XCTF

第4章 漏洞扫描

《Metasploit渗透测试指南》

目录 content

XCTF

目录 content

0x01 基本的漏洞扫描

XCTF

基本漏洞扫描

- 基本原理：通过网络对目标系统进行探测，向目标系统发送数据，将反馈数据与漏洞特征进行匹配，进而获得漏洞信息
- 渗透测试需要隐蔽进行时，建议不要使用漏洞扫描器
- 宁可误报，不可漏报
- 扫描质量很大程度上取决于漏洞特征库

目录 content

XCTF

0x02 使用Nexpose进行扫描

XCTF

Nexpose

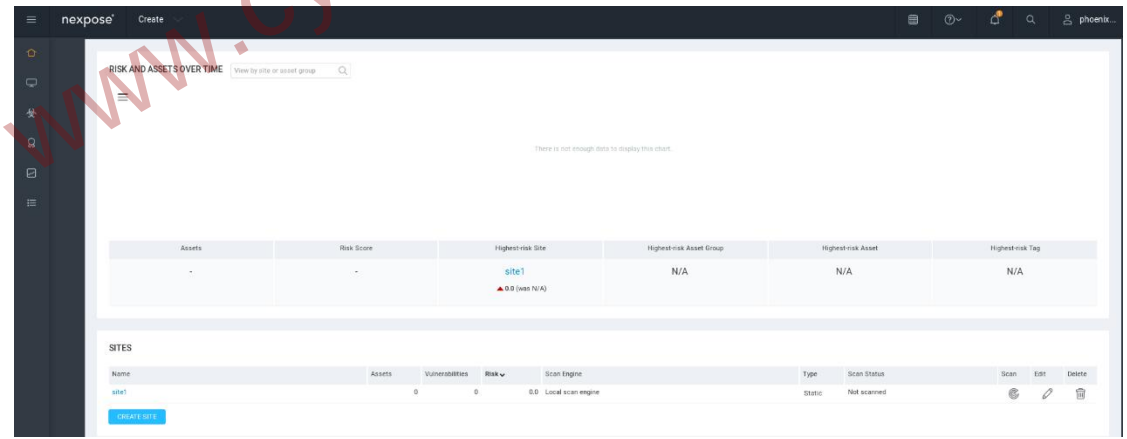
- Rapid7推出的漏洞扫描器，通过对网络进行扫描，查找出网络上正在运行的设备，最终识别出操作系统和应用程序上的安全漏洞。Nexpose随后对扫描得到的数据进行分析和处理，并生成各种类型的报告
- 可以在Rapid7官网申请试用Nexpose，试用没有时长限制
- 我们扫描的目标是一个默认安装的Windows XP SP2主机，其具体配置参考附录A。首先，我们对目标进行一次公开的白盒扫描；然后，将漏洞扫描的结果导入到Metasploit中。在本节结束前，还会为你介绍如何在MSF终端中调用Nexpose进行漏洞扫描，在MSF终端中运行Nexpose可以让你无需打开基于Web的图形用户界面，而且省去了从外部导入扫描报告的麻烦

