

使用 shodan 入侵打印机

作者: Eddie

- 原文链接: https://ld246.com/article/1544157102767
- 来源网站: 链滴
- 许可协议: 署名-相同方式共享 4.0 国际 (CC BY-SA 4.0)

1 shodan 搜索 product:"HP LaserJet"

我们这里是要搜索hp LaserJet系列的打印机设备;图示的地方我们选择台湾的设备。

👌 Shod	AN prod	luct "HP LaserJet"		۹ 🕈	Explore	Downloads	Reports	Developer Pricin
Exploits	🐁 Maps	Share Search	A Download Results	Le Create	Report			
TOTAL RESUL	.TS			78.186.3	8.28			
11 276				78.186.38.28 Turk Telekor	static.ttnet.co	om.tr	@PJL	INFO STATUS
1,270				Added on 20	18-12-07 03:4	45:02 GMT	CODE=	40608
TOP COUNTR	UES			Turkey,	Seyhan		DISPL	AY="
			***************	Details			ONLIN	E=TRUE
	ARC .	1 Contrain					@PJL	INFU ID
		18					OP TI	INFO PRODINFO
		ASP CONT					Produ	ctName = HP LaserJ
	-	Server Change					Forma	tterNumber = QJ62J
		T 🍋	2.4				Print	erNumber = Q1234A
United States		-	3 352				Produ	ctSerialNumber = 0
Korea Ropul	s		3,35Z				Servi	ceID = 172
Taiwan	one of		536					
Russian Fode	aration		492		17.11			
Brazil			477	61.252.1	47.14			
				Added on 20	18-12-07 03:4	44:58 GMT	@PJL	INFO STATUS
TOP SERVICES	S			Korea, R	epublic of		CUDE=	5V=""
Printer Job L	anguage		11,232	Detalls			ONLIN	E=TRUE
HTTP (8080)			19				@PJL	INFO ID
CUPS			12				HP La	serJet Professiona
HTTP			11				@PJL :	INFO PRODINFO
HTTP (8181)			1				Produ	ctName = HP LaserJ
							Forma	tterNumber = QA72N
OP ORGANIZ	ZATIONS						Printe	erNumber = Q1234A
Korea Teleco	m		422				Servi	ceID = 24078
Comcast Bus	siness		366				Firmw	areDateCode = 2
Spectrum			239					
Universidad I	Nacional Auton	oma de Mexico	179					
Taiwan Acade	emic Network		163	95.141.2	27.57			
				static-227-57	netbynet.ru		@PJL :	INFO STATUS
				Added on 20	18-12-07 03:4	43:42 GMT	CODE=	10023
				Russian	Federation,	Novocheboksarsk	DISPL	AY="Печатьдокуми

2 右侧我们随便选择一个服务器。貌似是一所大学。

@PJL INFO ID



	mems1.me.ncu.edu.tw View Raw Data	Ports
City	Taipei	21 80 443 515 631 9100
Country	Talwan	
Organization	Talwan Academic Network	:= Services
ISP	Talwan Academic Network (TANet) Information Center	
Last Update	2018-12-06T19:55:22.498456	21 220 FTP Server Ready 230-Hewlett-Packard FTP Print Server Version 3.0.
Hostnames	ladu.tw	ftp Directory: Description:
A5N	A518420	PORT HP LaserJet P3010 Series
		To print a file use the command put «filename» [por or 'cd' to a desired port and use put «filename»,
		230 User logged in. 214-The following commands are recognized:

	ABOR	ACCT	ALLO	APPE*	CDUP	CiD.
	LIST	MDTM*	MKD+	MODE	NUST	NOOP
	PORT	PHD	QUIT	REIN+	REST	RETR*
	STRU	SITE*	5IZE*	SYST	TYPE	USER
4	End of	comiand	list.			
90	Comman	d unreco	gnized o	r unimpl	emented.	



Virata-EmWeb Version: 6_2_1 HTTP/1.1 301 Moved Permanently Server: Vinata-Embeb/R6_2_1 Content-Type: text/html; charset=utf-8 X-Frame-Options: SAVEORIGIN

3 下拉查看我们的打印机设备,记住型号 (HP LaserJet P3010)

X-Content-Type-Options: nosniff Location: https://140.115.65.160/ Content-Type: text/html Content-Length: 91



HP LaserJet P3010 Series

@PJL INFO STATUS CODE=11204 DISPLAY="2 號紙匣已空 任何類型 A4" CODE2=10023 DISPLAY2="處理中..." ONLINE=TRUE @PJL INFO ID "HP LaserJet P3010 Series" @PJL INFO PRODINFO "2"

