

黑客入门，从HTB开始

原创

瑟荻 于 2019-10-20 20:25:42 发布 46322 收藏 906

分类专栏: [安全](#) 文章标签: [HTB](#) [安全攻防](#) [靶机](#) [web安全](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/real1991/article/details/102656213>

版权



[安全 专栏收录该内容](#)

6 篇文章 0 订阅

订阅专栏

Hack the box 是国外的一个靶机平台, 里面的靶机包含多种系统类型, 并且里面可以利用的漏洞类型多种多样, 有很多靶机其实非常贴近实战情景。因此 HTB 是一个很好的学习渗透测试靶场。

之前在 HTB 也玩过一些机器。里面的机器难度有好几个档次, insane 难度的一般都是极其困难的, 这种机器一般让我对着大神的 Writeup 我可能都没有办法复现出来。之前也有在公众号上分享过几篇 HTB 机器的 Writeup, 基本上都是比较简单的, 这一次整理出来给感兴趣的同学看一看。主要讲一下这些靶机主要的难点, 后面有相应的 Writeup 链接。

Bastion



这是一台 Windows 机器, 如果使用 Command VM 来进行渗透的话会更方便一点, 不过使用 Kali 也是可以的。这台靶机主要的难点是 VHD 的挂载以及 mRemoteNG 中配置密码的破解。

Holiday



Holiday 是一个困难度为 insane 的机器，获取普通用户的权限比较困难。这台靶机最大的难点就是如何通过 XSS filter，这台机器已经限制了很多 XSS 的 payload。

Help



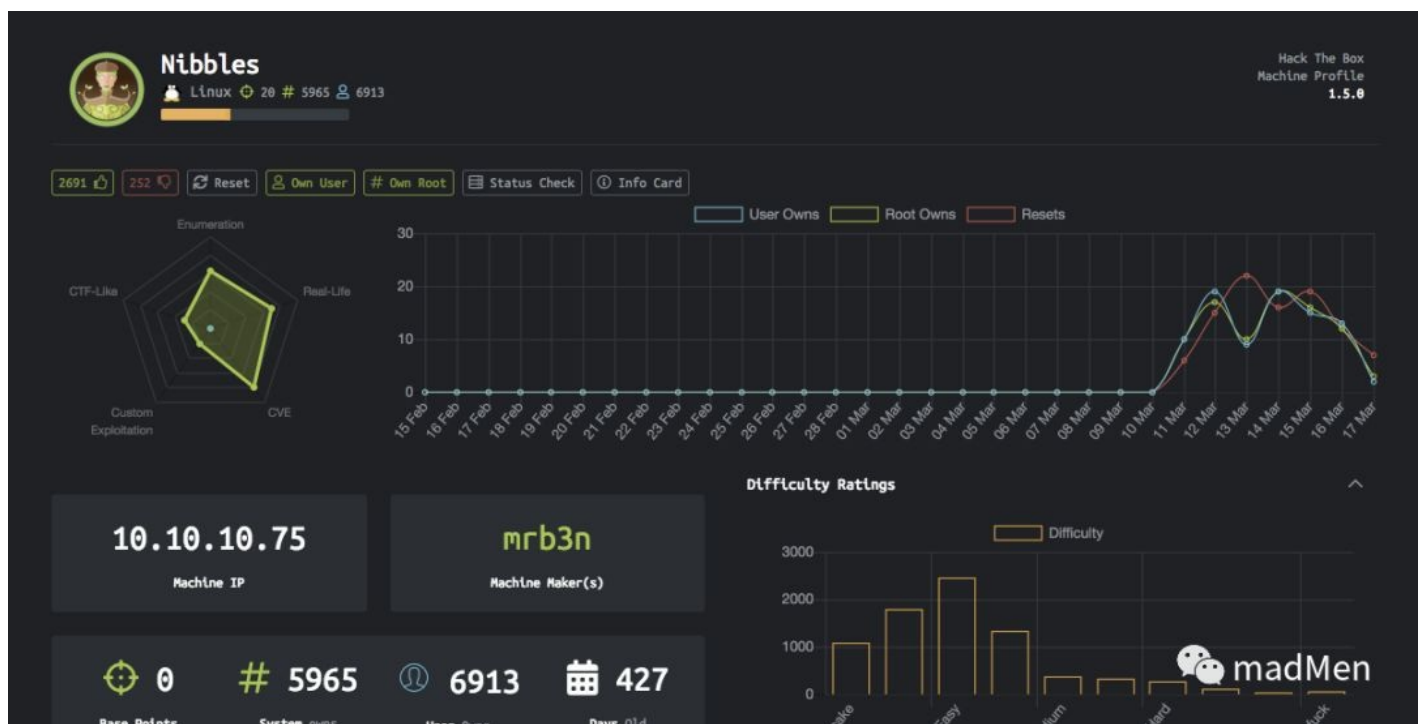
Help 是一台比较简单的靶机，获取普通用户的权限通过 HelpDeskZ 的漏洞即可，这里注意一点，不要被表面的一些提示所欺骗。提权使用的是一个内核漏洞来进行提权，属于提权基本套路，但经常会有人忘记这一点。

