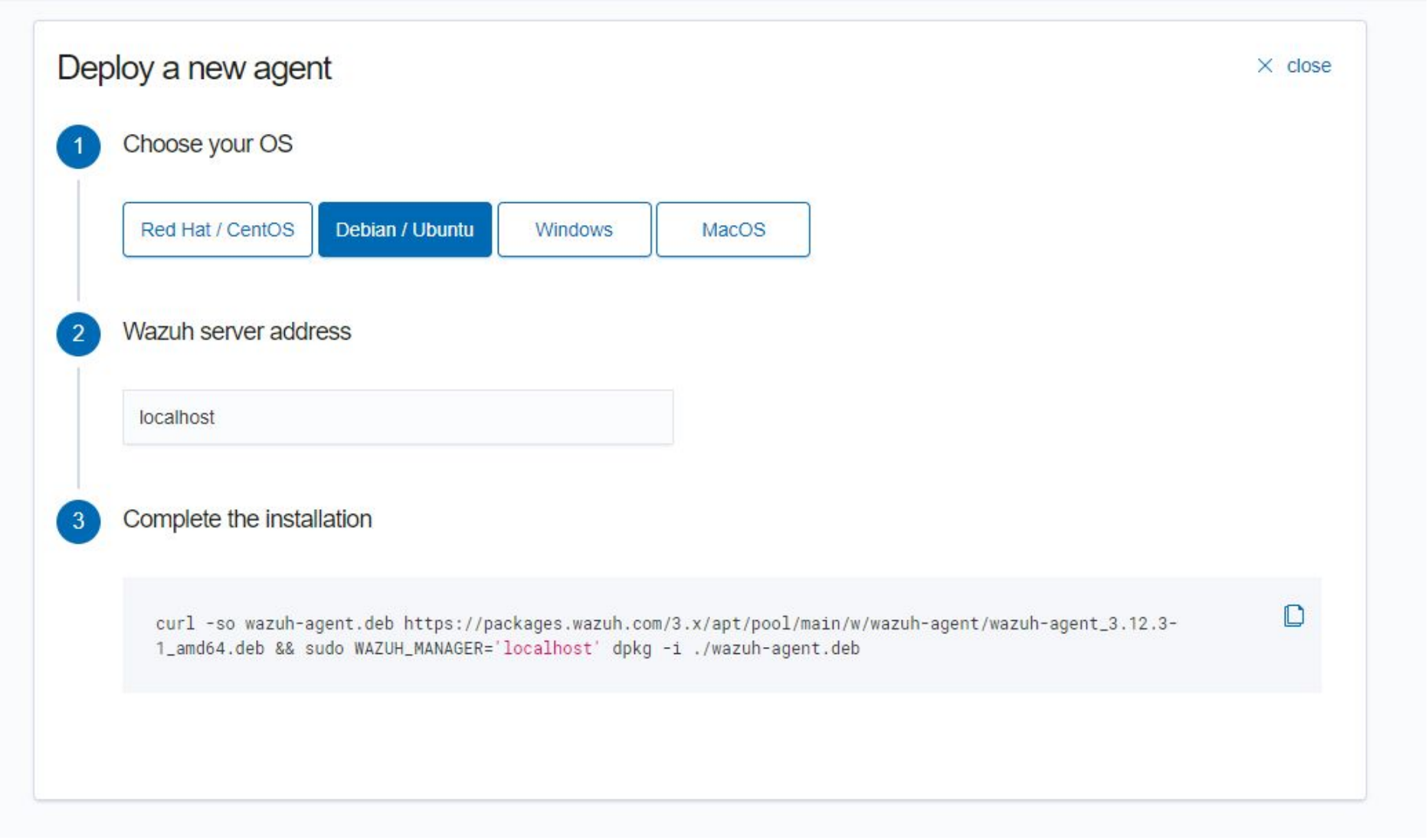
Отчет по работе с Wazuh

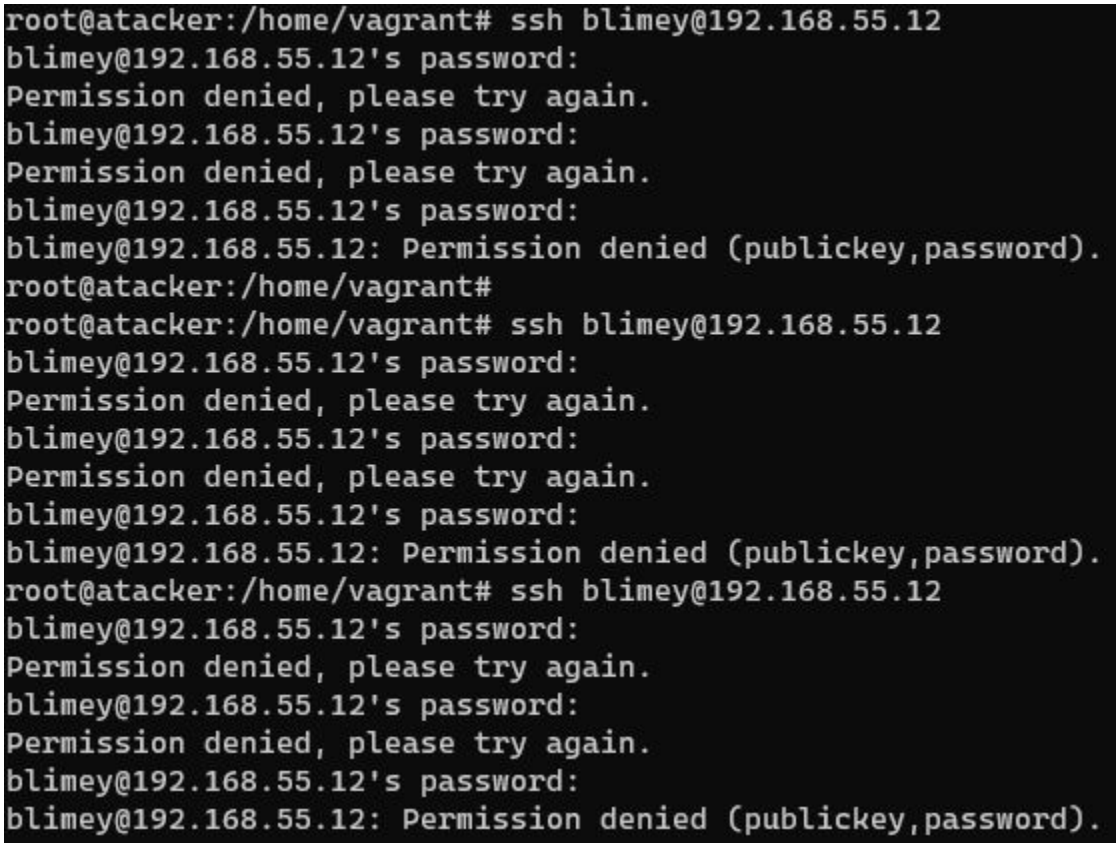
1. Настройка агентских машин.
   При заходе в веб-интерфейс кибаны, переходим в wazuh ->add new agent



