Master OTW's Hacker Training Camp

Fools talk;
The Wise listen.

Search Site

Log In

Return to Home

All Posts Your Community Getting Started

OTW Sep 8, 2019 3 min read

SCADA Hacking: Finding Vulnerable SCADA Systems using Google Hacking

Welcome back, my tenderfoot hackers!

Google Hacking and Dorks

As most of you know, Google crawls the globe and stores and indexes the information it finds on nearly every web site and page. Saying this involves a lot of information is an significant understatement. Few people, though, understand that Google has a proprietary language to extract that information beyond looking for keywords.

For a full explanation of Google hacking, please read my article on Google hacking here.

This capability of searching through all the pages that Google has indexed is a great convenience, but with a little knowledge of Google's keywords, you can find more information than you ever imagined.

Developing Google Dorks for SCADA

In this article, we will use this knowledge to find SCADA systems with web interfaces. There is no single Google dork that will reveal each and every SCADA interface, instead we need to know a bit about the manufacturer and the products being used. Each company creates their own embedded systems to do things such as manage water systems, manufacturing systems, heating and cooling systems, chemical process systems, nuclear power plants, etc. They share common protocols and procedures, but in general, they are unique.

Some of the major manufacturers in this industry are;

Seimens

Rockwell Automation

Schneider Electric

General Electric

and many more.

In addition, each of these companies makes multiple products. To find these products being used in the SCADA industry with Google, we will need to develop separate Google dorks for each.

Here is a short list of some Google dorks by company and specific product.

