专注APT攻击与防御

https://micropoor.blogspot.com/

引言（1）：

目标资产信息搜集的广度，决定渗透过程的复杂程度。

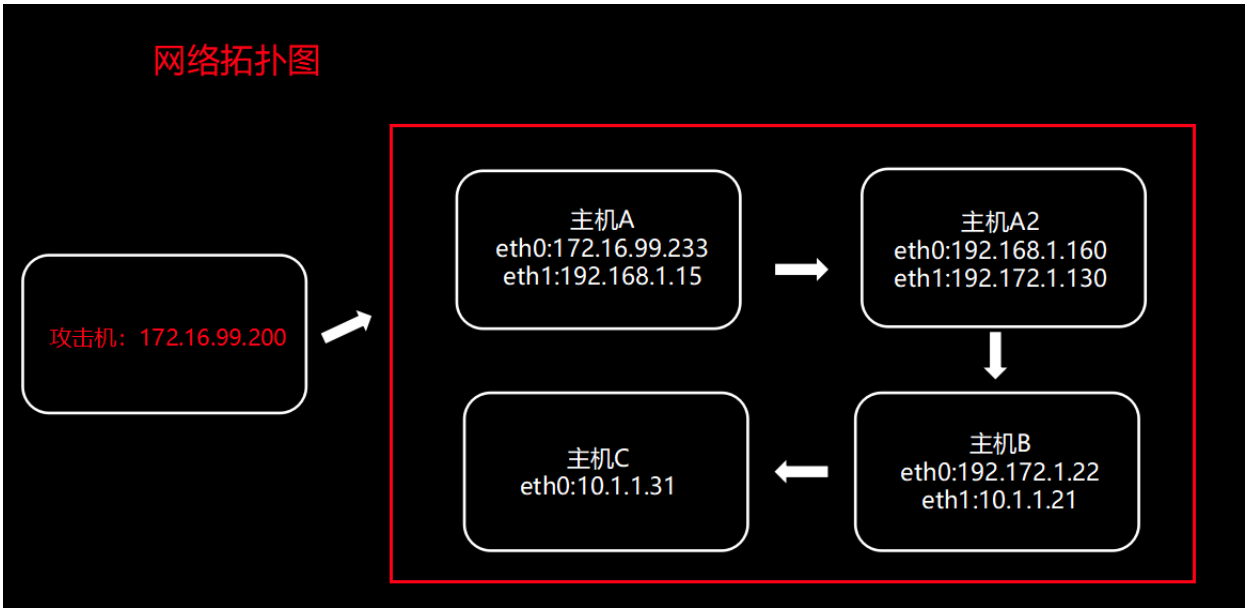
目标主机信息搜集的深度，决定后渗透权限持续把控。

渗透的本质是信息搜集，而信息搜集整理为后续的情报跟进提供了强大的保证。

持续渗透的本质是线索关联，而线索关联为后续的攻击链方提供了强大的方向。

后渗透的本质是权限把控，而权限把控为后渗透提供了以牺牲时间换取空间强大基础。

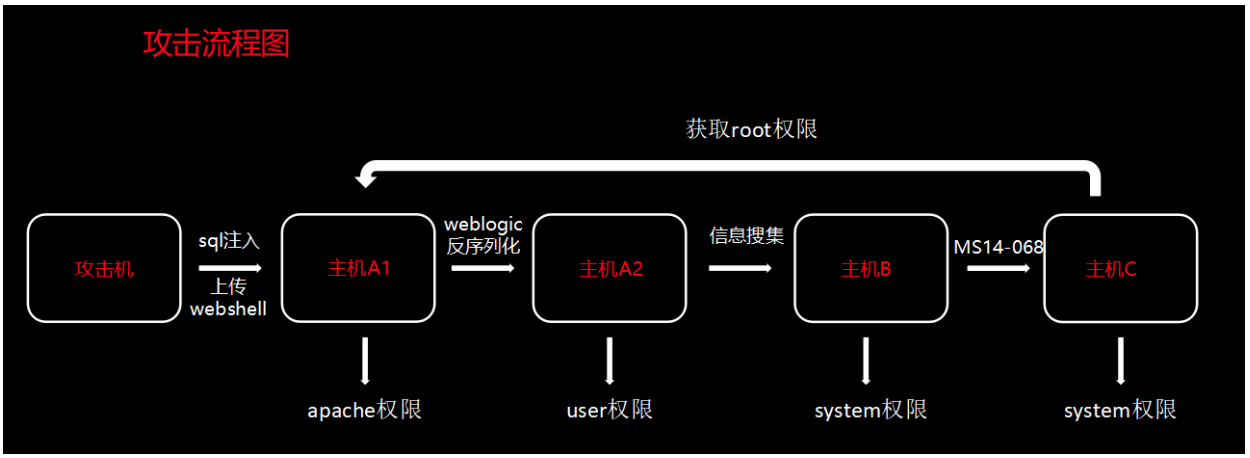
