NMAP Kullanılarak EKS/SCADA Sistemlerinde Aktif Tarama/Bilgi Toplama

10.04.2019

Yazar: Murat Aydemir

Sürüm 1.2

NMAP Kullanılarak EKS/SCADA Sistemlerinde Aktif Tarama/Bilgi Toplama

Endüstriyel Kontrol Sistemleri(EKS) ve Supervisory Control and Data Acquisition (SCADA) sistemleri, elektrik iletim/üretim ve dağıtım işletmelerinde, enerji ve nükleer santrallerde, kimyasal fabrikalarda, rafinerilerde, su ve arıtma işletmelerinde ve daha büyük endüstriyel komplekslerde bulunan kritik altyapıların bir parçasıdır. Endüstriyel işletmelerin artan verimlilik talepleri, tüm dünyayı etkisi altına alan dijitalleşme trendi ve belkide en önemlisi; IT-OT yakınsamasının kontrolsüz bir şekilde artması Kritik Altyapılar için yeni atak yüzeyleri oluştururken, izleme (monitoring) teknolojilerinin gelişmesi ve OT bileşenler arasındaki bağlantıyı(connectivity) iyileştirmeyi amaçlayan yeni nesil ağ teknolojileri, EKS ve Kritik Altyapıları "özelleşmiş OT ağı saldırıları" olarak isimlendirilen yeni atak vektörlerinin hedefi haline getirmeye başladı.

EKS güvenliği alanında yapılan çalışmalar incelendiğinde, endüstriyel organizasyonlarda bulunan izole edilmiş şebeke ve yapıların bir parçası olduğu düşünülen OT ağ ve sistemlerinin, İnternet'e doğrudan veya dolaylı bir şekilde bağlı ve uzaktan erişilebilir olduğu görülmektedir. İstatistiki analiz sonuçlarına göre; bu şekilde internete doğrudan erişimi bulunan kritik altyapıların sayısının sürekli olarak arttığı görülmektedir. Siber güvenlik uzmanlarının EKS' ler üzerine yaptığı analizler; bu alanda kullanılan birçok protokol ve ürünün evrensel güvenlik gerekliliklerini sağlamadığı ve bunun sonucu olarak siber saldırılara karşı savunmasız olduğunu işaret etmektedir.

Nmap; EKS-OT ağların için sızma testleri yapılırken, aktif bilgi toplama(active information gathering) aşamalarında kullanılan open source bir araçlardan bir tanesidir. Nmap bilinenin aksine sadece port taraması yapmakla kalmaz, desteklediği Nmap Script Engine(NSE) paketleriyle birlikte işletim sistemi bilgisi, kullanıcı listeleme(user enumeration), framework ve versiyon bilgisi gibi çok çeşitli özelleşmiş amaçlar içinde kullanılabilmektedir.

Biznet Bilişim EKS ekibi olarak yaptığımız saha çalışmalarında, "geleneksel IT güvenlik araçlarının OT ortamlarında nasıl kullanılabileceği" sıkça karşılaştığımız sorulardan bir tanesiydi. Bu sebepten dolayı "NMAP Kullanılarak EKS/SCADA Sistemlerinde Aktif Tarama/Bilgi Toplama" isimli bu yazıyı kaleme aldık.

Bu yazıda, EKS/SCADA sistemlerinin Nmap kullanılarak nasıl tarandığından bahsedilmekle beraber, OT ağlarında bulunan farklı protokolleri tanımlanıp, BACnet, EtherNET/IP, PC Worx, Modbus gibi birçok protokolü destekleyen endüstriyel cihazlar için "Nmap aracı ile nasıl tarama yapılır?" sorusunun cevabını verilmektedir.

1-) Nmap ile EKS/SCADA Sistemlerinde Kullanılan Genel Portların Durum Bilgisi Tespiti

Endüstriyel Kontrol Sistemleri(EKS) hem hizmet ettikleri amaçlar hem de yapısal ve foksiyonel işleyiş bakımından geleneksel IT ortamlarından oldukça farklı bir yapıya sahiptir. EKS'ler tasarlanırken, -bakım ve planlı duruşlar haricinde- uzun yıllar boyu ve sürekli(durmadan) olarak çalışabilecek (işletmeye bağlı olmakla birlikte en az 5-7 yıl) sistemler olarak tasarlanmaktadır. Bu durum, uzun yıllar boyunca hiçbir şekilde güvenlik yaması geçilmemiş, framework güncellemesi yapılmamış ve üzerinde çeşitli zafiyetler barından çok sayıda endüstriyel cihazla dolu bir OT ağı oluşturmaktadır.

Kritik Altyapılarda gerçekleştirilen aktif taramalar -bazı durumda ping taramaları bile- ilgili cihazlara geri dönülmez bir şekilde hasar verebildiği ya da sistemlerin manuel olarak yeniden başlatılması gibi endüstriyel proses açısından kritik sonuçlardan doğurabildiğinden dolayı, OT ağına paket gönderilen herhangi bir aktif tarama yapılırken IT ortamlarına göre çok daha hassas ve dikkatli olmak gerekmektedir. Tarama sonucunda doğabilecek hasar veya sistemdeki aksamalar finansal olarak ciddi kayıplara yol açacağı gibi -özellikle üretim alanlarında- ölümcül sonuçlarda doğurabileceği gibi çevre ve doğa hasarları da gerçekleşebilmektedir. Bu nedenle amacımızı; "tarama yaparken mümkün olduğunca çok bilgi toplamak, fakat bunu yaparken agresif bir tutum içerisinde olmak yerine ağa mümkün olduğu kadar az paket gönderilerek ve ilgili sistemler asgari ölçüde yoracak yöntemler kullanarak taramaları gerçekleştirmek" olarak belirlemek daha güvenli bir sızma testi gerçekleştirilmesine olanak sağlayacaktır.

-UYARI-

Bu yazıda bulunan aktif tarama/bilgi toplama metodlarının gerçek Kritik Altyapılar ya da endüstriyel ağlarda kullanılması sonucunda oluşabilecek olası hasar, kayıp vb. durumlarından Biznet Bilişim sorumlu değildir.

Aşağıdaki nmap komutu EKS/SCADA sistemlerinde ürünlerin genellikle kullandığı portların durum bilgisi vermektedir.

```
$ nmap -Pn -sT --scan-delay 1s --max-parallelism 1 -p80, 102, 443, 502, 530, 593, 789, 1089-1091, 1911, 1962, 2222, 2404, 4000, 4840, 4843, 4911, 9600, 19999, 20000, 20547, 34962-34964, 34980, 44818, 46823, 46824, 55000-55003 <hedef>
```

Yukarıda listelenen portlar, endüstriyel ağlarda en sık karşılaşılan ve çeşitli endüstriyel protokollerinin kullandığı varsayılan portlara karşılık gelmektedir. Aynı portu kullanan başka bir servis olması durumunda "false positive" olarak isimlendirilen durumların ortaya çıkacağını da unutmamak gerekir. Tarama sonucu çıktısı ise aşağıdaki formatta gözükmektedir.

```
PORT    STATE SERVICE
502/tcp open  modbus
```

Nasıl Çalışır?