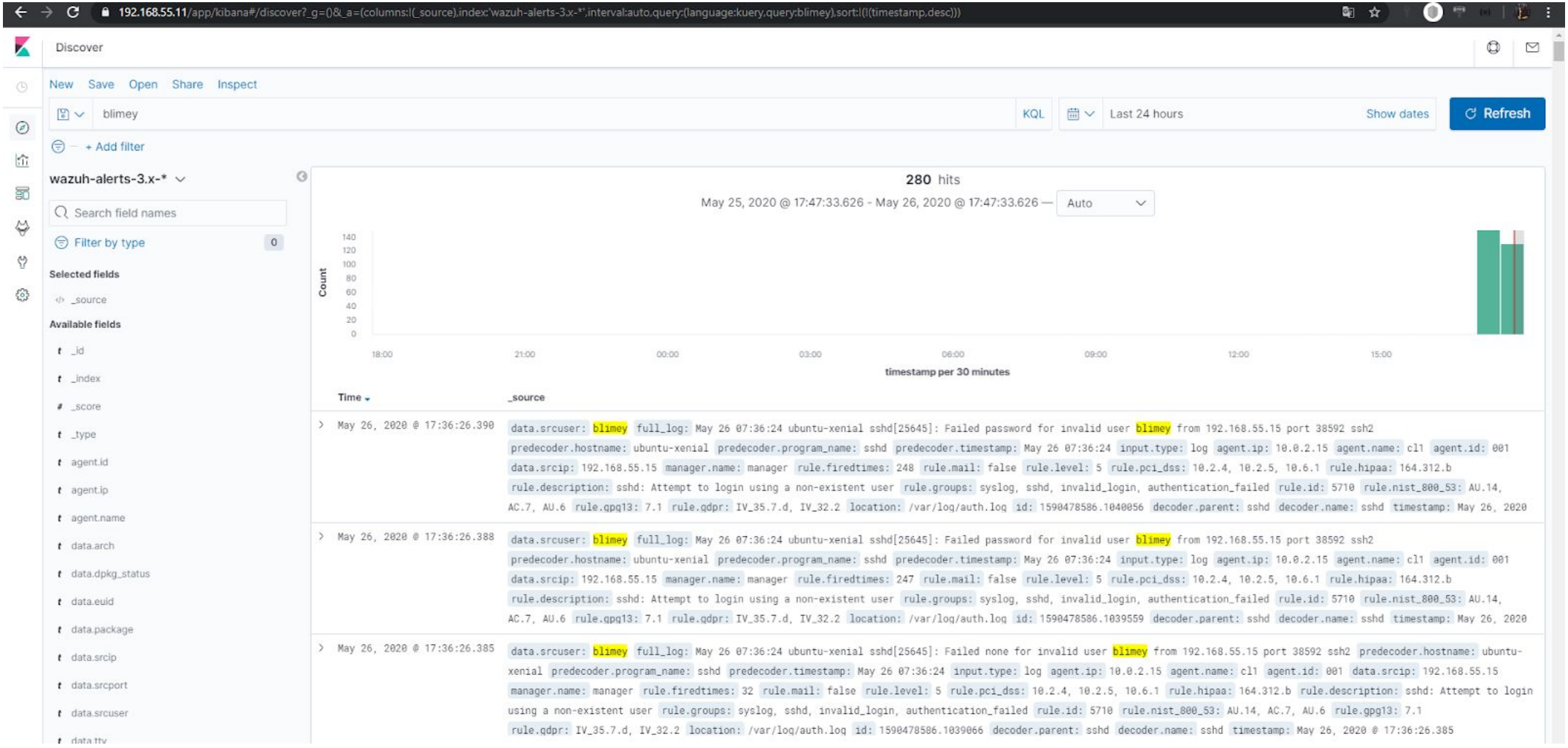
копируем строку инсталляции, заменяя localhost на ip-адрес сервера в нашем случае на 192.168.55.11 и выполняем на клиентских машинах. Данная часть реализована в **provision.sh** для **Vagrantfile**

2. Брутфорс-атака.

   После всех настроек пытаемся по ssh подключиться к одной из клиентских машин имитируя попытку брутфорс атаки.



3. В кибана проверяем наличие Alert-ов



4. Правила сработки брутфорса ssh.

```
[root@manager etc]# ID=5712; rulefiles=/var/ossec/ruleset/rules/*.xml; grep 'i
d="'$ID'"' $rulefiles -l; sed -e '/id="'$ID'"/,/\/rule>/!d' $rulefiles;
/var/ossec/ruleset/rules/0095-sshd_rules.xml
  <rule id="5712" level="10" frequency="8" timeframe="120" ignore="60">
    <if_matched_sid>5710</if_matched_sid>
    <description>sshd: brute force trying to get access to </description>
    <description>the system.</description>
    <same_source_ip />
    <group>authentication_failures,pci_dss_11.4,pci_dss_10.2.4,pci_dss_10.2.5,
gdpr_IV_35.7.d,gdpr_IV_32.2,hipaa_164.312.b,nist_800_53_SI.4,nist_800_53_AU.14
,nist_800_53_AC.7,</group>
  </rule>
[root@manager etc]#
```

5. Настройка active response на брутфорс ssh в wazuh

В wazuh уже имеются готовые скрипты для active response, находятся в каталоге /var/ossec/active-response/bin/. Для автоматической блокировки атакующего ip в файл /var/ossec/etc/ossec.conf необходимо добавить правило:

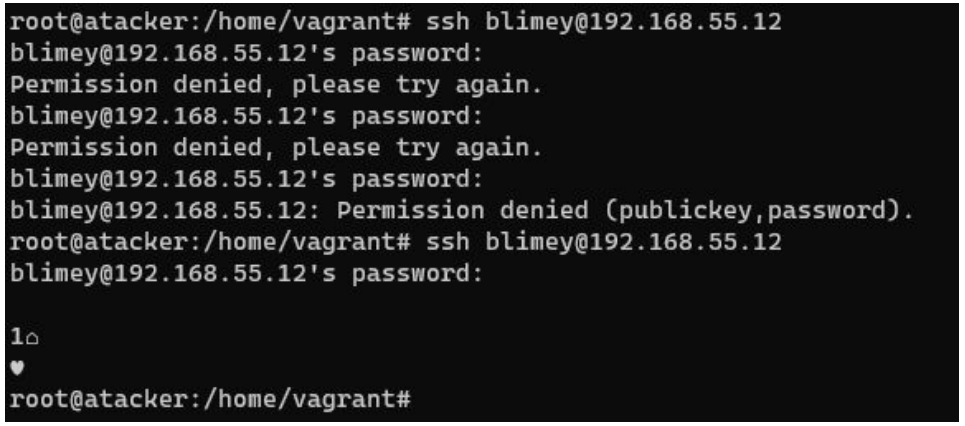
```
<active-response>
    <command>firewall-drop</command>
    <location>local</location>
    <rules_id>5712|5720</rules_id>
    <timeout>1800</timeout>
</active-response>
```

firewall-drop - название скрипта, **rules id** - идентификатор события безопасности "**sshd: brute force trying to get access to the system.|sshd: Multiple authentication failures.**". Первое правило срабатывает если злоумышленник не знает логин для

ssh. Второе правило затруднит возможность подобрать пароль если по какой то причине злоумышленник смог узнать имя пользователя для ssh. При данной настройке блокировка будет производиться только на хосте, который подвержен атаке.

6. Проверка правила.

   снова пытаемся выполнить брутфорс атаку



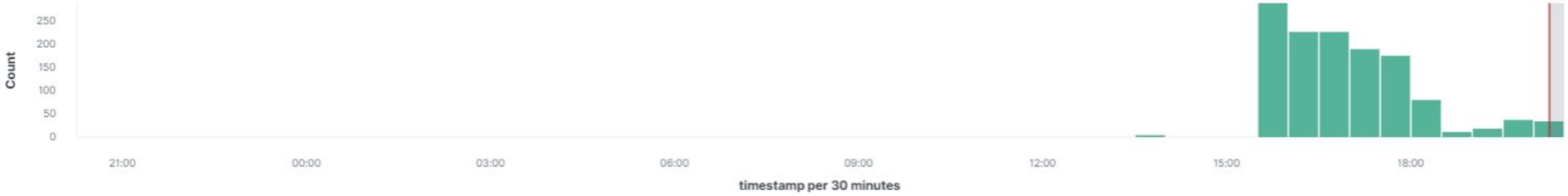
   iptables атакованной машины до и после атаки

```
root@cl1:/var/ossec/etc# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@cl1:/var/ossec/etc# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  192.168.55.15        anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  192.168.55.15        anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@cl1:/var/ossec/etc#
```

Проверяем в wazuh что правило отработало.

1,288 hits

May 25, 2020 @ 20:15:30.561 - May 26, 2020 @ 20:15:30.561 — Auto



	Time	rule.description	data.srcuser	rule.id
>	May 26, 2020 @ 20:09:10.735	Host Blocked by firewall-drop.sh Active Response	-	601
>	May 26, 2020 @ 20:09:08.738	sshd: Attempt to login using a non-existent user	blimey	5710
>	May 26, 2020 @ 20:09:08.736	syslog: User missed the password more than one time.	-	2502
>	May 26, 2020 @ 20:09:08.732	sshd: brute force trying to get access to the system.	blimey	5712
>	May 26, 2020 @ 20:09:04.738	sshd: Attempt to login using a non-existent user	blimey	5710
>	May 26, 2020 @ 20:09:02.720	sshd: Attempt to login using a non-existent user	blimey	5710