靶机背景介绍：



- 主机A1：CentOs x64 全补丁，无提权漏洞，可互联网
- 主机A2：Windows 2008 x64 全补丁 无提权漏洞，脱网机
- 主机B： Windows 2008 x64 全补丁 无提权漏洞，域内主机，脱网机
- 主机C： Windows 2008 x64 域控，存在ms14-068漏洞，脱网机
- 且A1，A2，B,C系统主机密码均为强口令

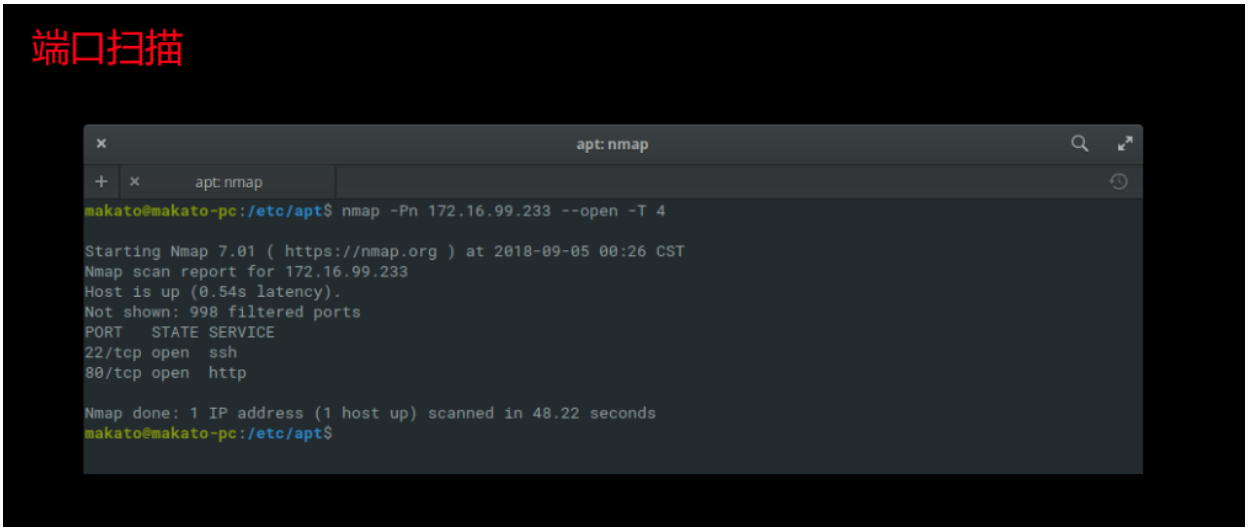
> A1，A2，B,C为标准ABC类网，允许访问流程，A1---->A2---->B---->C，不允许跨主机访问。（请注意每个主机的对应IP段）