Nmap tarama yaparken hedef sistem ile protokol seviyesinde bağlantı kurmayı temel almaktadır. Bu bağlantı bilgi toplamak/aktif tarama yapmak istenilen sistemin veya cihazın kullandığı protokole bağlı olmakla beraber TCP yada UDP seviyesinde olabilir. Örneğin, yukarıdaki tarama komutunda "host discovery" olarak isimlendirilen ve hedef ağdaki canlı (up) sunucuları listelemeye/belirlemeye yarayan "-Pn" komutu kullanılmamıştır. EKS/SCADA sistemlerinin çoğunun eski ve kırılgan bir yapıya sahip olması işletim sistemi, sürüm bilgisi ve agresif NSE taramalarında sistem üzerinde olumsuz etki/etkiler bırakmasına yol açabilmektedir. Bu sebeple tarama yapılırken zaman ve performans parametreleri dikkat edilmelidir.

Bu parametreleri örneklerle açıklamak gerekirse "--scan-delay <parametre(saniye)>" opsiyonu; TCP, UDP yada ICMP paketleri gönderilirken olası kayıp (package loss) durumunlarında, bir sonraki paket gönderiminin (retransmission) ne zaman başlayacağını belirtmektedir.

"--max-parallelism <parametre>" bir paketin aynı anda kaç farklı hedefe gönderileceğini belirlemekte kullanılan bir opsiyondur. Bu opsiyon genelde port taraması ve varlık keşfi (host discovery) durumlarında kullanılmaktadır. Nmap varsayılan olarak, ağ performansına göre sürekli değişen bir paralellik sağlamakla birlikte, ilgili parametre kullanılarak girerek ilgili paketin aynı anda kaç farklı hedefe gönderileceğini belirler ve böylece aşırı yük ve performans sorunlarından oluşabilecek ağ problemlerini minimize edebilir.

Aşağıda EKS/SCADA sistemlerinde yaygın olarak kullanılan protokoller ve ilgili protokollerin kullandığı port numaralarını gösterilmektedir.

PROTOKOL	**PORT**
BACnet/IP	UDP/47808
DNP3	TCP/20000, UDP/20000
EtherCAT	UDP/34980
Ethernet/IP	TCP/44818, UDP/2222, UDP/44818
FL-net	UDP/55000 - 55003
Foundation Fieldbus HSE	TCP/1089 to 1091, UDP/1089 to 1091
ICCP	TCP/102
Modbus TCP	TCP/502
OPC UA binary	Üretici uygulamasına özel
OPC UA discovery server	TCP/4840
OPC UA XML	TCP/80, TCP/443
PROFINET	TCP/34962 to 34964, UDP/34962 to 34964
ROC PLus	TCP/UDP 4000
Red lion	TCP/789
Niagara Fox	TCP/1911, TCP/4911
IEC-104	TCP/2404

2-) Human Machine Interface(HMI) Sistemlerinin Tespiti

HMI sistemleri EKS/SCADA altyapılarında bulunan ve sahadaki verilerin grafiksel olarak anlamlandırılıp operatörler tarafından izlenmesine olanak sağlayan kontrol sistemleridir. Bu sistemler diğer EKS/SCADA cihazlarıyla aynı portta çalışması zorunlu değildir. Bununla birlikte, bazı HMI'lar EKS protokollerini

kullanmaktadır. Örneğin, "Sielco Sistemi Winlog" uygulaması, uzaktan erişimlerin herkese açık olduğu PC'ler için basit ama çok popüler bir HMI yazılımdır.

Aşağıdaki Nmap komutu Sielco Sistemi Winlog HMI uygulaması için örneklendirilmiştir.

```
$ nmap -Pn -sT -p46824 <hedef>
```

Nasıl Çalışır?

Sielco Sistemi Winlog sunucusu TCP port 46824 üzerinde çalışmaktadır. "-Pn" opsiyonu ile hedef sistemin canlı olup olmadığı kontrolünün yapılması engellenmiştir. Farklı HMI uygulamaları için port numarası farklılık göstermekle beraber, tarama tekniği sistemin kritikliği performans gereklilikleri gibi parametrelere göre farklılık gösterebilmektedir.

Aşağıda EKS/SCADA sistemlerinde kullanılan HMI'lar için TCP port numaraları gösterilmektedir.

ÖZELLİK	**TCP PORT**
Remote HMI	8000
HMI project download	20248
VNC Viewer*	5900
VNC Http&Java**	80&5800
Ethernet Pass-through	2000
Printer Server	8005
Debugging	8001
EasyDiagnoser	8001

**: Bazı HMI yazılımları web uygulaması şeklinde olup varsayılan http protokol portlarını (80, 443 vb.) kullanabilmektedir.
*: Sık karşılaşılan bir durum olmamasına rağmen, bazı HMI yazılımları VNC üzerinden, varsayılan VNC portlarını (5800, 5900 vb.) kullanabilmektedir.

3-) Siemens SIMATIC S7 PLC'ler İçin Bilgi Toplama

Endüstriyel Kontrol Sistemleri'nde sahadaki ısı, sıcaklık, nem, basınç sensörleri, motor sürücüleri, regülatör devreleri gibi kritik enstürmanları kontrol etmek için kullanılan en yaygın ekipmanlardan birisi de Programmable Logic Controller(PLC)'lerdir. PLC'ler kontrolcü olarak çalışıp basınç, akış, sıcaklık, hareket kontrolü ve tüm süreç değişkenlerini yönetmek için otomatik kontrol fonksiyonları sağlayan özel bir dillerde programlanabilmektedir. Genelde her üreticinin PLC'ler için kendi programlama dillerini oluşturduğu görülse de, bu diller arasında yapısal ve fonksiyonalite bakımından büyük farkların olmadığı bilinmektedir.

S7 300/400 ailesinden olan Siemens S7 PLC cihazları, PLC'ler ve SCADA sistemleri arasındaki veri iletişimini için S7comm -ya da doğrudan S7- olarak isimlendirilen üreticiye özel bir protokol kullanmaktadır. Bu cihazlar normal olarak 102 numaralı portu (iso-tsap) dinler ve komut dosyası altyapısını kullanarak aygıtlardan bilgi edinmek için bazı tanılama(diagnostics) işlevlerinde kullanılır.

