelo docente. Esse recurso nos levou a um tutorial passo a passo, que nos orientou na instalação da ferramenta Pentbox e, conseqüentemente, na instalação do honeypot na máquina Kali.

A Pentbox é uma ferramenta de segurança cibernética que oferece uma variedade de recursos úteis, incluindo a instalação de honeypots. Com a ajuda dessa ferramenta e do guia fornecido, pude concluir a instalação sem dificuldades e colocar em prática meus estudos em segurança cibernética.

4.2 Idealização e teste de ataque ao IDS-honeypot

Para a resolução do exercício 2.1 realizamos uma breve pesquisa sobre ferramentas para ataques DDoS. O Low Orbit Ion Cannon é uma ferramenta que permite atacar por URL ou IP. Após a inserção dos dados da nossa máquina com o honeypot (PentBox) iniciámos o ataque DDoS e, como se pode observar nos printscreens (17), o PentBox deteta este ataque, mostra o IP do guest que está a realizar este ataque e mostra a mensagem predefinida pelo LOIC.

5 Investigação

5.1 Alternativa ao Wazuh

Durante a pesquisa por alternativas ao Wazuh, encontramos o **OSSEC**[4], um sistema de detecção de intrusão baseado em host, gratuito e de código aberto. Ambas as soluções oferecem funcionalidades semelhantes, como análise de logs, monitorização de integridade, detecção de rootkits e alertas [3], porém, existem algumas diferenças a serem consideradas.

- **Instalação e Configuração:**

Em relação à instalação, tanto o Wazuh quanto o Ossec suportam uma variedade de sistemas operativos, incluindo Windows, Linux e MacOS. Contudo, o processo de instalação e configuração pode ser mais complexo com o Wazuh, enquanto o Ossec possui uma documentação mais completa e fácil de seguir, o que pode tornar a configuração mais rápida e eficiente.

Para instalar o OSSEC, clonamos o repositório com o comando "git clone". Em seguida, navegamos até o diretório onde o repositório foi clonado e executamos o comando "./install.sh" para iniciar o processo de instalação do server OSSEC. Durante a instalação, foram solicitadas algumas informações, como a localização do diretório de instalação e a configuração do servidor de e-mail para envio de alertas. Depois de concluída a instalação, executamos o comando "./ossec-control start" para iniciar o serviço do OSSEC. A instalação (figura .18) foi realizada com sucesso e agora o OSSEC está pronto para ser configurado e utilizado. Para instalar o agente do OSSEC

```
- They can be used to stop SSHD brute force scans,
portscans and some other forms of attacks. You can
also add them to block on snort events, for example.

- Do you want to enable the firewall-drop response? (y/n) [y]: y

- firewall-drop enabled (local) for levels >= 6

-
- 127.0.0.53

- Do you want to add more IPs to the white list? (y/n)? [n]: n

3.5- Do you want to enable remote syslog (port 514 udp)? (y/n) [y]: y

- Remote syslog enabled.

3.6- Setting the configuration to analyze the following logs:
-- /var/log/auth.log
-- /var/log/syslog
-- /var/log/dpkg.log

- If you want to monitor any other file, just change
the ossec.conf and add a new localfile entry.
Any questions about the configuration can be answered
by visiting us online at http://www.ossec.net .

--- Press ENTER to continue ---

5- Installing the system
- Running the Makefile
cc -I./external/compat -DMAX_AGENTS=2048 -DOSSECHIDS -DDEFAULTDIR="/var/os
DHAVE_SYSTEMD -DLIB_SYSTEM -DUSE_PCRE2_JIT -DLIBOPENSSL_ENABLED -Wall -Wex
dcustomemail.o os_maild/sendmail.o os_crypto.a config.a shared.a os_net.a c
imsg-buffer.c -o ossec-maild
```

Figure 18: Instalação do servidor Manager OSSEC

no Windows, baixamos o arquivo de instalação do agente, concluímos a instalação e adicionamos o agente no OSSEC Manager. Exportamos a chave do agente e a copiamos para o agente Windows, iniciando o serviço.(Figura .20)

