

**CYBER STRUGGLE**

**TASK- STAY ALERT, STAY ALIVE**

**Hazırlayan:**

**DCS001 Hakan ŞEN**

**Ekim 2023**

**Ankara**

Dear Security Team,

URGENT : Immediate Action Required - Port Scan Alert

Our security systems have detected port scans, indicating potential intrusion attempts on our network. We must act swiftly to assess the situation.

Your task is to use our SIEM solution, Splunk, to identify and document any port scans involving more than 20 ports within a 5-minute timeframe. Time is of the essence, and we need to understand the extent of this threat promptly.

Also explain what log sources can be used to collect port traffic logs for further collection of logs? How can we distinguish normal port traffic from port scan ?

Thank you for your immediate attention and dedication to our security.

Stay vigilant and proactive.

Best regards,

Jennifer Lee

Senior Security Analyst

Bravo Solutions Ltd.

Note: Use the index "network".

Öncelikle port taramasını Vertical ve Horizantal olarak ikiye ayırabiliriz.

Vertical Port Scan = bir ip tek bir sistem üzerinde birçok porta tarama yapabilir.

Horizontal Port Scan = bir ip birden çok sistemi tek bir port için tarayabilir.

Task’tan anlaşıldığı üzere 20 üzerinde port taraması içeriği istendiğinden vertical port scan’e yönelik olarak bir araştırma yapmamız gerektiği değerlendirilmiştir.

|  |
| --- |
| index="network" source="cisco\_firewall.cef" | bin \_time span=5m | stats dc(dpt) as dc\_dest\_port by src, dst | where dc\_dest\_port > 20 |

A screenshot of a computer

Description automatically generated

Aslında iki yöntemide tek bir yerde toplayarak port veya network taramasını aşağıdaki sorgu ile kontrol edilmesinde fayda olacağını değerlendiriyorum.

|  |
| --- |
| index="network" source="cisco\_firewall.cef"|bin \_time span=5m |stats dc(dpt) as num\_dest\_port dc(dst) as num\_dest\_ip by src |where num\_dest\_port >20 OR num\_dest\_ip >20 |

A screenshot of a computer

Description automatically generated

Port taramasına yönelik olarak ip ve port bilgisini tutan firewall, IPS veya IDS, Switch, Router, Proxy Serverları, Uygulama Logları kullanılabilir.

Port taramasını normal trafikten ayırmak için;

Tarifiğin paternlerine bakılabilir, Örnek normal bir trafik düzenli ve beklenen bir iletişme sahipken port taramasında hızlı ve değişik portlara beklenmedik istekler gidecektir.

Başarı sayısına bakılabilir, örnek olarak normal trafik genellikle başarılı bağlantı kurarken port taramasında başarısız bağlantılar dikkat çekecektir.

TCP Flaglari dikkat çeker. Normal bağlantı düz bir şekilde 3 way handshake’i tamamlarken port taraması sadece SYN gönderebilir.

Bilinen servislere ulaşım sayısına bakılabilir. Örnek normal bir trafikte bilinen servisler arasında iletişim varken port taramasında bilinen servislerin dışına da bir istek bulunacaktır.