Vendor	Product	Product Version	Google Dork(inurl:)
ABB	RTU500	RTU560	ABB RTU560
ABB	Generic	Generic	ABB Webmodule
ACKP	Generic	Generic	AKCP Embedded Web Server
Adcon Telemetry	A850 Telemetry Gateway	Generic	A850 Telemetry Gateway
Adcon Telemetry	addUPI-OPC Server	Generic	addUPI Server
Adcon Telemetry	Generic	Generic	title:adcon
Allen-Bradley	Generic	Generic	Allen-Bradley
Allen-Bradley	Generic	Generic	Series C Revision
Beck IPC	IPC@CHIP	Generic	IPC@CHIP
BroadWeb	Generic	Generic	BroadWeb
BACnet	Modicon	Generic	Quantum BACnet
Cimetrics	Eplus - B/IP to B/WS Gateway Firewall	Generic	Cimetrics Eplus Web Server
Clorius Controls	Generic	Generic	ISC SCADA Service HTTPserv:00001
Codesys	WebVisu	Generic	Webvisu
Delta Controls	enteliTOUCH	Generic	DELTA enteliTOUCH
Echelon	i.LON 600	Generic	i.LON
Electro Industries GaugeTech	Generic	Shark 200 / 200T	MicroRTU
Electro Industries GaugeTech	Generic	Generic	EIG Embedded Web Server
Elster EnergyICT	Generic	Generic	EnergyICT
Elster EnergyICT	RTU	Generic	EnergyICT RTU
Elster EnergyICT	eiPortal	Generic	eiPortal
Fujitsu	ServerView	Generic	serverview
General Electric	Cimplicity	Generic	CIMPLICITY-HttpSvr
General Electric	Cimplicity	Generic	CIMPLICITY WebView
General Electric	Proficy	Generic	ProficyPortal
Generic	Generic	Generic	"Server: VTS" -IIS -Apache -nginx 401 -500 -Boa -Sitewatch -Apple -httpd -cpsrvd -Ubicom -DCS-6620
Generic	Generic	Generic	--All--
Generic	Generic	Generic	GoAhead-Webs InitialPage.asp
Generic	Generic	Generic	Jetty 3.1.8 (Windows 2000 5.0 x86)
Generic	Generic	Generic	NET ARM Web Server/1.00
Generic	Generic	Generic	Modbus Bridge
Generic	Generic	Generic	ModbusGW
Generic	Generic	Generic	PLC
Generic	Generic	Generic	Powerlink
Generic	Generic	Generic	SCADA
Generic	Generic	Generic	SLC-5
Generic	Generic	Generic	openerp server: CherryPy
Generic	Generic	Generic	webSCADA-Modbus
HMS	EtherNet/IP / Modbus-TCP Interface	Generic	HMS AnyBus-S WebServer
Moxa	Generic	Generic	MoxaHttp
Moxa	ioLogik	Generic	ioLogik Web Server
Novatech	Generic	Generic	NovaTech HTTPD
NRG Systems	WindCube	Generic	WindWeb
Rabbit	Generic	Generic	Z-World Rabbit
Rabbit	Generic	Generic	title:phasefale Z-World Rabbit
Reliance	Reliance 4 SCADA/HMI system	Generic	Reliance 4 Control Server
Rockwell Automation	Micrologix	Generic	Micrologix
Rockwell Automation	Generic	Generic	Rockwell Automation
RTS Services	Generic	Generic	RTS SCADA Server
SAP	NetWeaver Application Server	Generic	SAP NetWeaver Application Server
Schleifenbauer	SPbus gateway	Generic	Schleifenbauer SPbus gateway
Schneider Electric	CitectSCADA	Generic	CitectSCADA
Schneider Electric	Generic	Generic	ClearSCADA
Schneider Electric	PowerLogic EGX	EGX100MG	HMI, XP277
Schneider Electric	Modicon	M340	Modicon M340
Schneider Electric	Modicon	M340	Modicon M340 CPU
Schneider Electric	Generic	Generic	Power Measurement Ltd
Schneider Electric	PowerLogic ION	ION8650	Power Measurement Ltd ION8650
Schneider Electric	PowerLogic PM	PM800	PowerLogic PM800
Schneider Electric	PowerLogic PM	PM8205D	S7-200
Schneider Electric	PowerLogic PM	PM8205D	S7-300
Schneider Electric	PowerLogic ECC	ECC21	Schneider Electric ECC21
Schneider Electric	PowerLogic EGX	EGX100MG	Schneider Electric EGX100MG
Schneider Electric	PowerLogic PM	PM8205D	Schneider Electric PM8205D
Schneider Electric	PowerLogic PM	PM8705D	Schneider Electric PM8705D
Schneider Electric	Generic	Generic	Schneider-WEB
Siemens	Simatic S7	Generic	Portal0000.htm
Siemens	Simatic S7	Generic	Portal0000
Siemens	Scalance S	Generic	Scalance S
Siemens	Scalance W	Generic	Scalance W
Siemens	Scalance X	Generic	Scalance X
Siemens	Simatic HMI	Generic	SIMATIC HMI
Siemens	Simatic NET	Generic	SIMATIC NET
Siemens	Generic	Generic	Siemens
Siemens	Simatic HMI	Generic	Simatic
Siemens	Generic	Station[illegible]7-1200_1	Portal/Portal.mwsl
Siemens	Simatic S7	Generic	Simatic S7
Siemens	Simatic HMI	Generic	Simatic -S7 HMI
Siemens	Simatic HMI	Miniweb	Miniweb Start Page
Siemens	Simatic HMI	Miniweb	Miniweb
Siemens	Simatic HMI	Generic	Welcome to the Windows CE Telnet Service on HMI_Panel
SoftPLC	Generic	Generic	SoftPLC
Somfy	Generic	Generic	title:Somfy
SpiderControl	Generic	Generic	SpiderControl
Stulz	Generic	Generic	Stulz GmbH Klimatechnik
THUS	Generic	Generic	THUS plc FTP server
Trend	IQ3xcite	Generic	server: iq3
Tridium	Generic	Generic	Niagara Web Server
Tridium	Generic	Generic	niagara_audit
Tridium	Generic	Generic	niagara_audit -login
Wago	Generic	Generic	WAGO
Wind River	Generic	Generic	VxWorks
Wind River	Generic	Generic	WindRiver-WebServer

