SNMP协议攻击

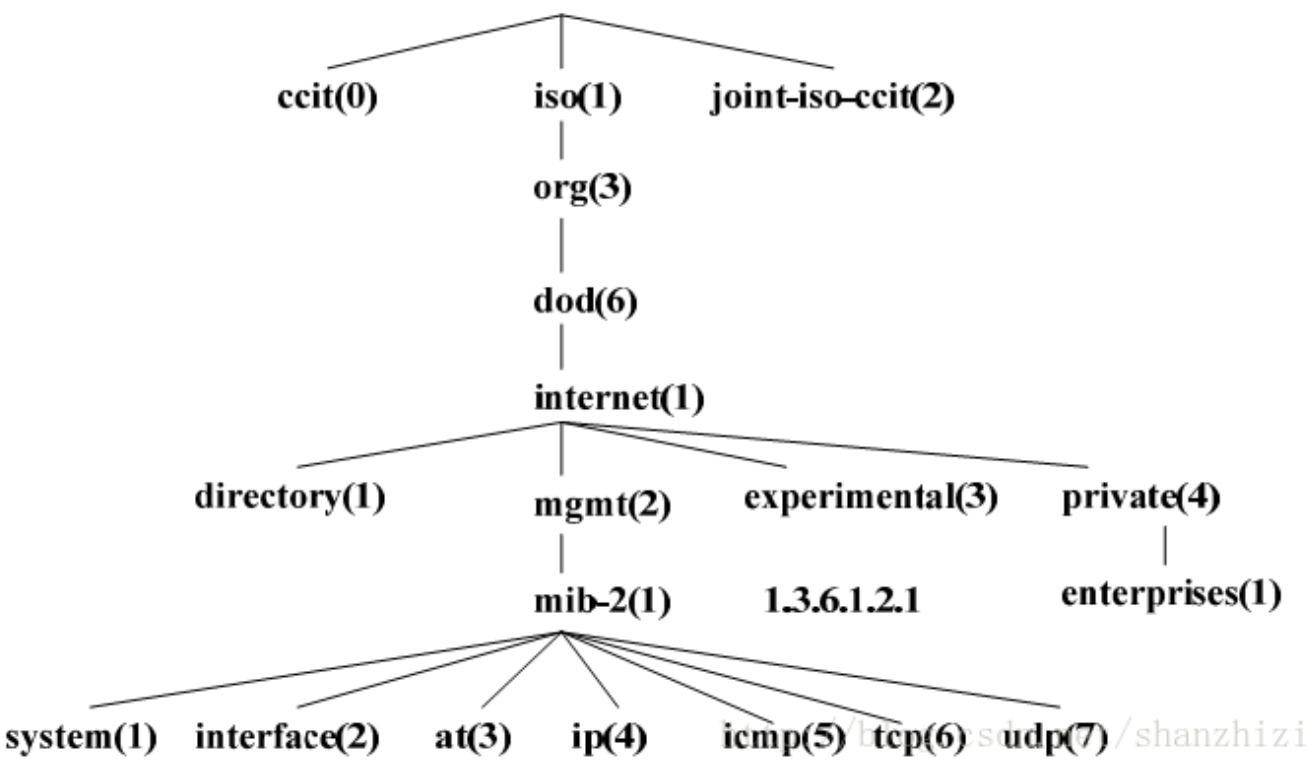
TimeS0ng / 2017-11-13 12:52:23 / 浏览数 3749 安全工具 工具 顶(0) 踩(0)

0x00. SNMP协议简介

简单网络管理协议（SNMP）是TCP / IP协议簇的一个应用层协议，工作在UDP
161端口，用于监控目标设备的操作系统、硬件设备、服务应用、软硬件配置、网络协议状态、设备性能及资源利用率、设备报错事件信息、应用程序状态等软

