Supernova测试仪特征库信息

Supernova测试仪可进行漏洞扫描、攻击报文重放、Web攻击靶场以及模糊测试，特征库（1.1.001473.sig）中漏洞扫描库漏洞数量120607个、攻击流量库攻击报文10925个、Web攻击靶场库攻击脚本数量11681个、模糊测试库协议数量40种

攻击流量库（10925个攻击流量）	
按种类划分	
类型	数量
其他安全漏洞	30
CGI漏洞	8
DNS协议拒绝服务漏洞攻击	179
IP分片攻击	10
SQL注入漏洞	64
Shellcode	105
后门程序	27
XSS跨站脚本攻击	36
任意代码执行漏洞	251
网络行为攻击	30
扫描攻击检测	40
缓冲区溢出漏洞	1022
蠕虫攻击	420
拒绝服务漏洞	143
逃逸攻击	63
暴力破解弱口令攻击	20
敏感信息泄露	15
任意文件下载漏洞	10
操作系统漏洞	495
MySQL应用层攻击	140
Oracle安全漏洞	123
任意文件创建漏洞	3
SMB应用层攻击	73
Web浏览器漏洞	68
HTTP应用层攻击	3584
FTP应用层攻击	275
HTTPS应用层攻击	272
IMAP应用层攻击	265
POP3应用层攻击	240
Portmap应用层攻击	697
SMTP应用层攻击	927
SSH协议安全漏洞	13
TELNET应用层攻击	32
UDP类型协议未知漏洞	120
任意命令执行漏洞	64
绕过身份认证漏洞	38
提权漏洞	17
文件上传漏洞	20
目录遍历漏洞	44
内存破坏漏洞	47
文件包含类漏洞	20
未授权访问漏洞	13
任意文件覆盖漏洞	3
虚假攻击	5
僵尸网络程序	100
勒索病毒	102
木马程序	102
Bitcoin	100
MixAttacks	265
NETBIOS攻击	154
LDAP攻击	31

漏洞扫描库（120607个漏洞）	
按严重程度划分	
严重程度	数量
高	49809
中	60090
低	10708
按CVE年份划分	
年份	数量
1999	145
2000	91
2001	256
2002	372
2003	415
2004	1259
2005	1472
2006	1429
2007	2284
2008	3358
2009	4598
2010	3694
2011	4614
2012	5031
2013	6289
2014	6951
2015	6786
2016	8377
2017	9197
2018	9738
2019	9083
2020	9096
2021	9651
2022	10135
2023	7181
2024	1012
按种类划分	
类型	数量
AIX Local Security Checks	1
Amazon Linux Local Security Checks	748
Brute force attacks	9
Buffer overflow	645
CISCO	650
CentOS Local Security Checks	3215
Citrix Xenserver Local Security Checks	30
Compliance	15
Credentials	4
Databases	1062
Debian Local Security Checks	9604
Default Accounts	302
Denial of Service	2173
F5 Local Security Checks	125
FTP	174
Fedora Local Security Checks	24625
FortiOS Local Security Checks	34
FreeBSD Local Security Checks	2009
Gain a shell remotely	109
General	7590
Gentoo Local Security Checks	2191
HP-UX Local Security Checks	15
Huawei	146
Huawei EulerOS Local Security Checks	11033
IT-Grundschutz	195
IT-Grundschutz-15	85
IT-Grundschutz-deprecated	363
JunOS Local Security Checks	136
Mac OS X Local Security Checks	385
Mageia Linux Local Security Checks	5106
Malware	57
Mandrake Local Security Checks	807
Nmap NSE	154
Nmap NSE net	177
Oracle Linux Local Security Checks	1895
Palo Alto PAN-OS Local Security Checks	40
Peer-To-Peer File Sharing	9
Policy	740
Port scanners	9
Privilege escalation	158
Product detection	2955
RPC	4
Red Hat Local Security Checks	1853
Remote file access	56
SMTP problems	52
SNMP	12
SSL and TLS	86
Service detection	253
Settings	11
Slackware Local Security Checks	1539
Solaris Local Security Checks	1
SuSE Local Security Checks	15186
Ubuntu Local Security Checks	8101
Useless services	16
VMware Local Security Checks	57
Web Servers	902
Web application abuses	9125
Windows	273
Windows : Microsoft Bulletins	3300

模糊测试库（40种协议）	
按协议类型划分	
协议类型	数量
61850_CMS	1
OPCUA	1
LLC	1
TCP	2
COTP	1
IMAP	1
HTTP	1
ARP	1
S7COMM_2L	1
DHCPv4	1
UDP协议RawL3	1
DNS	1
OSPF	1
VNC	1
MODBUS	1
HTTPS	1
LLDP	1
GTP	1
SNMP	1
IPV6	1
SSDP	1
POP3	1
IEC61850_GOOSE	1
SSH	1
DHCPv6	1
FTP	1
S7	1
TCP协议RawL3	1
BGP	1
ICMPv6	1
SMTP	1
MDNS	1
TCPv6	1
UDP	2
NTP	1
IEC61850_MMS	1
SMB	1
IPV4	1
TFTP	1
Omron-Fins	1

Web攻击靶场库（11681个攻击脚本）	
按种类划分	
类型	数量
File Upload	1926
Interesting File / Seen in logs	1868
Misconfiguration / Default File	674
Information Disclosure	870
Injection (XSS/Script/HTML)	877
Remote File Retrieval - Inside Web Root	211
Denial of Service	52
Remote File Retrieval - Server Wide	217
Command Execution / Remote Shell	317
SQL Injection	2333
Authentication Bypass	144
Software Identification	511
Remote source inclusion	2354
WebService	79
Administrative Console	214
XML Injection	12
按HTTP请求方式划分	
请求方式	数量
GET	8690
POST	2987
按场景类型划分	
类型	数量
Web攻击	6955
bWAPP靶场攻击	2440
DVWA靶场攻击	963
默认Mutillidae II靶场攻击列表	1139
SqliLabs靶场攻击列表	34
Pikachu靶场攻击列表	150