Bashed



Bashed 的普通用户权限非常的直白，通过提供的 webshell 工具就可以获取权限。提权则对比起来稍微有点困难，要找到一个特殊的脚本文件。这种情况在现实生活中也是存在的，使用 root 账户运行了某些脚本。

Nibbles



普通用户的权限需要基于一个开源的博客系统的漏洞，不过这个漏洞需要获取管理员的口令。一般对于靶机的登录口令，一般是不需要使用暴力破解的，一般如果尝试过 rockyou.txt 字典之后还是没有结果，建议就是需要换一换思路了。一般尝试密码的时候，可以先简单测试一些基本的弱密码或者与靶机有关的字符，比如这个管理员的密码就是 nibbles。

Cronos



Cronos 涉及到 DNS 域传输漏洞，往往可以通过这个漏洞收集更多的域名信息。这台机器的重点是发现应用中存在命令执行的地方，有一些工具，尤其是一些网络相关的工具，往往存在命令执行漏洞。

总结

HTB 是一个非常好的靶场，涵盖题型多，系统类型也丰富，贴近实战。最大的缺点可能就是网络问题了，延时较高，很多情况可能甚至都连不上。

文末福利：

本文留言点赞超过10个以上，可以后台回复 HTB 获取官方 Writeup 大礼包（44台靶机 Writeup）。

名称	修改日期	大小	类型
 Access.pdf	2019年3月6日 下午7:36	910 KB	PDF 文稿
 Apocalyst.pdf	2019年3月21日 下午8:45	563 KB	PDF 文稿
 Bashed.pdf	2019年4月3日 下午9:29	314 KB	PDF 文稿
 Bastard.pdf	2019年3月18日 下午6:38	248 KB	PDF 文稿
 Beep.pdf	2019年3月9日 下午4:45	292 KB	PDF 文稿
 Blue.pdf	2019年3月17日 下午10:14	343 KB	PDF 文稿
 Bounty.pdf	2019年3月16日 下午3:02	1.1 MB	PDF 文稿
 Brainfuck.pdf	2019年4月23日 下午10:16	524 KB	PDF 文稿
 Calamity.pdf	2019年3月20日 下午7:12	669 KB	PDF 文稿
 Celestial.pdf	2019年7月8日 下午7:09	401 KB	PDF 文稿
 Charon.pdf	2019年4月13日 上午10:20	368 KB	PDF 文稿
 Conceal.pdf	2019年6月16日 下午2:00	925 KB	PDF 文稿
 Cronos.pdf	2019年3月14日 下午9:09	448 KB	PDF 文稿
 Devel.pdf	2019年3月7日 下午9:22	324 KB	PDF 文稿
 Dropzone.pdf	2019年5月3日 上午8:18	451 KB	PDF 文稿
 Enterprise.pdf	2019年6月8日 下午1:31	388 KB	PDF 文稿
 Europa.pdf	2019年4月1日 下午8:04	503 KB	PDF 文稿

♥ □ 看完三件事

如果你觉得这篇内容对你挺有启发，我想邀请你帮我三个小忙：

点赞，让更多的人也能看到这篇内容（收藏不点赞，都是耍流氓 -_-）

关注公众号「mad_coder」，不定期分享原创知识。



点击菜单历史消息，获取往期精彩原创文章。