0x01.MIB-管理信息库

管理信息库MIB：任何一个被管理的资源都表示成一个对象，称为被管理的对象，MIB是被管理对象的集合。它定义了被管理对象的一系列属性：对象的名称、



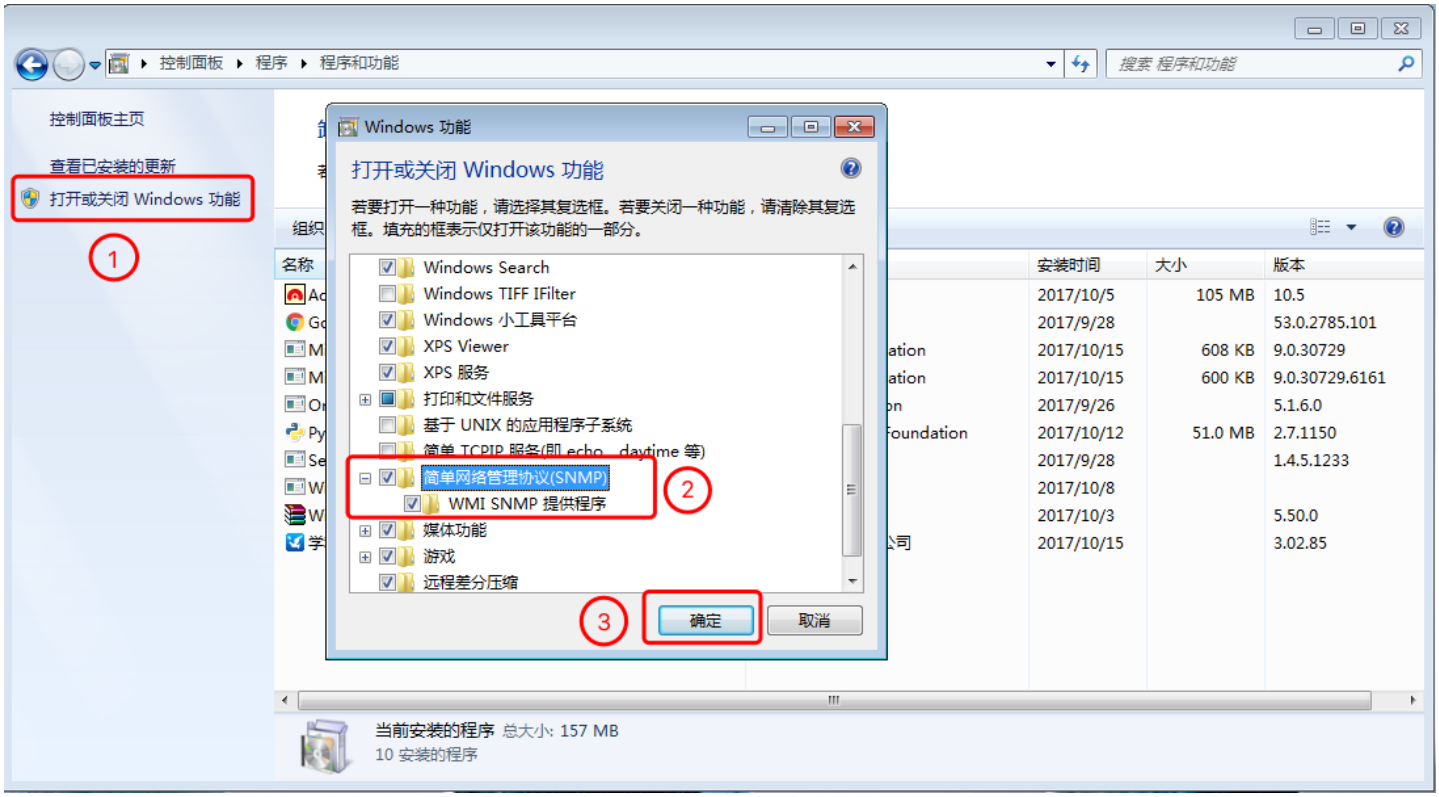
[*] 如上图所示，MIB是一种树形结构数据库，每个管理对象对应一个OID，如：.1.3.6.1.2.1.2.1.7