Aşağıdaki Nmap komutu Siemens SIMATIC S7 PLC' ler için örneklendirilmiştir.

```
$ nmap -Pn -sT -p102 --script s7-info <hedef>
```

Tarama sonucu çıktısı ise aşağıdaki formatta gözükmektedir.

```
PORT    STATE SERVICE
102/tcp open  iso-tsap
| s7-info:
|   Module: 6ES7 420-2FK14-1DB3
|   Basic Hardware: 6ES7 420-2FK14-1DB3
|   Version: 3.2.11
|   System Name: SIMATIC 300(1)
|   Module Type: CPU 317F-2 PN/DP
|   Serial Number: S C-F1UB42002417
|_  Copyright: Original Siemens Equipment
Service Info: Device: specialized
```

Nasıl Çalışır?

s7-info scripti bize Siemens SIMATIC S7 PLC'ler hakkında bilgi vermektedir. İlgili script Siemens tarafından geliştirilmiş olan s7comm protokolü üzerinden PLC cihazlarını algılamaktadır. Yukarıdaki komutta, hedef sistem üzerindeki 102 numaralı port ile bağlantı kurulur ve devamında "s7-info" scripti sayesinde hedef PLC için bilgi toplamaktadır.

4-) Modbus Cihazlar İçin Bilgi Toplama

Modbus, birçok SCADA cihazlarının veri iletimi/haberleşmesi için kullandığı TCP/IP bazlı, usta/köle(master-slave) temelli bir protokoldür. Eski bir protokol olmakla beraber hala EKS sistemlerinde kullanılan en popüler protokollerden birisidir. Bu protokol ile ilgili cihaz ve üzerinde çalışan firmware/yazılım hakkında bilgi almak mümkündür. Eski bir protokol olduğundan veri iletişimi düz metin(cleartext) olarak gerçekleşse de RS 232/485 (RTU ve ASCII standartları için) arabirimlerini desteklemektedir.

Aşağıdaki Nmap komutu Modbus protokolü için örneklendirilmiştir.

```
$ nmap -Pn -sT -p502 --script modbus-discover <hedef>
```

Tarama sonucu çıktısı ise aşağıdaki formatta gözükmektedir.

```
PORT    STATE SERVICE
502/tcp open  modbus
| modbus-discover:
|   sid0x0:
|_    Slave ID data: \xB4\xFFLMB3.0.3
```

Nasıl Çalışır?

modbus-discover scripti Modbus aygıtlarını ve bunların bağımlı kimlik bilgilerini(slave ID) numaralandırır. İlgili script default olarak ilk önce slave ID değerini göstermektedir fakat NSE bu ayarı yapılandırmamıza izin vermektedir. "-sT" tarama tekniği kullanılarak hedef ile TCP bağlantısı kurulmuş ve "-Pn" opsiyonuyla sunucu keşif(host discovery) kontrolü yapılmamıştır.

İlgili script bazı cihazlar için ise daha fazla bilgi toplayabilmektedir.

```
PORT    STATE SERVICE
502/tcp open  modbus
| modbus-discover:
|   sid0x64:
|     Slave ID data: \xFA\xFFPM710PowerMeter
|_    Device identification: Schneider Electric PM710 v03.110
```

Modbus için tarama yapılırken ilgili script argümanı agresif olarak ayarlanarak tüm slave ID' ler listenecek şekilde konfigüre edilebilir.

```
$ nmap -sT -Pn -p502 --script modbus-discover --script-args modbus-discover.aggresive=true <hedef>
```

Yukarıdaki komut çalıştırıldığı zaman, ilgili script agresif modda çalışarak ilk 256 slave ID'yi bulmaya çalışacaktır. Yukarıdaki komut çıktısı ise aşağıdaki formatta gözükmektedir.

```
PORT    STATE SERVICE
502/tcp open  modbus
| modbus-discover:
|   sid0x0:
|    Slave ID data: \xB4\xFFLMB3.0.3
|   sid0x1:
|     Slave ID data: \xFA\xFFPM710PowerMeter
<edited for conciseness>
|   sid0x64:
|     Slave ID data: \xFA\xFFPM710PowerMeter
|_    Device identification: Schneider Electric PM710v03.110
```

5-) BACnet Cihazlar İçin Bilgi Toplama

BACnet; açık sistem haberleşme protokolü olup, bu protokolü kullanan cihazlar güç ve havalandırma sistemlerini ve bina otomasyon sistemlerinde diğer birçok bileşeni birbirine bağlamak ve kontrol etmek için sıkça kullanılmaktadır. NSE kütüphanesinde bulunan scriptler kullanılarak bu cihazlardan aygıt adı, seri numarası, açıklama, konum ve hatta üretici yazılımı sürümü gibi bilgiler toplamak mümkündür.

Aşağıdaki Nmap komutu BACnet protokolünü kullanan cihazlar için örneklendirilmiştir.

```
$ nmap -Pn -sU -p47808 --script bacnet-info <hedef>
```

Tarama sonucu çıktısı ise aşağıdaki formatta gözükmektedir.

```
PORT     STATE SERVICE
47808/udp open  bacnet
| bacnet-info:
|   Vendor ID: CarelS.p.A. (77)
|   Vendor Name: CarelS.p.A.
|   Object-identifier: 77000
|   Firmware: A1.4.9 - B1.2.4
|   Application Software: 2.15.2
|   Object Name: pCOWeb77000
|   Description: CarelBACnet Gateway
|_  Location: Unknown
```

Nasıl Çalışır?

BACnet cihazların 47808 portunu kullandığı bilinmektedir. bacnet-info scripti kullanılarak ilgili cihazla alakalı üretici kimlik bilgileri(vendor ID), üretici ismi, firmware bilgisi ve lokasyon bilgisi gibi bilgiler elde edilebilmektedir. BACnet protokolü UDP bazlı bir protokol olduğu için "-sU" parametresi kullanılarak UDP tarama yapılmış ve aynı zamanda gereksiz trafik oluşturmamak için sunucu keşif özelliği kullanılmamıştır.

Not: İlgili cihazlar protokolün eski bir sürümünü kullanıyor yada protokolle uyumlu değilse, script çalıştırıldığı zaman hata mesajı dönecektir. Ancak bu hatanın dönmesinin sonucu olarak, karşıdaki cihazın bir BACnet cihazı olduğuna anlaşılabilmektedir.

6-) EtherNET/IP Cihazlar İçin Bilgi Toplama

EtherNET/IP; EtherNetIP verinin, TCP veya UDP paketlerinde organize edilebilmesini, kullanılabilmesini sağlayan ve aktarım katmanı olarak Ethernet'i ve uygulamalar için gerekli servisleri ve profilleri sağlamak için CIP'yi kullanan yaygın bir endüstriyel protokoldür. Çoğu satıcı tarafından üretilen EtherNET/IP cihazları 44818 portu üzerinden çalışmaktadır. NSE kütüphanesinde bulunan scriptler kullanılarak bu cihazlardan aygıt adı, seri numarası, açıklama, konum ve hatta üretici yazılımı sürümü gibi bilgiler toplamak mümkündür.

