|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 姓名：崔文帅 | | 学号：2025060163 | 专业年级： 2020 | 班级： 网三 |
| 分组： | | 实验室：402 | 指导教师：郭念 | 实验日期：2023-03-17 |
| **实验的准备阶段**  **(指导教师填写)** | **课程名称** | **网络协议分析与攻防技术** | | |
| **实验名称** | 实验四 主机扫描技术 | | |
| **实验目的** | 1. 掌握主机扫描的技术原理 2. 掌握漏洞扫描技术原理。 3. 了解常见的系统漏洞及防范方法。 4. 掌握典型的综合扫描工具。 | | |
| **实验内容** | 一、NMap，也就是Network Mapper，用来扫描网络上计算机开放的网络连接端口。它是网络管理员必用的软件之一，用以评估网络系统安全。正如大多数被用于网络安全的工具，NMap也是不少黑客及骇客（又称脚本小子）爱用的工具 。系统管理员可以利用NMap来探测工作环境中未经批准使用的服务器，但是黑客会利用nmap来搜集目标电脑的网络设定，从而计划攻击的方法。  NMap相关命令简单介绍（IP地址仅供参考）   |  |  | | --- | --- | | 扫描单机端口 | nmap 192.168.1.12 | | 扫描IP段端口 | nmap 192.168.1.2-200 | | 扫描指定端口 | namp -p 21,80,3389 192.168.1.12 | | 扫描端口段 | nmap -p 1-65535 192.168.1.12 | | 半开连接扫描 | nmap -sS 192.168.1.12 | | 全连接扫描 | nmap -sT 192.168.1.12 | | 显示banner信息 | nmap -sV 192.168.1.12 | | TCP FIN 扫描Unix系统 | nmap -sF 192.168.1.12 | | TCP NULL 扫描Unix系统 | nmap -sN 192.168.1.12 | | TCP Xmax 扫描Unix系统 | nmap -sX 192.168.1.12 |     扫描原理  全连接扫描（TCP Connect 扫描），通过调用socket函数connect()连接到目标计算机上，完成一次完整的三次握手过程。如果端口处于侦听状态，那么connect()就能成功返回。否则，这个端口不可用，即没有提供服务。优点是稳定可靠，不需要特殊的权限。缺点是扫描方式不隐蔽，服务器日志会记录下大量密集的连接和错误记录 ，并容易被防火墙发现和屏蔽。  半连接扫描（TCP SYN 扫描），扫描器向目标主机端口发送SYN包。如果应答是RST包，那么说明端口是关闭的；如果应答中包含SYN和ACK包，说明目标端口处于监听状态，再传送一个RST包给目标机从而停止建立连接。由于在SYN扫描时，全连接尚未建立，所以这种技术通常被称为半连接扫描。优点是隐蔽性较全连接扫描好，一般系统对这种半扫描很少记录。缺点是通常构造SYN数据包需要超级用户或者授权用户访问专门的系统调用。  隐蔽扫描技术  隐蔽扫描是指在网络端口扫描过程中隐蔽自身的技术。具体来讲，就是能够不被目标系统的日志机制，扫描监测系统和入侵检测系统扑捉，绕过防火墙二侦测到目标主机运行服务的扫描技术。NMap下的相关扫描方式有TCP FIN扫描、TCP NULL 扫描和TCP Xmax扫描。  TCP FIN 扫描就是TCP Xmas和Null扫描是FIN扫描的两个变种。Xmas扫描打开FIN，URG和PUSH标记，而Null扫描关闭所有标记。这些组合的目的是为了通过对FIN标记数据包的过滤。当一个这种数据包到达一个关闭的端口，数据包会被丢掉，并且返回一个RST数据包。否则，若是打开的端口，数据包只是简单的丢掉（不返回RST）。优点是隐蔽性好。缺点是通常适用于Unix主机，而不适用于Windows。  TCP Xmas和Null扫描是FIN扫描的两个变种。Xmas扫描打开FIN，URG和PUSH标记，而Null扫描关闭所有标记。这些组合的目的是为了通过对FIN标记数据包的过滤。当一个这种数据包到达一个关闭的端口，数据包会被丢掉，并且返回一个RST数据包。否则，若是打开的端口，数据包只是简单的丢掉（不返回RST）。  二、利用X-Scan工具进行：   1. 漏洞扫描：IPC、RPC、POP3、FTP、TELNET、WEB。 2. 暴力破解：FTP、POP3、HTTP。 | | |
