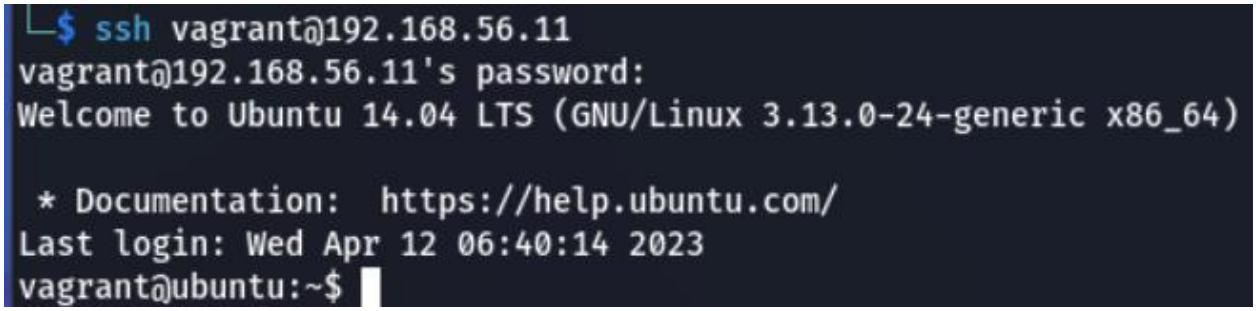
Создала копию ВМ. Подключился к ней по ssh



Настроила ip адрес на eth2. Выполнила apt update.

Установила пакет mod_security для apache2

apt install libapache2-mod-security2

Открыла директорию /etc/apache2/mods-enabled и отредактировала файл

security2.conf

nano /etc/apache2/mods-enabled/ security2.conf

Подключила конфиги правил и конфиг для управления правилами и

действиями. В открытом файле дописала:

Include /usr/share/modsecurity-crs/modsecurity_crs_10_setup.conf

Include "/usr/share/modsecurity-crs/activated_rules/*.conf"

Активировала правила для защиты от XSS

cd /usr/share/modsecurity-crs/activated_rules/

ln -s /usr/share/modsecurity-

crs/base_rules/modsecurity_crs_41_xss_attacks.conf

/usr/share/modsecurity-crs/activated_rules/

modsecurity_crs_41_xss_attacks.conf

Дописала в файл modsecurity_crs_10_setup.conf строки для блокирования

nano /usr/share/modsecurity-

crs/activated_rules/modsecurity_crs_10_setup.conf

SecDefaultAction "phase:1,deny,log" – действие для правил фазы 1.

SecDefaultAction "phase:2,deny,log" – действие для правил фазы 2.

Перезагрузила Apache 2

service apache2 restart

Стандартный конфигурационный файл WAF (/etc/modsecurity/modsecurity.conf) настроен на работу в режиме DetectionOnly, т.е. фаервол отслеживает логи, при этом ничего не блокируя.

Чтобы изменить поведение, нужно в файле:

/etc/modsecurity/modsecurity.conf изменить директиву SecRuleEngine DetectionOnly на SecRuleEngine On.

Прочие полезные директивы:

● SecRequestBodyNoFilesLimit (по умолчанию 131 072 б, или 128 КБ) – ограничивает размер данных POST за вычетом размера файлов

● SecResponseBodyAccess (значения «on» или «off», по умолчанию «on») – доступ к анализу тела ответа. Включение увеличит нагрузку на WAF и логи.

● SecRequestBodyLimit (по умолчанию 13 107 200 б, или 12,5 МБ) – максимальный размер данных POST. Если клиентом будет отправлено больше, будет ошибка 403.