Aşağıdaki Nmap komutu EtherNET/IP protokolünü kullanan cihazlar için örneklendirilmiştir.

```
$ nmap -Pn -sU -p44818 --script enip-info <hedef>
```

Tarama sonucu çıktısı ise aşağıdaki formatta gözükmektedir.

```
PORT     STATE SERVICE
44818/udp open  EtherNet-IP-2
| enip-info:
|   Vendor: Rockwell Automation/Allen-Bradley (1)
|   Product Name: PanelViewPlus_6 1500
|   Serial Number: 0x00123456
|   Device Type: Human-Machine Interface (24)
|   Product Code: 51
|   Revision: 3.1
|_  Device IP: 10.19.130.20
```

Nasıl Çalışır?

EtherNET/IP cihazların 44818 portunu kullandığı bilinmektedir. enip-info scripti kullanılarak ilgili cihazla alakalı üretici bilgisi, seri numarası, cihaz tipi, üretim kodu ve versiyon bilgisi gibi bilgiler elde edilebilmektedir. EtherNET protokolü UDP bazlı bir protokol olduğu için "-sU" tekniği kullanılarak UDP tarama yapılmış ve aynı zamanda ilgili cihazın bulunduğu ağda gerekiz trafik oluşturmamak için sunucu keşif özelliği kullanılmamıştır.

7-) Niagara Fox Cihazlar İçin Bilgi Toplama

Niagara Fox -yada doğrudan Fox- protokolü endüstriyel bir protokol TCP temellidir. Kimlik doğrulama(authentication) aşamasında Lightweight Directory Access Protocol (LDAP) yapısını desteklediği için endüstriyel alanda sıklıkla tercih edilmektedir.

Aşağıdaki Nmap komutu Niagara Fox protokolünü kullanan cihazlar için örneklendirilmiştir.

```
$ nmap -Pn -sT -p1911,4911 --script fox-info <hedef>
```

Tarama sonucu çıktısı ise aşağıdaki formatta gözükmektedir.

```
PORT     STATE SERVICE
1911/tcp open  niagara-fox
| fox-info:
|   fox.version: 1.0.1
|   hostName: 192.168.1.128
|   hostAddress: 192.168.1.128
|   app.name: Station
|   app.version: 3.7.106.1
|   vm.name: Java HotSpot(TM) Client VM
|   vm.version: 1.5.0_34-b28
|   os.name: Windows XP
|   timeZone: America/Mexico_City
|   hostId: QAQ-APX1-0000-420A-AB21
|   vmUuid: 32d6faaa-1111-xxxx-0000-000000001a12
|_  brandId: Webs
```

Nasıl Çalışır?

Niagara Fox cihazlarının varsayılan olarak 1911 ya da 4911 portunu kullandığı bilinmektedir. fox-info scripti kullanılarak ilgili cihazla alakalı versiyon bilgisi, sunucu ismi, uygulama ismi, işletim sistemi, time zone, lokal IP adres ve yazılım versiyon bilgisi gibi bilgiler elde edilebilmektedir. Yukarıdaki örnek için; "-sT" tekniği kullanılarak TCP bağlantı kurularak tarama yapılmış ve aynı zamanda ilgili cihazın bulunduğu ağda gereksiz trafik oluşturmamak için sunucu keşif özelliği kullanılmamıştır. fox-info scripti ile "-O" komutu kullanmadan işletimi sistemi sürümü elde edilebildiği için ayrıca tercih edilmektedir.

8-) ProConOS Cihazlar İçin Bilgi Toplama

ProConOS, TCP temelli bir protokol olup gömülü veya PC tabanlı kontrol uygulamaları için tasarlanmış yüksek performanslı bir PLC çalışma zamanı motorudur(runtime engine). ProConOS, sistem bilgisi edinmek için kimlik doğrulaması olmadan sorgu yapmaya izin veren bir yapıya sahiptir.

Aşağıdaki Nmap komutu ProConOS protokolünü kullanan cihazlar için örneklendirilmiştir.

```
$ nmap -Pn -sT -p20547 --script proconos-info <hedef>
```

Tarama sonucu çıktısı ise aşağıdaki formatta gözükmektedir.

```
PORT     STATE SERVICE
20547/tcp open  ProConOS
| proconos-info:
|   LadderLogicRuntime: ProConOS V4.1.0230 Feb  4 2018
|   PLC Type: Bristol: CWM V05:40:00 02/04
|   Project Name: Test
|   Boot Project:
|_  Project Source Code: Test_2
```

Nasıl Çalışır?

ProConOS cihazlarının varsayılan olarak 20547 portunu kullandığı bilinmektedir. proconos-info scripti kullanılarak ilgili cihazla alakalı PLC tipi, proje adı, proje kaynak kodu adı ve ladder logic runtime bilgisi gibi bilgiler elde edilebilmektedir. Yukarıdaki örnek için; "-sT" tekniği kullanılarak TCP bağlantı kurularak tarama yapılmış ve aynı zamanda ilgili cihazın bulunduğu ağda gereksiz trafik oluşturmamak için sunucu keşif özelliği kullanılmamıştır.

9-) Omron PLC' ler için Bilgi Toplama

Omron PLC'ler ağdaki endüstriyel cihazlarla haberleşmek ve kontrol işlemleri için UDP veya TCP üzerinden iletişim kuran FINS protokolünü kullanmaktadır. NSE' de bulunan omron-info scripti kullanılarak bu PLC' ler hakkında bilgi elde etmek mümkündür.

Aşağıdaki Nmap komutu UDP protokolü kullanan Omron PLC'ler için örneklendirilmiştir.

```
$ nmap -Pn -sU -p9600 --script omron-info <hedef>
```

UDP protokolü kullanan Omron PLC'ler için tarama sonucu çıktısı aşağıdaki formatta gözükmektedir.

```
9600/udp open  OMRON FINS
| omron-info:
|   Controller Model: CJ2M-CPU32        02.01
|   Controller Version: 02.01
|   For System Use:
|   Program Area Size: 20
|   IOM size: 23
|   No. DM Words: 32768
|   Timer/Counter: 8
|   Expansion DM Size: 1
|   No. of steps/transitions: 0
|   Kind of Memory Card: 0
|_  Memory Card Size: 0
```

XML formatında tarama çıktısı ise aşağıdaki formatta gözükmektedir.

```
<elem key="Controller Model">CS1G_CPU44H        03.00</elem>
<elem key="Controller Version">03.00</elem>
<elem key="For System Use"></elem>
<elem key="Program Area Size">20</elem>
<elem key="IOM size">23</elem>
<elem key="No. DM Words">32768</elem>
<elem key="Timer/Counter">8</elem>
<elem key="Expansion DM Size">1</elem>
<elem key="No. of steps/transitions">0</elem>
<elem key="Kind of Memory Card">0</elem>
<elem key="Memory Card Size">0</elem>
```

TCP protokolü kullanan Omron PLC'ler için tarama sonucu çıktısı aşağıdaki formatta gözükmektedir.

```
9600/tcp open  OMRON FINS
| omrontcp-info:
|   Controller Model: CJ2M-CPU32        02.01
|   Controller Version: 02.01
|   For System Use:
|   Program Area Size: 20
|   IOM size: 23
|   No. DM Words: 32768
|   Timer/Counter: 8
|   Expansion DM Size: 1
|   No. of steps/transitions: 0
|   Kind of Memory Card: 0
|_  Memory Card Size: 0
```

Nasıl Çalışır?