0x02 使用Nexpose进行扫描

XCTF

创建站点向导

- 站点是指一系列相关设备的逻辑集合，可能是子网、一个或多个服务器/工作站
- 站点是Nexpose的扫描对象



0x02 使用Nexpose进行扫描

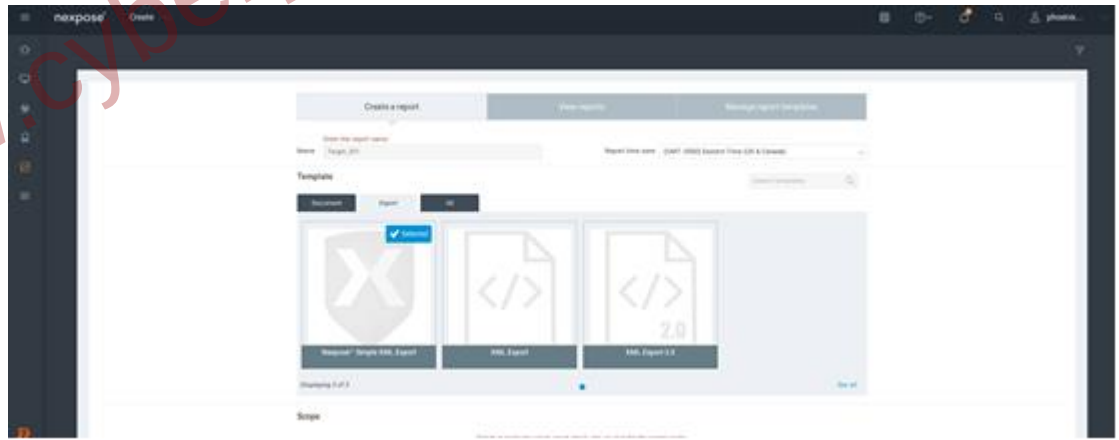
手动扫描向导

- 指定哪些资产包含在扫描任务内
- 扫描状态页面显示扫描进度和资产识别状态

0x02 使用Nexpose进行扫描

生成报告向导

- 选择报告模版
- 选择报告内容
- 生成扫描报告



0x02 使用Nexpose进行扫描

将扫描报告导入到Metasploit中

- msfconsole中，执行db_import
- 完成扫描报告导入后，可使用hosts, vulns, services, loot, notes查看报告中各项信息
- 旧版本的msfconsole中，使用db_hosts –c <option1, option2…>来查看扫描结果中的各项信息，使用db_hosts –help查看命令详细参数。这条命令已经不推荐使用，可能会在未来的版本被移除

0x02 使用Nexpose进行扫描

在MSF控制台中运行Nexpose

- msf > load nexpose
- 执行扫描前，使用Nexpose凭据连接到运行中的Nexpose实例
- 在Metasploit连接数据库的情况下，在msfconsole中调用Nexpose，扫描结果将直接存入数据库，便于后续分析与利用

目录 content

XCTF

0x03 使用Nessus进行扫描

XCTF

Nessus

- Nessus漏洞扫描器由Tenable Security（*http://www.tenable.com/*）推出，是当前使用最为广泛的漏洞扫描器之一。使用Metasploit的Nessus插件，你可以在MSF终端中启动扫描并从Nessus获取扫描结果。但在下面的例子中，我们将演示如何导入由独立运行的Nessus扫描器所生成的扫描结果。
- 我们将使用免费的家用版Nessus 4.4.1，对本章中所提到的扫描目标进行授权扫描。
- 在渗透测试的前期，你使用的工具越多，你就能对后续的渗透攻击工作提供更多有效的攻击方案选择。
- Nessus也使用postgresql，默认安装的Nessus会连接自集成的postgresql，默认配置下，这个数据库实例使用的端口与msfconsole默认连接的数据库端口不同，在同时运行Nessus和msfconsole时，注意修改相关数据库连接配置。

0x03 使用Nessus进行扫描

XCTF

配置Nessus

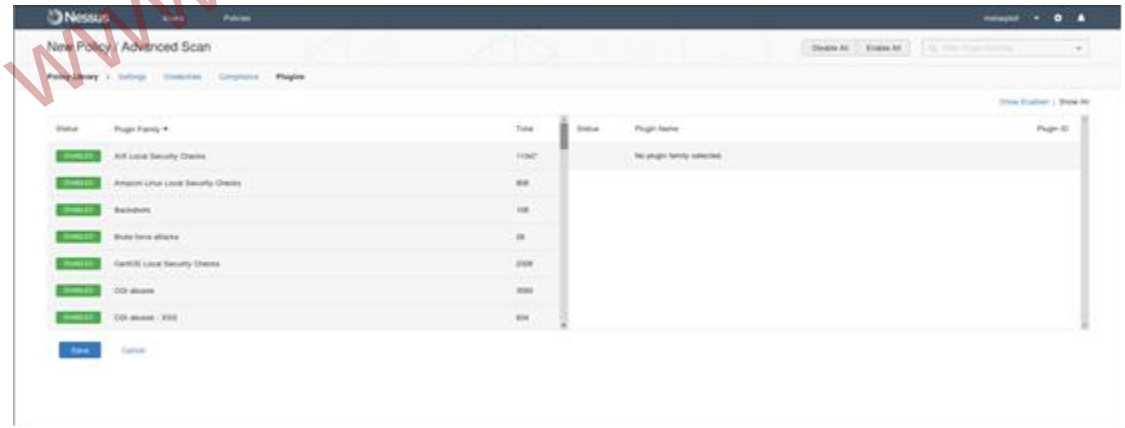
- 务必记住安装Nessus时设置的登录凭据
- Reports（报告）：所有曾运行过的漏洞扫描任务
- Scan（扫描）：创建新的扫描或查看当前的扫描进度
- Policies（策略）：设置Nessus在扫描时所包含的扫描插件
- Users（用户）：添加能够访问Nessus服务器的用户账户