| **实验类型**  （打☑） | ☑验证性 □演示性 □设计性 □综合性 | | |
| **实验的重点、难点** | Nmap的命令行操作  X-Scan工具的使用 | | |
| **实验环境** | 本次实验根据本地主机和扫描目标主机的真实网络地址进行。 | | |
| **实验的实施阶段** | **实验步骤及实验结果** | 1. **Zenmap GUI** 2. 安装Nmap后，并打开Zenmap GUI。**实验过程截图如下：**     点击菜单栏中的【Scan】，点击【New Windows】，即可创建新的扫描窗口，并可以输入Target：IP1。IP1为扫描目标的IP地址，可以选择同学主机或者其他IP地址。**实验过程截图如下：**     1. 在Profile框格中，点击右侧小三角号，即可选择扫描方式，在此处可以选择【Regular scan】。**实验过程截图如下：**      1. 点击右侧【Scan】按钮即可进行扫描。**实验过程截图如下：**        1. 经过一段时间之后，即可得到扫描结果。**实验过程截图如下：**      1. 点击【Services】和【Prots/Hosts】即可查看目标主机开起的服务所对应的窗口。**实验过程截图如下：**      1. **ZenMap命令行模式** 2. 打开cmd，输入命令【nmap】即可得到命令帮助信息。**实验过程截图如下：**      1. 在命令行下输入命令【namp IP1】，进行Regular Scan。**实验过程截图如下：**      1. 在命令行下输入命令【nmap -p 21,22,80,3389 IP1】，对指定的21，22，80，3389端口进行扫描。      1. 在命令行输入【nmap -sT **IP1**】，对目标主机进行全连接扫描。全连接扫描完成完整的三次握手过程，稳定可靠但容易被日志记录。此种方法花费时间可能较长。**实验过程截图如下：**     30s﷽﷽﷽﷽﷽﷽﷽﷽﷽﷽﷽﷽﷽﷽﷽﷽﷽﷽﷽行服务的扫描行为。   1. 在命令行输入【nmap -sS **IP1**】，对目标主机进行半开连接扫描。扫描器向目标主机发送SYN包测试主机是否监听某个端口而不进行全连接。此种方法比全连接扫描方式隐蔽。**实验过程截图如下：**      1. 输入命令【nmap -sV **IP1**】，用以显示banner信息。**实验过程截图如下：**      1. 输入命令【nmap -oX 1.xml **IP1**】，即将扫描结果以xml的形式输出，文件名为【1.xml】。**实验过程截图如下：**      1. 保存文档的位置在【C:\Documents and settings\Administrator】，双击保存好的【1.xml】文件，即可查看结果。**实验过程截图如下：**      1. 在命令行界面，nmap命令也可以组合使用，具体命令说明请参考命令【nmap】的结果，具体组合方式请同学们自行尝试。   **三、设置X-Scan参数。**   1. 解压Xscan压缩包，并打开xscan\_gui.exe,打开运行界面进行设置，点击菜单栏设置中的扫描参数进入参数设置界面。**实验过程截图如下：**      1. 点击载入按钮可载入预先设置好的参数文件，另存可将当前设置好的各个参数信息保存至一个文件内，以便下次应用时直接进行读取。地址簿可将预先添加好的各个地址直接加入到ip地址内(此步骤可跳过)。