Omron PLC' lerin 9600 portunu kullandığı bilinmektedir. omron-info scripti kullanılarak FINS protokolü üzerinden ilgili kontrolcüye "data oku" komutu gönderilip ağdaki Omron PLC cihazlarını algılamaktadır.

omron-info scripti kullanılarak ilgili cihazla alakalı kontrolcü model/versiyon, counter/timer, bellek kart boyut bilgisi ve sistem bilgileri gibi bilgiler elde edilebilmektedir.

10-) PCWorx Cihazlar İçin Bilgi Toplama

PCWorx protokolü seri haberleşme teknolojisini kullanan endüstriyel bir protokoldür. Genellikle kontrol mekanizması sağlayan cihazların(PLC, RTU, bazı gömülü sistemler) kullandığı bir protokol olup, çeşitli endüstriyel protokolleri(Profinet, Modbus, EtherNET/IP vs) desteklemektedir.

Aşağıdaki Nmap komutu PCWorx protokolü kullanan endüstriyel cihazlar için örneklendirilmiştir.

```
$ nmap -Pn -sT -p1962 --script pcworx-info <hedef>
```

Tarama sonucu çıktısı ise aşağıdaki formatta gözükmektedir.

```
PORT    STATE SERVICE
1962/tcp open  pcworx
| pcworx-info:
|   PLC Type: ILC 330 ETH
|   Model Number: 2737193
|   Firmware Version: 3.95T
|   Firmware Date: Mar  2 2012
|_  Firmware Time: 09:39:02
```

Nasıl Çalışır?

PCWorx protokolünü kullanan cihazların 1962 portunu kullandığı bilinmektedir. pcworx-info scripti kullanlarak ilgili cihaz algılanır, tür, model numarası ve firmware bilgisi gibi bilgiler elde edilebilmektedir. Yukarıdaki örnek için; "-sT" tekniği kullanılarak TCP bağlantı kurularak tarama yapılmış ve aynı zamanda ilgili cihazın bulunduğu ağda gereksiz trafik oluşturmamak için sunucu keşif özelliği kullanılmamıştır.

11-) DNP3 Cihazlar İçin Bilgi Toplama

Distributed Network Protocol(DNP3) 3 protokolü TCP temelli bir protokol olup başta Remote Terminal Unit(RTU)'lar olmak üzere HMI, Historian, SCADA gibi sistemlerle ve birçok OPC istemci(client) uygulaması arasında güvenilir bir bağlantı kurmaya yarayan bir protokoldür. Başlıca kullanım alanları elektrik ve su arıtma gibi endüstriyel tesislerdir.

Aşağıdaki Nmap komutu DNP3 protokolü kullanan endüstriyel cihazlar için örneklendirilmiştir.

```
$ nmap -sT -Pn --script dnp3-enumerate.nse -p20000 <hedef>
```

Tarama sonucu çıktısı ise aşağıdaki formatta gözükmektedir.

```
PORT     STATE SERVICE REASON
20000/tcp open  dnp3    syn-ack
| dnp3-enumerate:
|   Source address: 20
|   Destination address: 0
|_  Control code: 68
```

Nasıl Çalışır?

DNP3 protokolünü kullanan cihazların 2000 portunu kullandığı bilinmektedir. dnmp3-enumerate.nse scripti kullanlarak ilgili cihaz algılanır, kaynak ve hedef adres bilgisi ve cihaz üzerinde çalışan kontrol kodu bilgisi gibi bilgiler elde edilebilmektedir. Yukarıdaki örnek için; "-sT" tekniği kullanılarak TCP bağlantı kurularak tarama yapılmış ve aynı zamanda ilgili cihazın bulunduğu ağda gereksiz trafik oluşturmamak için sunucu keşif özelliği kullanılmamıştır.

12-) Melsec-Q Cihazlar İçin Bilgi Toplama

Melsec-Q protolü Mitsubishi tarafından geliştirilmiş olup sadece Mitsubishi Q Serisi PLC' ler tarafından kullanılan bir protokoldür. Bu PLC'ler genelde yüksek hız ve yüksek veri işleme(data processing) gerektiren üretim santrallerinde kullanılmaktadır.

Aşağıdaki Nmap komutu Melsecq protokolü kullanan endüstriyel cihazlar için örneklendirilmiştir.

```
$ nmap -script melsecq-discover-udp.nse -sU -Pn -p5006 <hedef>
```

Tarama sonucu çıktıları ise aşağıdaki formatta gözükmektedir.

```
PORT     STATE SERVICE            REASON
5006/udp open  Mitsubishi/Melsoft udp syn-ack
| melsecq-discover:
|_ CPUINFO: Q03UDECPU
```

TCP bağlantısı kuran PLC modelleri için;

```
PORT     STATE SERVICE            REASON
5007/tcp open  MelsoftTCP syn-ack
| melsecq-discover:
|_ CPUINFO: Q03UDECPU
```

Nasıl Çalışır?

Melseq protokolü hem TCP hem UDP temelli çalışabilen bir protokol olup bu protokolü kullanan cihazların varsayılan olarak 5006 portunu kullandığı bilinmektedir. melsecq-discover-udp.nse scripti kullanılarak MELSEC-Q Serisi PLC'ler üzerindeki işlemci bilgisi elde edilebilmektedir. Yukarıdaki örnekler için; TCP bağlantısı kuran PLC modelleri için "-sT" tekniği, UDP bağlantısı kuran PLC modelleri için ise "-sU" tarama tekniği kullanılmıştır. Ek olarak cihazın bulunduğu ağda gereksiz trafik oluşturmamak için sunucu keşif özelliği kullanılmamıştır.

13-) ATG İçin Bilgi Toplama

ATG ürünleri temel işlevi yakıt seviyelerini izlemektir. Ek olarak hacim ve sıcaklık, su seviyeleri gibi değişkenleri izler ve gerektiği durumlarda ilgili tesislerle iletişime geçebilen cihazlardır. Genellikle doğrudan bir bilgisayar ile iletişim halinde yapılandırılırlar.

Aşağıdaki Nmap komutu ATG konsollar için örneklendirilmiştir.

```
$ nmap --script atg-info -p 10001 <hedef>
```

Tarama sonucu çıktıları ise aşağıdaki formatta gözükmektedir.

```
10001/tcp open   Guardian AST reset
| atg-info:
| I20100
| SEP 19, 2015  5:33 PM
|
|    Fuel Company
|    12 Fake St
|    Anytown, USA 12345
|
|
| IN-TANK INVENTORY
|
| TANK PRODUCT          VOLUME TC VOLUME   ULLAGE   HEIGHT    WATER     TEMP
|   1  UNLEADED          5135       0    6647   42.71    0.00   72.01
|   2  UNLEADED          5135       0    6647   42.70    0.00   71.55
|   3  PREMIUM UNLEADED    5135       0    5350   19.27    0.00   72.52
|_
```

Nasıl Çalışır?