0x03 使用Nessus进行扫描

XCTF

创建Nessus扫描策略

- 在Policies（策略）选项卡上，点击绿色的Add（添加）按键
- 根据目标的操作系统和扫描任务范围，选择使用的插件
- 如有需要，可以为扫描设置系统登录凭据，更全面地执行扫描

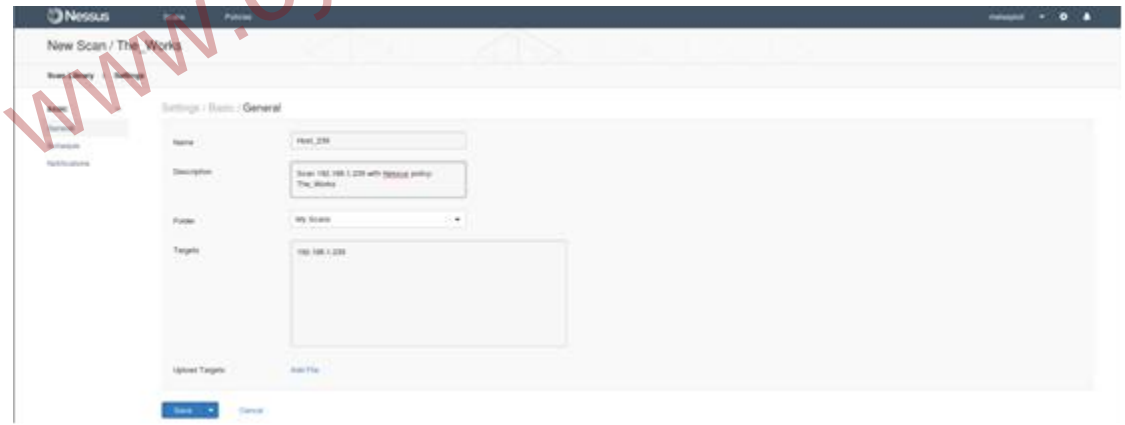


0x03 使用Nessus进行扫描

XCTF

执行Nessus扫描

- 根据扫描目标，选择合适扫描策略
- 填写扫描目标的地址或地址块

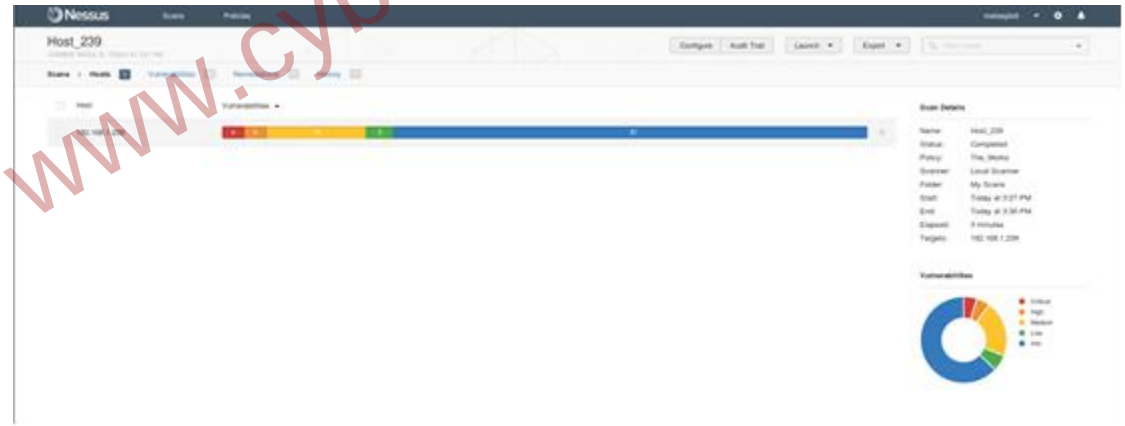


0x03 使用Nessus进行扫描

XCTF

Nessus报告

- 报告首页显示漏洞和漏洞等级的摘要，可以查看漏洞详情



0x03 使用Nessus进行扫描

将扫描结果导入Metasploit框架中

- msfconsole中，执行db_import
- 完成扫描报告导入后，可使用hosts, vulns, services, loot, notes查看报告中各项信息
- 旧版本的msfconsole中，使用db_hosts –c <option1, option2…>来查看扫描结果中的各项信息，使用db_hosts –help查看命令详细参数。这条命令已经不推荐使用，可能会在未来的版本被移除
- Nessus扫描结果中的漏洞信息包含漏洞编号，在撰写渗透测试报告时非常有价值，使用vulns命令查看