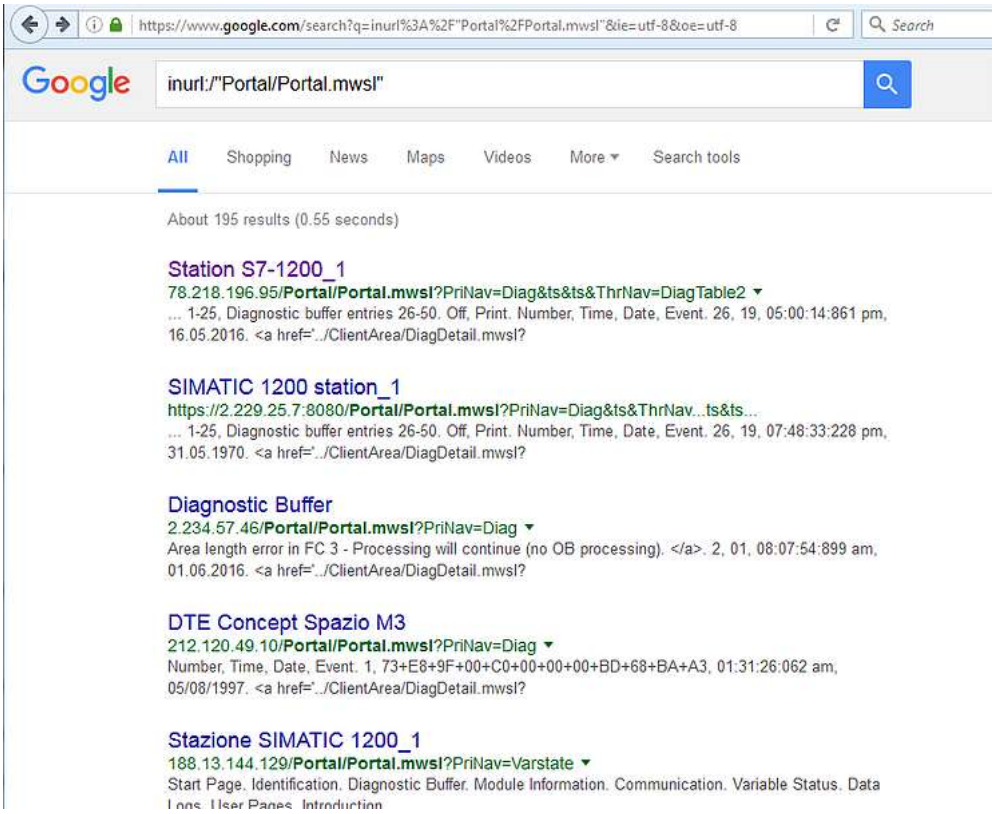
Using The Google Dorks

Now that we have a few sample Google dorks to find specific SCADA systems, let's try some out and see what we can find. Let's start with the first one on the list, the dork for the Siemens S7 series of PLC controllers.These are almost the exactly same controllers that were the target of the infamous Stuxnet attack against the Iranian uranium-enrichment facility in 2010, probably THE most sophisticated SCADA attack at the time and a milestone in cyber war fare.

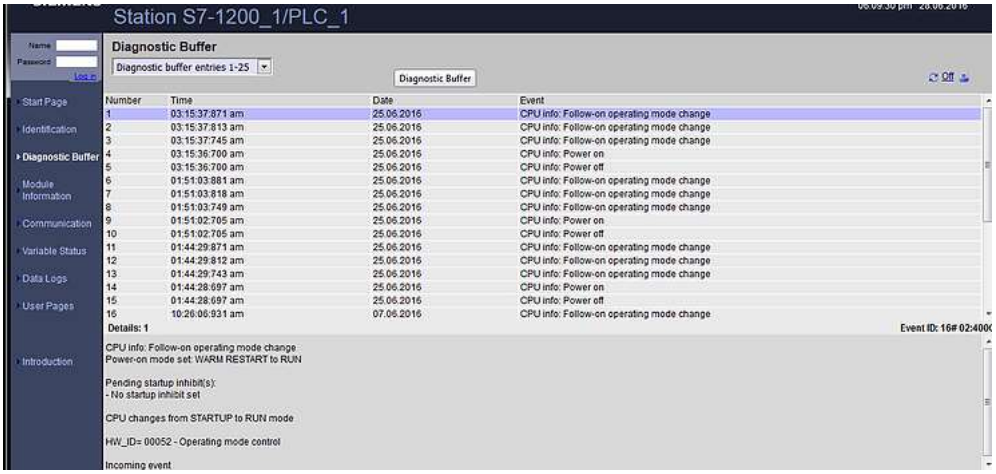
The Google dork for that controller is:

inurl:/Portal/Portal.mwsl

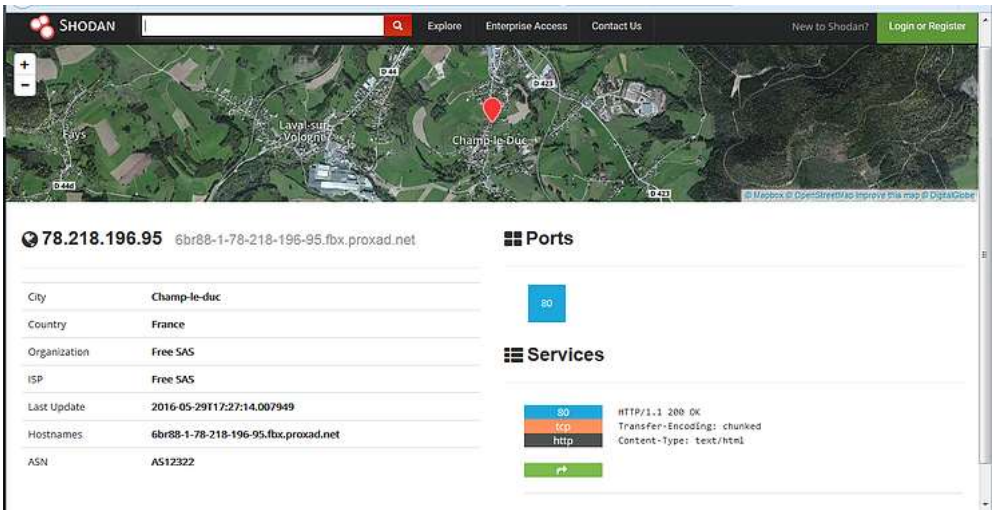
When we use it in a Google search, we get the results displayed below.



If we click on the first result above (Station S7-1200_1), it opens web portal as seen below.

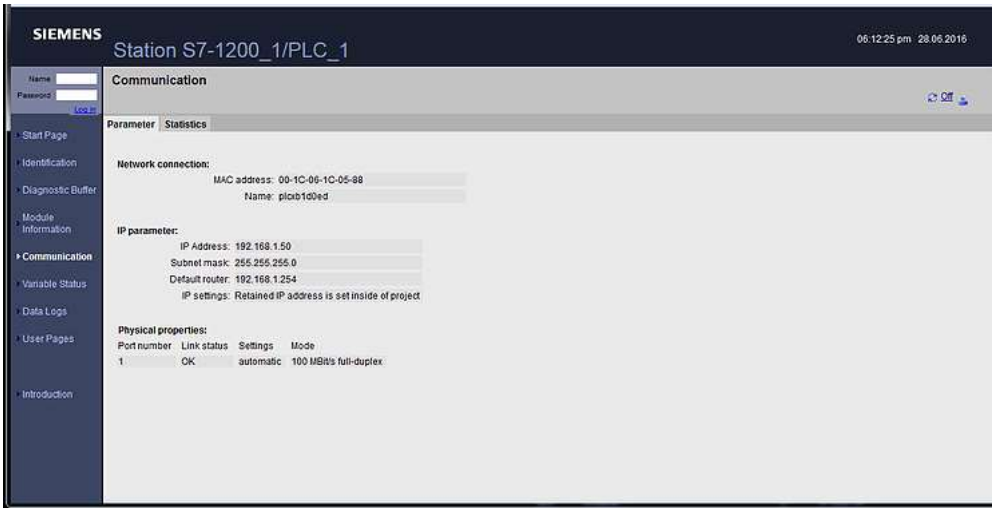


This appears to be an admin portal to this Siemens S7 PLC controller somewhere on Earth. If we put the IP address into Shodan, we can see that it is located at Champ-is-Luc in France.



When we click on the identification tab to the left, the PLC identifies itself as a Station S7-1200_1/PLC_1. It addition, it gives us its serial number and version of the firmware.

Finally, if we click on the Communications tab to the left, this portal gives us its MAC address (useful for spoofing), IP address, netmask, default router and physical properties all without logging in!



SCADA system security is still in its infancy, relying primarily on security by obscurity. These simple Google dorks though, can change those systems from obscure to easy visible to anyone on the planet. Even a hacker with rudimentary skills can now find these systems and if they have malicious intent, access these control systems and wreak havoc.

Keep coming back my tenderfoot hackers as we explore the scary world of SCADA and the most valuable skills of the 21st century--hacking!

Dark Angel

Best book for Kali Linux Beginner, Jr. Level Pen Tester

May 1, 2019

Format: Paperback

This is one of the best books for Jr. Level Penetration Tester and students who are eager to learn Information Security. To me, as professional Sr. InfoSec Person (Executive), 6. Process Management and 7. Managing User Environment Variables are very helpful to understand current processes and optimizing environments. 15. Managing the Linux Kernel and Loadable Kernel Modules are very unique chapter, which I don't find information from other books. Thanks a lot. Well done.