整体攻击流程图：



模拟开始攻击：

- 扫描主机A1对攻击机开放端口：80,22



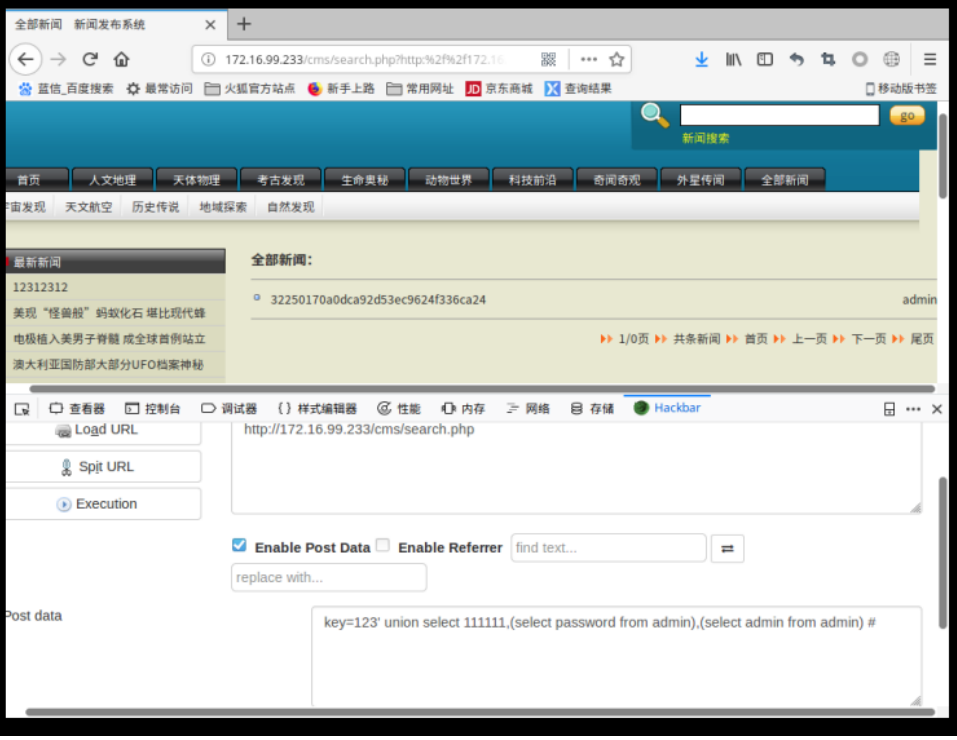
- 扫描主机A1-Web目录结构：

web目录扫描

```
[14:55:12] 200 -   95B  - http://172.16.99.233/INSTALL.txt
[14:55:12] 200 -   18KB - http://172.16.99.233/LICENSE.txt
[14:55:17] 403 -  210B  - http://172.16.99.233/cgi-bin/
[14:55:17] 301 -  233B  - http://172.16.99.233/cms  ->  http://172.16.99.233/cms/
[14:55:17] 200 -    3KB - http://172.16.99.233/composer.json
[14:55:17] 200 -  160KB - http://172.16.99.233/composer.lock
[14:55:18] 200 -    3KB - http://172.16.99.233/cms/
[14:55:18] 301 -  234B  - http://172.16.99.233/core  ->  http://172.16.99.233/core/
[14:55:21] 301 -  236B  - http://172.16.99.233/manual  ->  http://172.16.99.233/manual/
[14:55:21] 200 -    9KB - http://172.16.99.233/manual/index.html
[14:55:22] 301 -  237B  - http://172.16.99.233/modules  ->  http://172.16.99.233/modules/
[14:55:24] 403 -  211B  - http://172.16.99.233/php5.fcgi
[14:55:25] 301 -  238B  - http://172.16.99.233/profiles  ->  http://172.16.99.233/profiles/
[14:55:26] 200 -    2KB - http://172.16.99.233/robots.txt
[14:55:27] 301 -  235B  - http://172.16.99.233/sites  ->  http://172.16.99.233/sites/
[14:55:28] 301 -  236B  - http://172.16.99.233/themes  ->  http://172.16.99.233/themes/
[14:55:29] 200 -    4KB - http://172.16.99.233/web.config
[14:55:29] 301 -  233B  - http://172.16.99.233/cms  ->  http://172.16.99.233/cms/
[14:55:30] 400 -  226B  - http://172.16.99.233etc/passwd
[14:55:30] 400 -  226B  - http://172.16.99.233etc/sysconfig/network-scripts/ifcfg-eth1
[14:55:30] 400 -  226B  - http://172.16.99.233etc/passwd
[14:55:30] 400 -  226B  - http://172.16.99.233etc/passwd
[14:55:30] 400 -  226B  - http://172.16.99.233etc/hosts
[14:55:30] 200 -    9KB - http://172.16.99.233/index.php
[14:55:31] 200 -    2KB - http://172.16.99.233/robots.txt
```