0x03 使用Nessus进行扫描

在Metasploit内部使用Nessus进行扫描

- msf > load nessus
- 执行扫描前，使用Nessus凭据连接到运行中的Nexssus实例
- 添加扫描任务：使用**nessus_scan_new**命令，并在后面加上扫描策略的ID号、扫描任务的名字、扫描任务的描述以及目标IP地址，然后输入**nessus_scan_launch**命令手动启动扫描，策略ID使用**nessus_policy_list**命令查看
- 查看扫描报告：使用**nessus_scan_list**命令查看任务状态；使用**nessus_db_import <Scan_ID>**将指定扫描任务的报告导入到Metasploit数据库中，Scan_ID通过**nessus_scan_list**命令获得

目录 content

XCTF

0x04 专用漏洞扫描器

专用漏洞扫描器

虽然市面上有很多商业的漏洞扫描产品，但你的选择并不仅限于它们。当你想要在一个网络上查找某个特定的漏洞时，Metasploit自带的许多辅助模块可以帮助你完成这样的任务。

- 验证SMB登录
- 扫描开放的VNC空口令
- 扫描开放的X11服务器

0x04 专用漏洞扫描器

验证SMB登录

- msf > use auxiliary/scanner/smb/smb_login
- SMBPass，SMBUser可以设置为字符串或文件，设置为文件时可以与wordlist等结合进行爆破
- 在内网中，可能很多机器都是由同一个管理员安装，或者使用同一个镜像克隆，这意味着大量机器可能使用同样的登录凭据

0x04 专用漏洞扫描器

扫描开放的VNC空口令

- msf > use auxiliary/scanner/vnc/vnc_none_auth
- 虽然最新版本的VNC服务器已经不再允许空口令，但是老旧且疏于维护的服务器并不少见
- 在执行VNC空口令扫描之前，执行VNC版本扫描，有助于提高扫描效率

0x04 专用漏洞扫描器

扫描开放的X11服务器

- msf > use auxiliary/scanner/x11/open_x11
- 现在X11一般作为VNC服务组件出现，在这种应用场景下扫描器不会发现免验证的X11服务器
- 有兴趣的可以使用该扫描器对Metasploitable V1进行测试

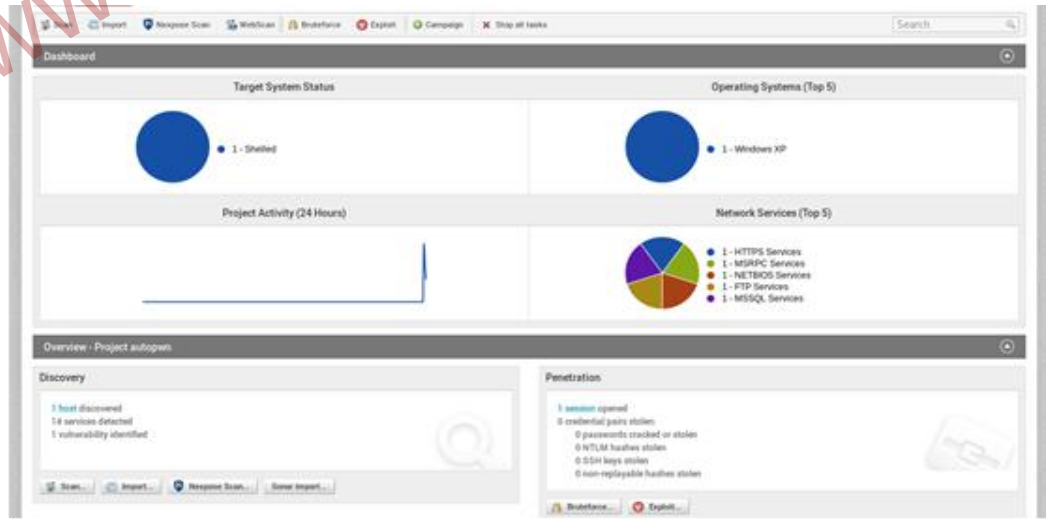
目录 content

XCTF

0x05 利用扫描结果进行自动化攻击

利用扫描结果进行自动化攻击

- 目前Metasploit Framework不再提供autopwn功能，想要进行自动化渗透攻击，需要使用收费版本Metasploit Pro
- 在Metasploit Pro中，利用自动化攻击，只需要配置扫描目标，即可完成漏洞扫描、渗透攻击和会话建立



XCTF

Thanks for watching 谢谢