**实验过程截图如下：**      1. 选择“载入”可读取多台主机IP地址并对多台主机同时实施操作，由于本实验使用默认配置文档，所以没有读取出IP地址（此步骤可跳过）。**实验过程截图如下：**     **四、全局设置(此模块包含所有全局性扫描选项)**   1. 扫描模块：主要包含一些服务和协议弱口令等信息的扫描，根据字典探测主机各种服务的开启情况及相应的弱口令，对应到每一项都有相应的说明。**实验过程截图如下：**      1. 并发扫描：主要是对扫描的并发数量进行设置，包括最大并发主机数、最大并发线程数和各插件最大并发数量的设置。**实验过程截图如下：**        1. 扫描报告：对主机进行扫描完成后的报告生成情况进行设定。**实验过程截图如下：**      1. 其它设置：主要是对扫描过程中对扫描进度的显示和附加的一些设置，可根据实际环境进行设置，本实验注意勾选“无条件扫描”。**实验过程截图如下：**     **五、插件设置（此模块包含各扫描插件的相关设置）**   1. 端口相关设置：主要设置想要扫描的各个端口、检测方式和预设的各个服务协议的端口等内容（本次实验主要检测FTP弱口令，所以只填写了21端口）。**实验过程截图如下：**      1. SNMP相关设置：主要设置检测SNMP的相关信息。**实验过程截图如下：**      1. NETBIOS相关设置：主要设置检测NETBIOS的相关信息。**实验过程截图如下：**10所示      1. 漏洞检测脚本设置：主要是针对于各个漏洞编写的检测脚本进行筛选，选择需要利用的脚本，为方便起见一般设置为全选，也可根据自己需要进行选择。**实验过程截图如下：**        1. CGI相关设置：对CGI的一些参数进行设置。**实验过程截图如下：**      1. 字典文件设置：主要是对扫描过程中所需要用到的字典进行选取，也可自己手动进行添加数据字典。**实验过程截图如下：**     **六、进行扫描：**   1. 设置完成后点击绿色按钮或菜单中文件->开始扫描进行探测扫描，此扫描的速度与网络环境情况和本机配置等有关，不尽相同。**实验过程截图如下：**      1. 报告生成：扫描完成后会根据报告设置中自动生成报告项生成报告。**实验过程截图如下：**      1. 根据探测扫描报告取得的信息进行漏洞测试，检测到FTP弱口令漏洞。**实验过程截图如下：**      1. 打开我的电脑，输入地址ftp://**IP1**/，进行漏洞攻击测试。右键点击空白，选择登陆，利用扫描得到的弱口令进行登陆。**实验过程截图如下：** | | |
| **实验结果的处理阶段** | **实验结果的分析与总结** | **【实验思考】**   * + - 1. 使用NMap的目的在于什么？   一般来说，系统防火墙可以通过阻止入站或出站连接来限制网络流量，从而防止未经授权的访问或攻击。这意味着，如果扫描软件需要建立或发送网络连接，它可能会受到防火墙的屏蔽作用，从而无法正常工作。  另外，一些系统防火墙还可能会检测和阻止具有特定行为或特征的程序，例如端口扫描或恶意软件。如果扫描软件被认为具有类似恶意程序的行为，防火墙可能会阻止其运行或访问网络资源。  然而，如果扫描软件被允许在防火墙中进行例外设置，或者如果防火墙规则明确允许扫描软件进行特定类型的网络连接，则防火墙可能不会对其进行屏蔽作用。   * + - 1. 系统防火墙对扫描软件有屏蔽作用吗？   确定网络上的主机：Nmap可以扫描网络上的所有主机，并列出它们的IP地址和MAC地址等信息。  发现开放的端口：Nmap可以扫描网络上的所有端口，并列出它们的状态（开放、关闭、过滤等）和服务类型（如SSH、HTTP、FTP等）等信息。  识别网络服务：Nmap可以识别运行在开放端口上的网络服务，并列出它们的版本号和其他信息，以便管理员评估这些服务的安全性。  检测网络漏洞：Nmap可以利用已知的漏洞和攻击方法，对网络上的主机和服务进行攻击和测试，以发现可能存在的漏洞。 | | |