ATG cihazları/konsolları bağlandıkları ve iletişime geçtiği cihazlar ile TCP protokolü kullanarak haberleşmektedir. Bu cihazların 100001 portunu kullandığı bilinmektedir. atg-info scripti kullanılarak ATG cihazlarında kayıt altına alınan hacim, sıcaklık, seviye gibi bilgiler elde edilebilmektedir.

14-) CSPV4 Paketlerini Kullanarak Bilgi Toplama

2222/TCP portu CIP, CSPV4 paketlerinin gönderimi sırasında ve AB PLC5'ler tarafından kullanılmaktadır. CSPV4 paketleri -AB/Ethernet gibi- RSLinux sistemler ile PLC'ler(genellikle Rockwell Automation ürünü olan Allen Bradley PLC'ler) arasında haberleşmeyi sağlayan paketlerdir.

Aşağıdaki Nmap komutu CSPV4 paketlerinin simüle edilmesini sağlamaktadır.

```
$ nmap --script cspv4-info -p 2222 <hedef>
```

Tarama sonucu çıktıları ise aşağıdaki formatta gözükmektedir.

```
2222/tcp open  CSPV4
| cspv4-info:
|_  Session ID: 657
```

Nasıl Çalışır?

cspv4-info scripti kullanılarak CSPV4 paketleri hedef sisteme gönderilerek gerçek bir haberleşme simüle edilmektedir. CSPV4 paketleri gönderildikten sonra hedef tarafından dönen cevaplar anlamlandırılarak sistemin oturum kimlik doğrulama (session ID) bilgisi elde edilebilmektedir.

15-) Modicon Cihazlar İçin Bilgi Toplama

Modicon; Schneider Electric tarafından geliştirilmiş, Modbus protokolünü destekleyen bir PLC ürünüdür. Giriş/Çıkış (I/O) sayısı diğer PLC'lere göre nispeten fazla olduğu, geniş ölçekli projelerde daha çok tercih edilen bir üründür.

Aşağıdaki Nmap komutu Modicon için örneklendirilmiştir.

```
$ nmap --script modicon-info -p 502 <hedef>
```

Tarama sonucu çıktıları ise aşağıdaki formatta gözükmektedir.

```
502/tcp open  Modbus
| modicon-info:
|   Vendor Name: Schneider Electric
|   Network Module: BMX NOE 0100
|   CPU Module: BMX P34 2000
|   Firmware: V2.60
|   Memory Card: BMXRMS008MP
|   Project Information: Project -  V4.0
|   Project File Name: Project.STU
|   Project Revision: 0.0.9
|_  Project Last Modified: 7/11/2013 5:55:33
```

XML formatında tarama çıktısı ise aşağıdaki formatta gözükmektedir.

```
<elem key="Vendor Name">Schneider Electric</elem>
<elem key="Network Module">BMX NOE 0100</elem>
<elem key="CPU Module">BMX P34 2000</elem>
<elem key="Firmware">V2.60</elem>
<elem key="Memory Card">BMXRMS008MP</elem>
<elem key="Project Information">Project -  V4.0</elem>
<elem key="Project File Name">Project.STU</elem>
<elem key="Project Revision">0.0.9</elem>
<elem key="Project Last Modified">7/11/2013 5:55:33</elem>
```

Nasıl Çalışır?

modicon-info scripti kullanılarak hedef PLC ile Modbus protokolü aracılıyla bir haberleşme başlatılmaktadır. PLC ye yapılabilecek sorgular bir mühendislik yazılımı tarafından önceden belirlenmiş olup, modbus protokolü kullanılarak toplanan bilgiler fonksiyon kodlarına bağlı olmak üzere ikiye ayrılır; 43 numaralı kod ve 90 numaralı kod. 43 numaralı fonksiyon kodu üretici ismi, ağ modülü ve firmware versiyonu gibi bilgiler içerirken, 90 numaralı fonksiyon kodu ise bize PLC üzerinde bulunan işlemci modülü, bellek kart modeli ve PLC üzerine yüklenen proje hakkında bilgiler vermektedir.

16-) Siemens WinCC HMI Yazlımı İçin Bilgi Toplama

WinCC uygulaması, HMI'lar için geliştirilmiş, otomatik süreçleri izlemeye olanak tanıyan, ve ölçeklenebilir(scalable) bir fiziksel işlem görselleştirme programı olup sadece Windows platformlarda çalışmaktadır.

Aşağıdaki Nmap komutu WinCC HMI yazılımı için örneklendirilmiştir.

```
$ nmap -sU --script Siemens-WINCC.nse -p137 <hedef>
```

Tarama sonucu çıktıları ise aşağıdaki formatta gözükmektedir.

```
Host script results:
| Siemens-WINCC:
|_  Detected Siemens WINCC_SRV
```

Nasıl Çalışır?

WinCC yazılımı 137 portunu kullanan bir uygulama olup HMI sistemlerle UDP protokolü üzerinden haberleşmektedir. Siemens-WINCC.nse scripti kullanılarak ilgili hedefin bir WinCC sunucu olup olmadığı tespiti yapılıp, eğer hedef WinCC sunucu ise hostname bilgisi tespit edilebilmektedir.

17-) Scalance S Modülleri İçin Bilgi Toplama

Siemens tarafından geliştirilen Scalance modülleri farklı amaçlara hizmet vermektedir; bir kısım Scalance ürünleri endüstriyel firewall olarak(SC632-2C ve SCALANCE SC636-2C gibi) kullanılırken, kimi modülleri ise VPN aracı olarak(SCALANCE S615 gibi) kullanılmaktadır.

Aşağıdaki Nmap komutu Scalance S modülleri için örneklendirilmiştir.

```
$ nmap -sU --script ./Siemens-SCALANCE-module.nse -p161
```

Tarama sonucu çıktıları ise aşağıdaki formatta gözükmektedir.

```
@output
| Siemens-Scalance-module:
|_  SCALANCE W788-1PRO
```

Nasıl Çalışır?

Scalance S modülleri hedef cihazlar ile UDP protokolü kullanarak haberleşmeyi sağlar ve varsayılan olarak 161 portunu kullanmaktadırlar. Siemens-SCALANCE-module.nse scripti kullanılarak 161 portundan haberleşen Scalance S modülünün model bilgisi elde edilebilmektedir. Hedef cihazdan dönen cevaba göre cihaz tipi anlaşılabilmektedir. Eğer dönen string değeri;

W ise -> Wireless device
X ise -> Network switch
S ise -> firewall

olduğu anlaşılmaktadır.

18-) MMS Cihazlar İçin Bilgi Toplama

Manufacturing Message Specification(MMS) protokolü endüstriyel bir protokol olup, ağ cihazları yada bilgisayar uygulamaları arasındaki gerçek zamanlı olarak işlemiş data transferleri için kullanılmaktadır.