4 在系统中连接打印机。



G	👼 添加打印机		
	按名称或 TCP/IP 地址查	找打印机	
	 ● 根据位置或功能在目录中查找 ● 按名称选择共享打印机(S) 	之一个打印机(F)	
			浏览(R)
	示例: \\computername\ http://computername/p	printername 或 printers/printername/.printer	
	◎ 使用 TCP/IP 地址或主机名添	加打印机(1)	
			下一步(N) 取消
0	🖶 添加打印机		×
0	豪加打印机 □ </th <th>地址</th> <th></th>	地址	
0	➡ 添加打印机 键入打印机主机名或 IP 5 设备类型(T):	地址	×
0	 ➡ 添加打印机 → 録入打印机主机名或 IP : ⇒ 设备类型(T): 主机名或 IP 地址(A): 	地址 自动检测 .160 ip地址,无需端口	
0	 → 添加打印机 ◆ 添加打印机主机名或 IP 5 ◆ 資音类型(T): 主机名或 IP 地址(A): ◆ 満口名称(P): 	地址 自动检测 .160 ip地址,无需端口 给打印机一个别名	
•	 ➡ 添加打印机 键入打印机主机名或 IP 式 设备类型(T): 主机名或 IP 地址(A): 端口名称(P): ☑ 查询打印机并自动选择要使用 	地址 自动检测 .160 ip地址,无需端口 给打印机一个别名 的打印机驱动程序(Q)	
•	 → 添加打印机 健入打印机主机名或 IP : 26番类型(T): 主机名或 IP 地址(A): 端口名称(P): 図 查询打印机并自动选择要使用 	地址 自动检测 .160 ip地址,无需端口 给打印机一个别名 验打印机驱动程序(Q)	×
	 → 添加打印机 ◆ 漆加打印机主机名或 IP : ◆ 设备类型(T): 主机名或 IP 地址(A): ○ 黄洵打印机并自动选择要使用 	地址 自动检测 160 ip地址,无需端口 给打印机一个别名 3885打印机驱动程序(Q)	1
	 → 添加打印机 健入打印机主机名或 IP : 设备类型(T): 主机名或 IP 地址(A): 端口名称(P): ☑ 查询打印机并自动选择要使用 	地址 自动检测 .160 ip地址,无需端口 给打印机一个别名 3的打印机驱动程序(Q)	₹

参加打印机 参加打印机	
键入打印机主机名或	IP 地址
设备类型(T):	目动检测
主机名或 IP 地址(A):	60
端囗名称(P):	
☑ 查询打印机并自动选择	長使用的打印机驱动程序(Q)
正在与打印机联	<u>E</u>
	下一步(N) 取消
豪加打印机 家加打印机	Passenet Process Press Price
需要额外端口信息	
网络上沿右地到沿条	· · · · · · · · · · · · · · · · · · ·
1. 波雷巴打开.	MIAE.
2. 网络已连上。 3. 设备配置正确。	
4 前一页上的地址正确	
如果您认为地址不正确 索。如果您认为地址是正	请单击 "上一步" 返回到上一页,然后改正地址并在网络上执行另一次搜)确的,请选择下面的设备类型。
设备举型	
◎ 标准(S) Ger	eric Network Card
◎ 自定义(C) 1	置(E)
	下一步(N) [] [] []

出现这种情况代表打印机连接成功!