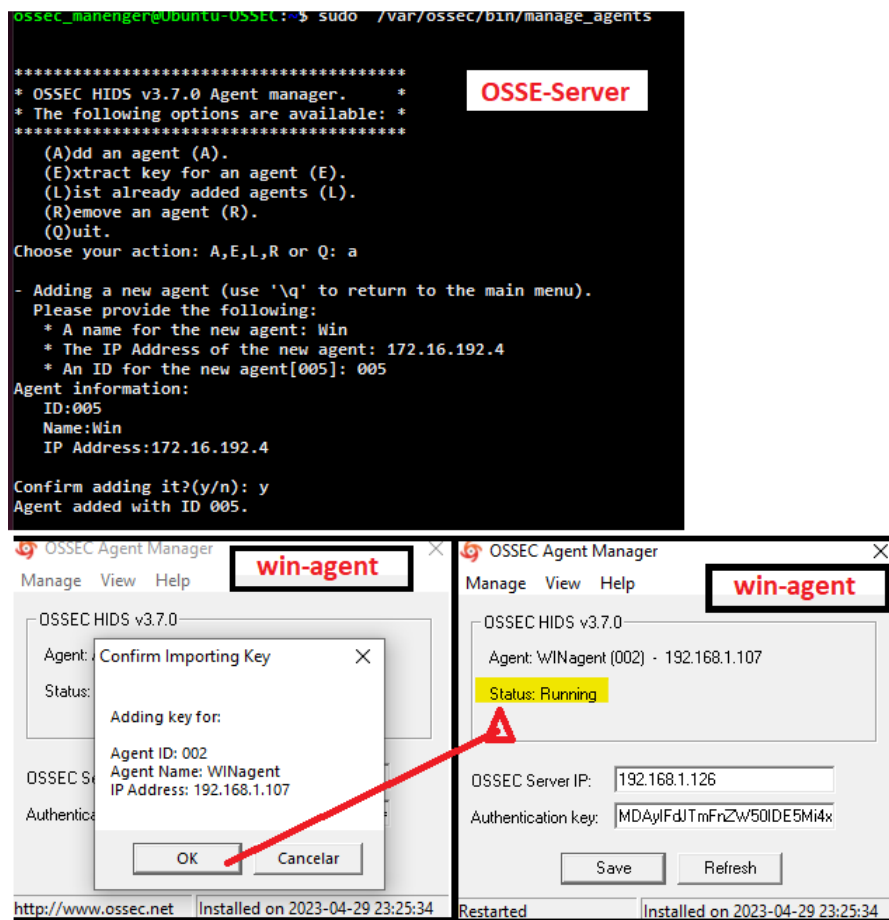


Figure 19: Instalação do agente OSSEC no Windows

Já no Linux, durante a instalação do OSSEC, escolhemos a opção de instalar o agente. Adicionamos o agente no OSSEC Manager, exportamos e copiamos a chave para o agente Linux, reiniciando o serviço.(Figura .20)

```
ossec_manenger@Ubuntu-OSSEC:/tmp/ossec-hids-3.7.0$ sudo /var/ossec/bin/manage_agents

*****
* OSSEC HIDS v3.7.0 Agent manager.      *
* The following options are available: *
*****

(A)dd an agent (A).
(E)xtract key for an agent (E).
(L)ist already added agents (L).
(R)emove an agent (R).
(Q)uit.
Choose your action: A,E,L,R or Q: A

- Adding a new agent (use '\q' to return to the main menu).
Please provide the following:
* A name for the new agent: linux
* The IP Address of the new agent: 192.168.1.124
* An ID for the new agent[001]: 003
Agent information:
ID:003
Name:linux
IP Address:192.168.1.124

Confirm adding it?(y/n): y
Agent added with ID 003.
```

Figure 20: Instalação do agente OSSEC no Ubuntu

- **Funcionalidades Avançadas:**

Quanto às funcionalidades avançadas, o Wazuh destaca-se pela sua capacidade de análise de segurança, com recursos como análise de comportamento e detecção de ameaças [6]. O File Integrity Monitoring (FIM) é uma funcionalidade avançada que está disponível em ambas as soluções, mas a implementação no Wazuh é mais intuitiva e fácil de configurar, o que pode resultar em maior facilidade de uso e menor tempo de configuração.

- **Gestão de Alertas:**

Com relação à gestão de alertas, o Wazuh oferece uma interface de usuário mais fácil de usar e configurar, com várias opções para personalização de alertas. Porém, o Ossec possui uma capacidade mais robusta de correlação de alertas, o que pode ser útil em ambientes de alta densidade de eventos. Sendo assim, dependendo do contexto, uma das duas soluções pode ser mais adequada.

- **Suporte da Comunidade:**

Em termos de suporte da comunidade, ambas as soluções possuem uma comunidade ativa e em crescimento, com fóruns de discussão e documentação disponíveis. No entanto em termos de suporte da comunidade, o Wazuh tem uma comunidade de usuários um pouco maior e uma presença mais forte na indústria de segurança [5], o que pode ser relevante para quem busca soluções mais estabelecidas.

Outra diferença significativa é que o Wazuh oferece uma plataforma de gerenciamento de eventos integrada, permitindo visualizar alertas em tempo real, o que pode tornar a detecção de ameaças mais eficaz e permitir uma resposta mais rápida a incidentes. Por outro lado, o Ossec não oferece essa funcionalidade nativamente.

Abaixo encontram-se alguns pontos fortes de cada um dos dois sistemas:

- **Wazuh**

- Análise de segurança avançada, incluindo análise de comportamento e detecção de ameaças
- Fácil configuração e implementação do File Integrity Monitoring (FIM)
- Interface de usuário fácil de usar e configurar para gestão de alertas
- Personalização de alertas.
- Comunidade de usuários forte e presença na indústria de segurança

- **Ossec**

- Documentação[2] completa e fácil de seguir para instalação e configuração
- Detecção de rootkits e alertas.
- Funcionalidades de monitorização de integridade e análise de logs.
- Capacidade robusta de correlação de alertas.
- Solução de detecção de intrusão baseada em host mais simples e fácil de configurar.

No geral, ambas as soluções são altamente confiáveis e eficazes em suas funcionalidades, mas a escolha entre uma ou outra pode depender de fatores específicos do ambiente e necessidades de cada pessoa ou organização. Na nossa opinião, o Wazuh é uma escolha mais adequada devido à sua interface do usuário amigável e plataforma de gerenciamento de eventos integrada, que tornam a detecção de ameaças mais eficaz e a resposta a incidentes mais rápida.

References

- [1] Wazuh Inc. *Wazuh Virtual Appliance*. <https://wazuh.com/products/installer/download/ova/>. Acessado em 1 de maio de 2023. 2023.
- [2] OSSEC. *OSSEC Documentation*. <https://www.ossec.net/docs/>. Accessed: 2023-04-30. 2021.
- [3] OSSEC. “OSSEC Features”. In: (2023). Accessed on April 30, 2023.
- [4] *OSSEC - Open Source HIDS Security*. <https://www.ossec.net/>. Acesso em: 01/05/2023.
- [5] Wazuh. “Wazuh Community”. In: (2023). Accessed on April 30, 2023.
- [6] Wazuh. “Wazuh Features”. In: (2023). Accessed on April 30, 2023.