Aşağıdaki Nmap komutu MMS protokolünü kullanan cihazlar için örneklendirilmiştir.

```
$ nmap -d --script mms-identify.nse  --script-args='mms-identify.timeout=500' -p102 <hedef>
```

Tarama sonucu çıktıları ise aşağıdaki formatta gözükmektedir.

```
PORT    STATE SERVICE
102/tcp open  iso-tsap?
| mms-identify:
|   Raw answer: 030000>02f08001000100a10/020103a0*a1(020101a2#800flibiec61850.com810blibiec6185082030.5
|   Vendor name: libiec61850.com
|   Model name: libiec61850
|_  Revision: 0.5
```

Nasıl Çalışır?

MMS protokolünün 102 portunu kullandığı bilinmektedir. mms-identify.nse scripti kullanılarak MMS protokolü kullanan hedef cihaza doğrulama istekleri gönderilmektedir. Bu istekler sonucunda üretici ismi, model numarası ve sürüm bilgisi gibi bilgiler elde edilebilmektedir.

19-) IEC 60870-5 Standardını Kullanan Cihazlar İçin Bilgi Toplama

IEC 60870-5 elektrik mühendisliği ve güç sistemi otomasyonu uygulamalarında SCADA sistemleri için kullanılan sistemleri tanımlayan IEC 60870 standartlarından biridir. IEC 60870-5 standardı, iki sistem arasında temel kontrol mesajlarını göndermek için kullanılmaktadır.

Aşağıdaki Nmap komutu IEC 60870-5 standardını kullanan cihazlar için örneklendirilmiştir.

```
$ nmap -Pn -n -d --script iec-identify.nse  --script-args='iec-identify.timeout=500' -p2404 <hedef>
```

Tarama sonucu çıktıları ise aşağıdaki formatta gözükmektedir.

```
PORT     STATE SERVICE        REASON
2404/tcp open  IEC 60870-5-104 syn-ack
| iec-identify:
|   testfr sent / recv: 680443000000 / 680483000000
|   startdt sent / recv: 680407000000 / 68040b000000
|   c_ic_na_1 sent / recv: 680e00000000640106000ffff00000000 / 680e00000200640147000ffff00000014
|_  asdu address: 65535
```

Nasıl Çalışır?

Sistem haberleşmesi için IEC 60870-5 standardını kullanan cihazlar TCP temelli haberleşme gerçekleştirir ve varsayılan olarak 2404 portunu kullanmaktadır. iec-identify.nse scripti kullanılarak hedef cihaza çeşitli sorgular yapılır; bu sorgular sonucunda cihaz hakkında bilgiler elde edilebilmektedir.

20-) MicroLogix PLC'ler için Bilgi Toplama

MicroLogix PLC'ler Rockwell firması tarafından üretilen ve Allen-Bradley ailesine menzup endüstriyel ürünlerdir. İlgili cihazlar EtherNET/IP, DH-485, Modbus, DNP3 ve ASCII gibi çeşitli protokollerini desteklemektedir.

Aşağıdaki Nmap komutu MicroLogix PLC'ler için örneklendirilmiştir.

```
$ nmap --script=./micrologix1400.nse --script-args='dox=1' -PN -sU -p161 <hedef> -v
```

Tarama sonucu çıktıları ise aşağıdaki formatta gözükmektedir.

```
PORT    STATE SERVICE
161/udp open  snmp
| micrologix1400: CONFIRM DEVICE AS ALLEN-BRADLEY/ROCKWELL MICROLOGIX
| ** PHASE 1: SNMP verification
| ....Step 1: MicroLogix device info : CONFIRMED
| ............Version S/W          : A/5.00
| ....Step 2: SNMP device detailed information
| ............Manufacturer name     : Allen-Bradley
| ............Model number         : 1766-L32AWAA
| ............Type/model type      : MicroLogix 1400
| ............Series type          : A
| ............Revision number      : 5.0
| ** PHASE 2: Documentation
| ....Step 1: Documentation exist?  : YES
| ............ninja.infracritical.com/dox/1766-in001_-en-p.pdf
```

```
|_.....ninja.infracritical.com/dox/1766-um002_-en-p.pdf
```

Nasıl Çalışır?

Micrologix PLC'ler haberleşmek için UDP protokolünü kullanmakla beraber genellikle 161 portunu kullanırlar. micrologix1400.nse scripti iki fazdan oluşmaktadır; ilk fazda hedef cihaza SNMP istekleri yapılarak doğrulama(verification) yapılmaktadır. Bu doğrulama işlemi sonucunda versiyon bilgisi, üretici ismi, model/seri numarası bilgisi gibi bilgiler elde edilebilmektedir. İkinci fazda ise hedef PLC üzerinde -varsa- döküman ve proje bilgileri elde edilmektedir.

21-) Siemens Communications Processor(CP) İçin Bilgi Toplama

CP'ler farklı haberleşme sistemleri ve noktadan noktaya(point-to-point) haberleşme kurmak için Siemens S7-300 PLC'lerde kullanılan işlemcilerdir. Uygulamaya bağlı olmakla beraber PROFIBUS gibi farklı bus sistemlerini de desteklemektedir.

Aşağıdaki Nmap komutu Siemens CP'ler için örneklendirilmiştir.

```
$ nmap --script ./Siemens-CommunicationsProcessors.nse -p 80
```

Tarama sonucu çıktıları ise aşağıdaki formatta gözükmektedir.

```
80/tcp  open   http   syn-ack
|_Siemens-CommunicationsProcessor: CP 343-1 CX10
```

Nasıl Çalışır?

Siemens CP'ler 80 portunu kullanarak http protokolü üzerinden haberleşmektedir. Siemens-CommunicationsProcessors.nse scripti kullanılarak 80 portu üzerinde çalışan web uygulamanın çeşitli dizinlerine istekler yapılarak çeşitli bilgiler açığa çıkarılabilir ve işlemci model bilgisi elde edilebilmektedir.

22-) CodeSys v2 ile Programlanmış PLC'ler için Bilgi Toplama

CodeSys "Controller Development System" in kısaltması olup açık kaynak kodlu, endüstriyel bir yazılımdır. Bu yazılımın ana hedefi; PLC'ler için donanımdan bağımsız yazılım mimarisi sunmasıdır. EKS' lerde bazı özel durumlarda farklı PLC yapıları ile çalışmak ve bunları bütünüyle yönetebilmek gerekebilmektedir. Herhangi bir marka PLC için yazılan PLC kodu, ufak donanım değişiklikleri ile başka bir marka PLC'ye uyarlamak CodeSys programı ile mümkündür.