0x02. SNMP安装简介

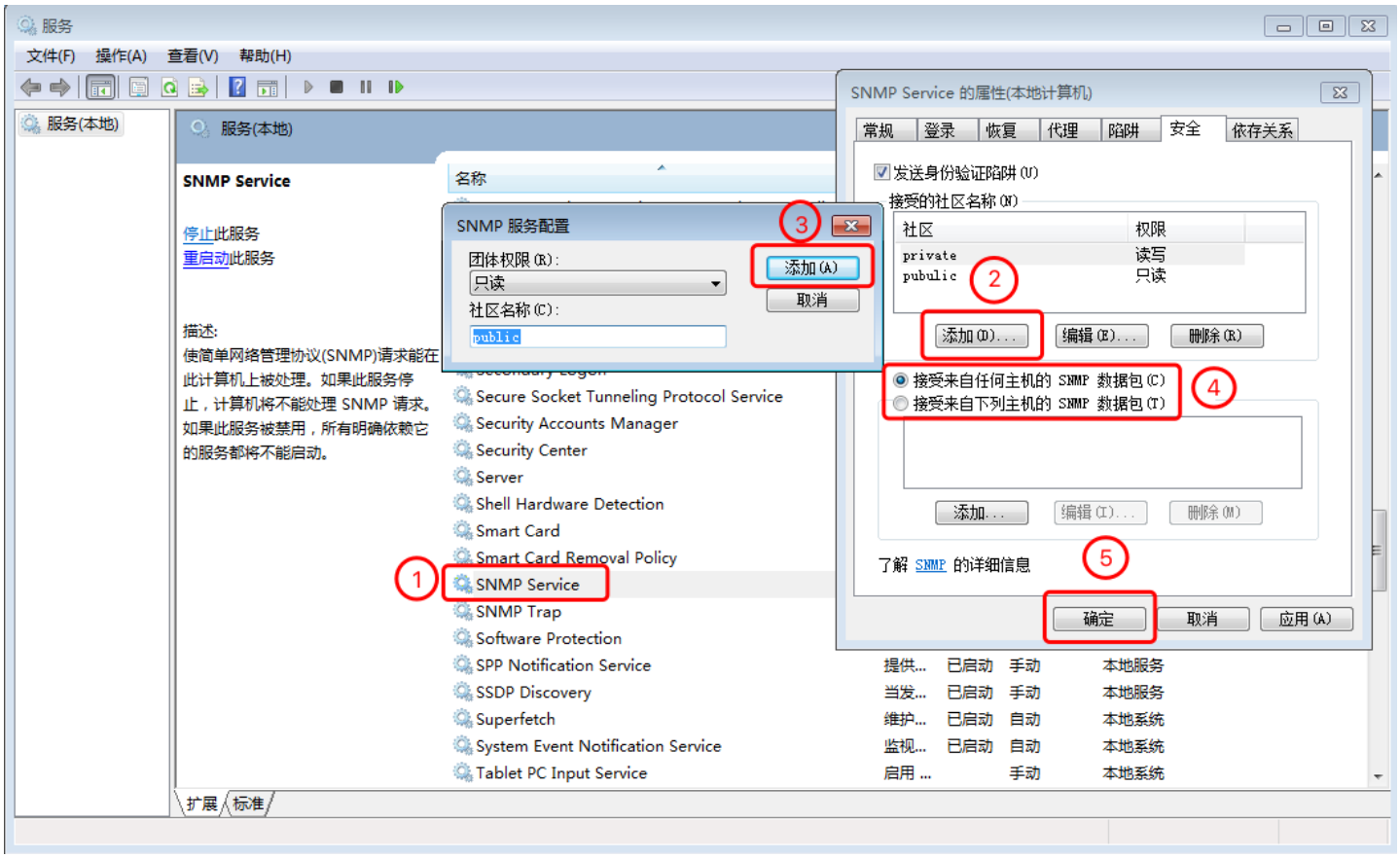
由上面介绍的SNMP服务可以看出SNMP对于渗透测试者来说简直就是信息宝藏，一旦这个服务协议被利用，那么目标的大部分配置信息都会暴露无遗，对于企

