专注APT攻击与防御

https://micropoor.blogspot.com/

在办公区的内网中，充斥着大量的ftp文件服务器。其中不乏有部分敏感文件，也许有你需要的密码文件，也许有任务中的目标文件等。本季从讲述内网ftp服务器的发现以及常用的相关模块。

靶机介绍：

靶机一：Windows 2003 | 192.168.1.115靶机二：Debian | 192.168.1.5

msf内置search模块，在实战中，为了更快速的找到对应模块，它提供了type参数（未来会

具体讲到模块参数），以ftp模块为例。

msf > search type:auxiliary ftp

Matching Modules ================

Name Disclosure Date Rank Description

---- --------------- ---- -----------

auxiliary/admin/cisco/vpn\_3000\_ftp\_bypass 2006-08-23 normal Cisco VPN Concentrator 3000 FTP

Unauthorized Administrative Access

auxiliary/admin/officescan/tmlisten\_traversal

normal TrendMicro OfficeScanNT Listener

Traversal Arbitrary File Access

auxiliary/admin/tftp/tftp\_transfer\_util

normal TFTP File Transfer Utility

auxiliary/dos/scada/d20\_tftp\_overflow 2012-01-19 normal General Electric D20ME TFTP Server

Buffer Overflow DoS

auxiliary/dos/windows/ftp/filezilla\_admin\_user 2005-11-07

normal FileZilla FTP Server Admin

Interface Denial of Service

......

auxiliary/scanner/ftp/ftp\_version

auxiliary/scanner/ftp/ftp\_login

auxiliary/scanner/ftp/anonymous

当然msf也内置了nmap，来内网大量发现FTP存活主机，参数与使用与nmap一致。

msf auxiliary(scanner/ftp/anonymous) > db\_nmap -sS -T4 -p21 192.168.1.115

msf更多针对了ftpd。

ftp本地模糊测试辅助模块：

auxiliary/fuzzers/ftp/ftp\_pre\_post

关于ftp的f本地uzzer，更推荐的是本地fuzz，msf做辅助poc。

关于后期利用，poc编写，在未来的季中会继续讲述。

Micropoor