Aşağıdaki Nmap komutu CodeSys v2 ile Programlanmış PLC'ler için örneklendirilmiştir.

```
$ nmap -p 1200,2455 --script codesys-v2-discover <hedef>
```

Tarama sonucu çıktıları ise aşağıdaki formatta gözükmektedir.

```
Host is up (0.18s latency).
PORT     STATE SERVICE
1200/tcp open  scol
|_codesys:
\xBB\xBB\xCE\x00\x00\x00C\x00\x01\x00\x00\x00\x00\x00\x00\x00\xB0\x0C\x00\x00\x00\x00\x02\x00~\x13\x00\x00\x88\x13\x00\x00\xF4\x01\x00\x00\
x00\x04\x00\x00\xFA\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\xC5\x06\x00\x00\x01\x00\x01\x00Windows\x00\x00\x00\x00\x00
\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00unknown
CE version [runtime por\x003S-Smart Software
Solutions\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x01\x00\x00\x00\x00\x00\xFF\xFF\x00\x00\xC8\x00\x00\x00\x00\x00\x00\x00\x03\x0
0\x00\x01\x00\x10\x00\x00\x00\x10\x00\x00\x00\x10\x00\x00\x00\x00`\x00\x00\x00@\x00\x01
```

Yukarıdaki NSE script çıktısı bize işletim sistemi bilgisi ve 3S-Smart Sofftware Solutions "banner grap" bilgisi vermektedir.

Nasıl Çalışır?

codesys-v2-discover scripti, PLC' lere giden CoDeSys isteklerini herhangi bir açık bağlantı noktasına göndermeye çalışmaktadır. CodeSys yazılımı hedef cihaz ile haberleşmek/veri akışını sağlamak için TCP

protokolünü kullanmaktadır. Çoğu kontrolcüler tarafından 1200 veya 2455 portları standart olarak kullanılırken, bazı denetleyiciler 1201, 1217 ve diğer bağlantı noktaları gibi alternatif portlar kullanabilmektedir.

23-) Siemens HMI'lar için Bilgi Toplama

HMI miniweb, Siemens SIMATIC HMI'lar için özelleştirilmiş bir yazılımdır. Bu yazılım HMI operatörlerine yada HMI'dan sorumlu kişilere uzak bağlantı, kontrol fonksiyonları, sisteme yüklenen proje dosyaları görme ve yeni bir proje dosyası yükleme gibi çeşitli fonksiyonların gerçekleştirilmesi ve yönetilebilmesini sağlamaktadır. İlgili yazılım Java tabanlı olup http protokolü aracılığla tarayıcı (Siemens tarafından Internet Explorer önerilmektedir) üzerinden erişilebilmektedir.

Aşağıdaki Nmap komutu Siemens HMI miniweb yazılımı için örneklendirilmiştir.

```
$ nmap -p80 --script Siemens-HMI-miniweb.nse <hedef>
```

Tarama sonucu çıktıları ise aşağıdaki formatta gözükmektedir.

```
80/tcp  open   http   syn-ack
|_SIEMENS-HMI-miniweb: Not implemented verify_version
```

Nasıl Çalışır?

İlgili yazılımın Siemens HMI'lar üzerinde varsayılan olarak 80 portunu kullandığı bilinmektedir. Siemens-HMI-miniweb.nse scripti kullanılarak HTTP protokolü üzerinden sisteme çeşitli istekler yapılmaktadır. Bu isteklerin sonucunda dönen cevaplar filtrelenip, anlamlandırılarak cihaz tipi, bootloader versiyon bilgisi, bootloader sürüm bilgisi, cihaz ismi gibi bilgiler elde edilebilmektedir.

24-) Moxa Nport Cihazlar İçin Bilgi Toplama

"Moxa Nport" cihazlar genellikle seri cihaz ve portları ethernet protokolüne çevirmek için kullanılmaktadır. Endüstriyel ortamlarda doğrudan enstrümanlarla haberleşmek için kullanılan protokoller farklılık gösterebilmektedir. Enstrümanlardan alınan verilerin bir merkeze gönderilmesi ve oradan kontrol edilip izlenmesi EKS'ler için tercih edilen bir yaklaşımdır. Seri haberleşmeyi teknolojisini kullanan cihazları ethernet protokolüne çevirmekteki amaç; sahadan toplanan verileri bir kontrol/izleme merkezine gönderilmesi sırasında -gerek güvenli bir kanal kullanma isteği gerekse datanın işlenip anlamlandırılmasının daha kolay ve verimli olması sebebiyle- TCP/IP yada UDP protokolünü kullanmaktır. Bu sebeple EKS'lerde protokol çeviriciler sıklıkla kullanılmaktadır. Moxa Nport cihazlar endüstriyel ortamlarda sıkça kullanılan protokol çeviricilerdir.

Aşağıdaki Nmap komutu Moxa Nport protokol çeviriciler için örneklendirilmiştir.

```
$ nmap -sU --script moxa-enum -p 4800 <hedef>
```

Tarama sonucu çıktıları ise aşağıdaki formatta gözükmektedir.

```
4800/tcp open|filtered  iims    no-response
| moxa-enum:
|   Moxa Nport Devices Status: Fixed --Password setting status
| Server Name: NP5110_2439 --Target device information
```

Nasıl Çalışır?

moxa-enum.nse scripti kullanılarak hedef cihaza çeşitli istekler yapılmaktadır. Bu isteklerin sonucunda hex değerli cevaplar dönmektedir. Cevap olarak dönen her hex değeri sunucu ismi, cihaz ismi ve modeli, parola ayarları gibi bilgileri adreslemektedir.

25-) Maintenance Operation Protocol (MOP) Protokolü İçin Bilgi Toplama

Endüstriyel ortamlarda haberleşme en önemli ve kritik süreçlerden birisidir. EKS'lerde haberleşmeyi sağlayan cihazlara her zaman fiziksel erişim şansımız olmayabilir. Bu sebeple haberleşmeyi sağlayan cihazlar üzerinde olası bir arıza durumunda uzaktan teşhis ve müdahale edebilmek süreci sekteye

uğratmaması konusunda önem arz etmektedir. MOP protokolü genellikle Cisco cihazlarda uzaktan test ve problem teşhisi için kullanılır ve ayrıca sistem yazılımları, uzaktan test ve problem teşhisi, download ve upload gibi hizmetler için de kullanılmaktadır.

Aşağıdaki Nmap komutu MOP protokolünü kullanan cihazlar için örneklendirilmiştir.

```
$ nmap --script mop-discover <hedef>
```

```
$ nmap --script mop-discover --script-argets target=<hedef MAC adresi>
```

Tarama sonucu çıktıları ise aşağıdaki formatta gözükmektedir.

```
Host script results:
|_mop-discover: Maintenance Operation Protocol (MOP) is supported.
```

Nasıl Çalışır?

mop-discover.nse scripti hedef cihazın MOP protokolünün kullanıp kullanmadığını yada destekleyip desteklemediğini tespit etmektir. Bu tespit işlemi sırasında hedef cihaz yada sunucuya "DEC" diye isimlendirilen Layer 2 (data link layer) istekler gönderilmektedir. ilgili script bu isteklerin sonucunda cihazın MOP protokolünü desteklediğine/kullandığına -yada tam tersi- karar vermektedir.