SNMP安装：

1. 打开控制面板卸载程序，然后进行如下操作就能安装SNMP服务



2. 在菜单栏输入 services.msc ，然后右键属性配置SNMP server，进行如下默认配置，然后重启服务



0x03. snmp-check 用法简介

snmp-check 支持对windows、类Unix、网络设备、打印机等安装SNMP服务的设备进行攻击。

攻击原理：

snmp-check通过发送各种预定义的OID对目标进行探测，收集目标SNMP管理的信息。

基础语法：

snmp-check 192.168.1.109 -c public -v 2c

参数：

-p 指定SNMP服务端口

-c 指定community（默认 public）

-v 指定snmp版本（1、2c，默认1）

-w 检查是否可写

-r 重试次数（默认1次）

-t 超时时长（默认5秒）

-d 禁用TCP 连接尝试

0x04. snmp-check实战

环境准备：

靶机win 7 IP=192.168.1.09

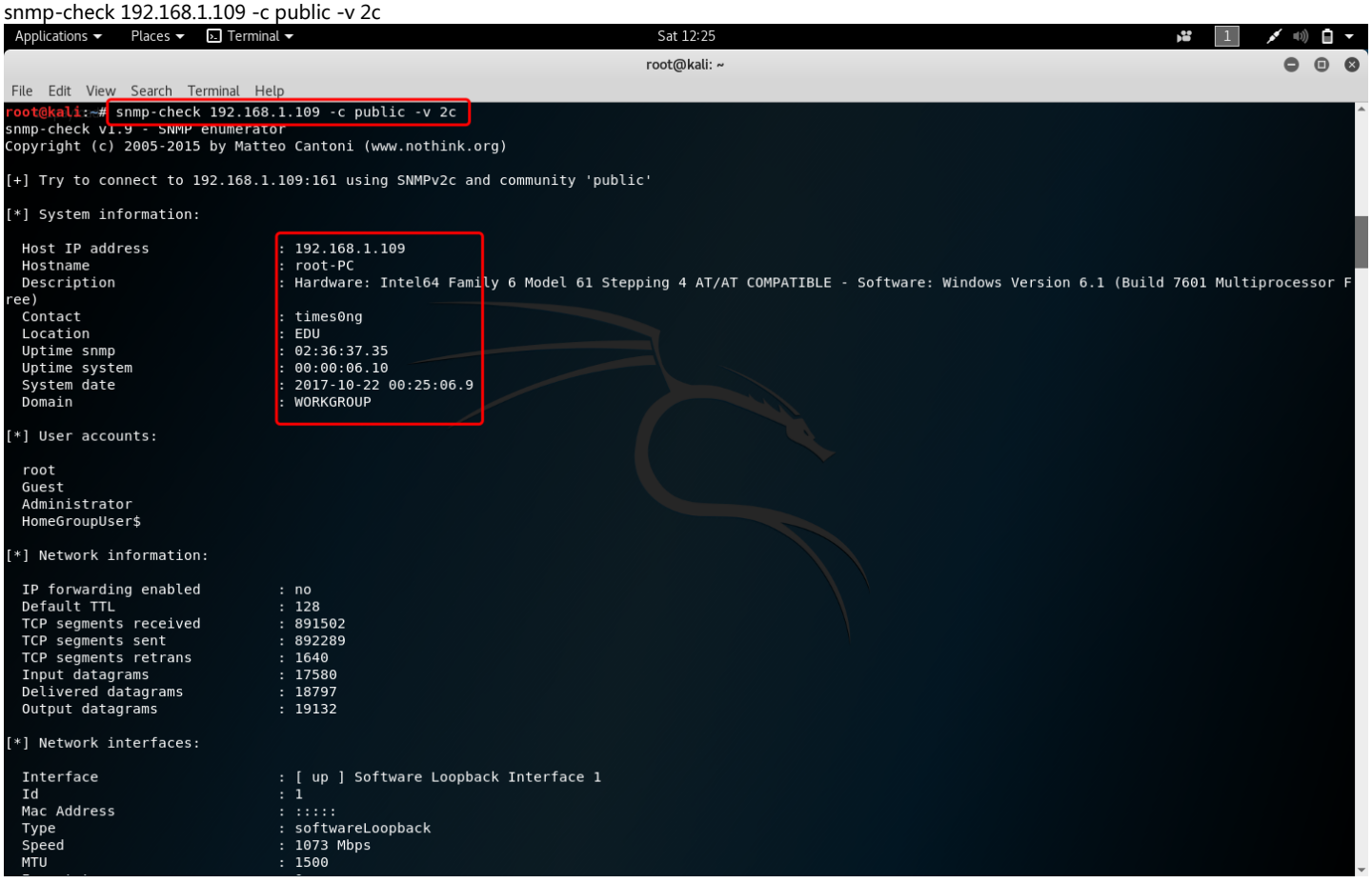
kali Linux

实战演示：

1. 靶机开启SNMP服务，并进行默认配置

2. 利用snmp-check 获取靶机信息

snmp-check 192.168.1.109 -c public -v 2c



上一篇：SMB协议探测攻击 下一篇：DNS查询工具

1. 2 条回复

 hades 2017-11-13 13:17:00

@TimeS0ng ^^

0 回复Ta

 xkkhh 2019-01-09 10:02:40

要是能修改文件或者执行命令就好了

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板