 ◆ 秋湖西市 ◆ 秋湖西市 ◆ 秋湖市市 ◆ 秋湖市市 ◆ 秋湖市市 ◆ 秋湖市
Skatubulan Apl为年市送得打印机,单击 Windows Update 以置看更多型号, 者要从安装 CD 安装驱动程序,请单击"从送盘安装"。 「「」」「」」「」」「」」「」」「」」」」」」」」 「「」」」」」」」 「「」」」」」 「「」」」」」 「「」」」」」 「」」」」 「」」」」 「」」」」 「」」」 「」」」 「」」」 「」」」」 「」」」 「」」」」 「」」」」 「」」」 「」」」 「」」」 「」」」」 「」」」」 「」」」」 「」」」」 「」」」」 「」」」 「」」」 「」」」 「」」」
SP#STIPUNIESDAREP
W列泰中选择打印机。单击 Windows Update 以查看更多型导。 者要从安装 CD 安装驱动程序,请单击"从滋盘安装"。
★型林安装 CD 安装驱动程序,请单击"从磁盘安装"。 「● 「丁印印 「申」 「丁印印 「申」 「丁印印 「日日 「日日 「「日日 「日日 「日日 「日日 「日 「日 「日
★型外装装 CD 装装和式用度, 博申击"从磁盘装装"。 「商 打印机 「申」 「申」 「」 「」 </th
「前 「町川 「町 「日 13005 PCL6 「日 14014/P4015 PCL6 14014/P4015
「申」 打印机 「uji Xerox 「申」 Generic 「申」 Gestetner 「申」 HP LaserJet P3005 PCL6 「申」 「申」 「」」 LaserJet P3011/P3015 PCL6 「」」 「申」 「」」 「」」 「」」 「」」 「」」 「」」 「」」 「」」 「」」 「」」 「」」 「」」 「」」 「」」 「」」 「」」 「」」 「」」 「」」 「」」 「」」 「」」 「」」 「」 「」」 「」 「」」 「」 「」」 「」」 「」」 「」 「」」 「」 「」 「」 「」 「」 「」 「」 「」 「」 「」 「」 「」 「」 「」 「」 「」 「」 「」 「」 「」 「」
「商 Fuji Xerox Generic Gestetner HP infotec 定 全个驱动程序已经过数字签名。 受 小型 上 支 小型 小型 一 一 少 一 、 文 小型 一 一 一 一 一 一 一 一 一 一 一 一 一
Fuji Xerox Fuji Xerox Generic Fuji Xerox Gestetner FP Laser/et P3005 PCL6 HP Laser/et P3011/P3015 PCL6 Finifotec Fuji Merce John String Kindows Update Kadagek Kindows Update
Generic 日日 日日 140 LaserJet P3001/P3015 PCL6 日日 日日 日日 140 LaserJet P3011/P3015 PCL6 日日 日日 日日 140 LaserJet P4515 PCL6 日日 日日 日日 140 LaserJet P4515 PCL6 日日 日日 日日 140 LaserJet P4515 PCL6 日日 日日 日日 140 LaserJet P3011/P3015 PCL6 , 日日 日日 140 LaserJet P3011/P3015 PCL6 , 140 LaserJet P3011/P3015 PCL6 ,
HP ・
infotec ▼ HP LaserJet P4515 PCL6
告诉我为什么驱动程序签名很重要 下一步(N) 取消 基择一个跟目标打印机相似的型号,如果没有考虑安装官方驱动。
下一步(N) 取消 选择一个跟目标打印机相似的型号,如果没有考虑安装官方驱动。 でののまた。 全のので、「「」、 を対面板,硬件和声音,设备和打印机,HP LaserJet P3011/P3015 PCL6, ・ 4, 援索 HP LaserJet P3011/P3015 PCL6,
下一步(N) 取消 基择一个跟目标打印机相似的型号,如果没有考虑安装官方驱动。 © ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●
选择一个跟目标打印机相似的型号,如果没有考虑安装官方驱动。
○ □ ↓ · · · · · · · · · · · · · · · · · ·
C □ ■ × C □ ■ × E → 控制面板 → 硬件和声音 → 设备和打印机 → HP LaserJet P3011/P3015 PCL6 → マ □ → 任 → 推要 HP LaserJet P3011/P3015 PCL6 →
◆ ● ◆ 控制面板 ◆ 硬件和声音 ◆ 设备和打印机 ◆ HP LaserJet P3011/P3015 PCL6 ◆ ◆ 4 ◆ 4 ◆ ◆ 4 ◆ ◆ ◆ ◆ ◆ ◆
HP LaserJet P3011/P3015 PCL6
HP LaserJet P3015 Series
 ■ N列中有 2 个文档 ① 打印机: 就绪
打印照片、文档和调整设置 在线订购耗材 空雪当前打印内容 目定义您的打印机 经格利 经公司
9mm 9

看到打印机了!打印一个测试页面看看?

			(an a start of	02011/0	2015 001	6 22 44	-	L	
●●● 注制面板 ● 硬件	HP LaserJet P3011	L/P3015 PCL6		HP L	aserJet i	P3011/P	3015 PCI	10 准注			LACT
	31000(F) 又信(D)	旦信(V) 	657	吊戏	天导	瑞山	一局級	颜巴官埋	安全	设备设置	天士
	XIBB	Ma		-	4	HP Las	erJet P3	011/P3015	PCL6		
				位置	L):						
				注释(C):						
打印机操作 打印服台 文林印度整设备	•										
调整打印选项(查看当前打				型号(0):	HP Lase	erJet P30	011/P3015 P	CL6		
				功前彩	e 色: 是			可用	纸张:		
				双	面: 否			A4	69090		
	•			装	丁: 否						
				速	賽: 22 p	pm					
				最	大分辨率	\$: 600 dp	pi -			-	
							<u> </u>	and the set	_	(
								自远坝(E).	•	FJEJW	版贝(1)
				L							
aserJet P3011/P3015 PCL6	j										
7 已将测试页发送到	打印机										
此测试页简要说明了打印 提供了有关打印机的技术	口机打印图形和文本的功 K信息。如果测试页未正 2006	b能,并 E常打									

<u>获取有关打印的帮助</u>

打印机(P) 文档(D) 看	琶看(V)					
文档名	状态	所有者	页数	大小	提交时间	端
	C41E1		1/1	320 KB	12:19:51 2018	/12//

关闭

打印成功了