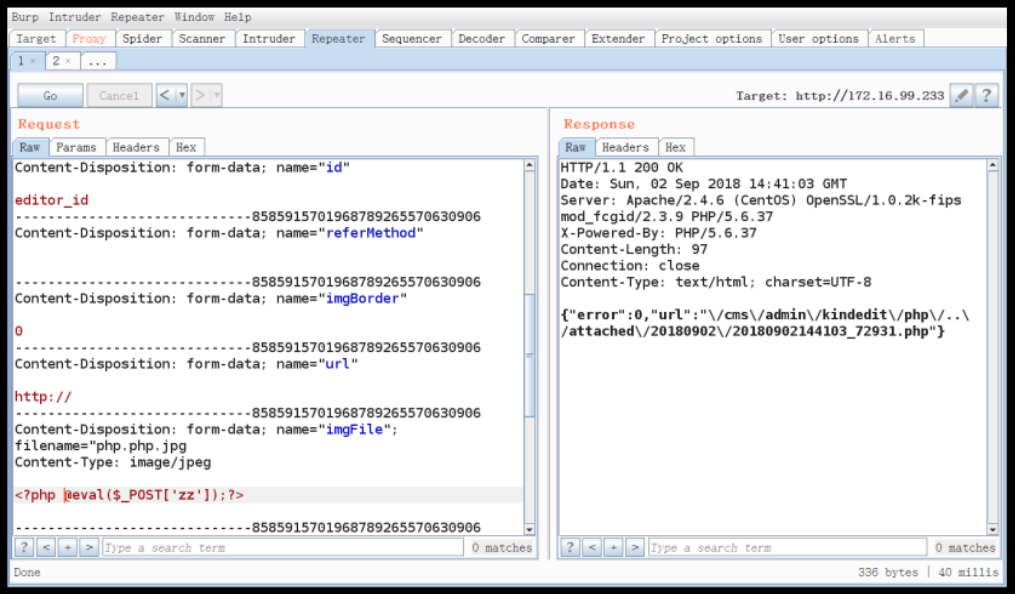
- 主机A1-Web搜索处存在sql注入：

Sql注入



- 登录后台得到shell：

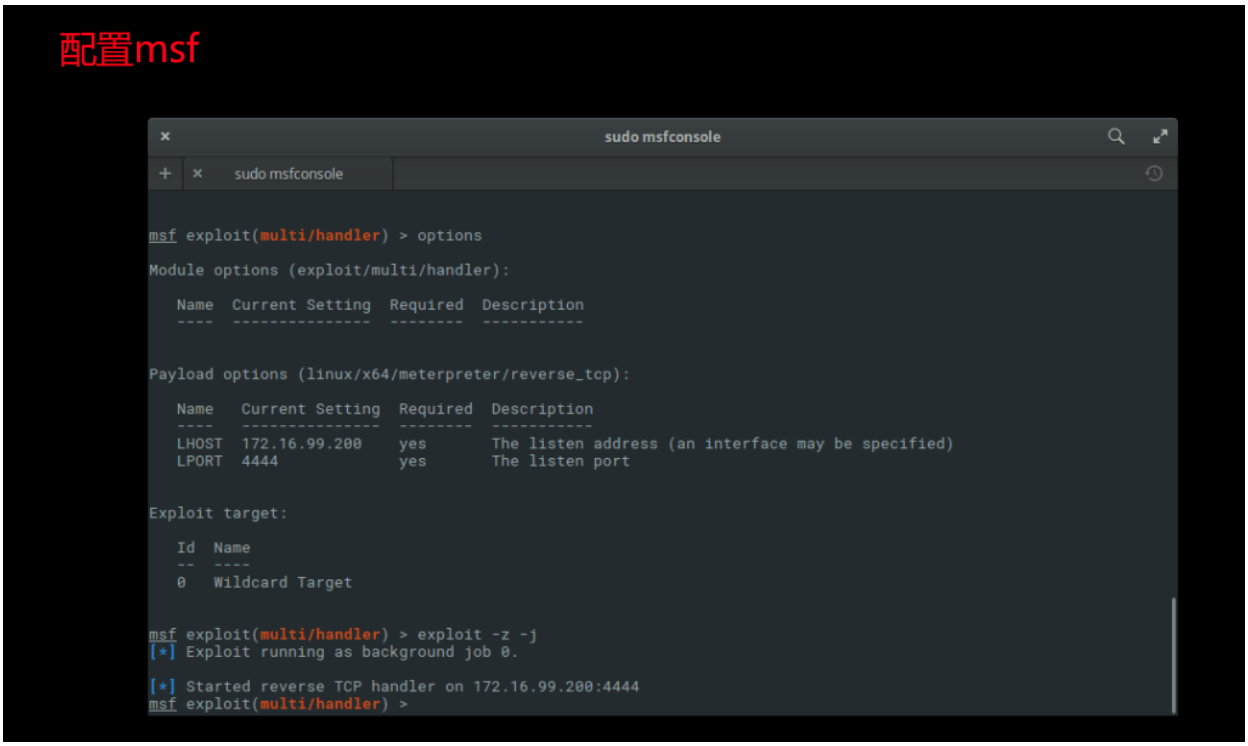
登录后台，上传一句话



- 生成tcp payload 以php一句话执行：

生成msf payload

配置msf

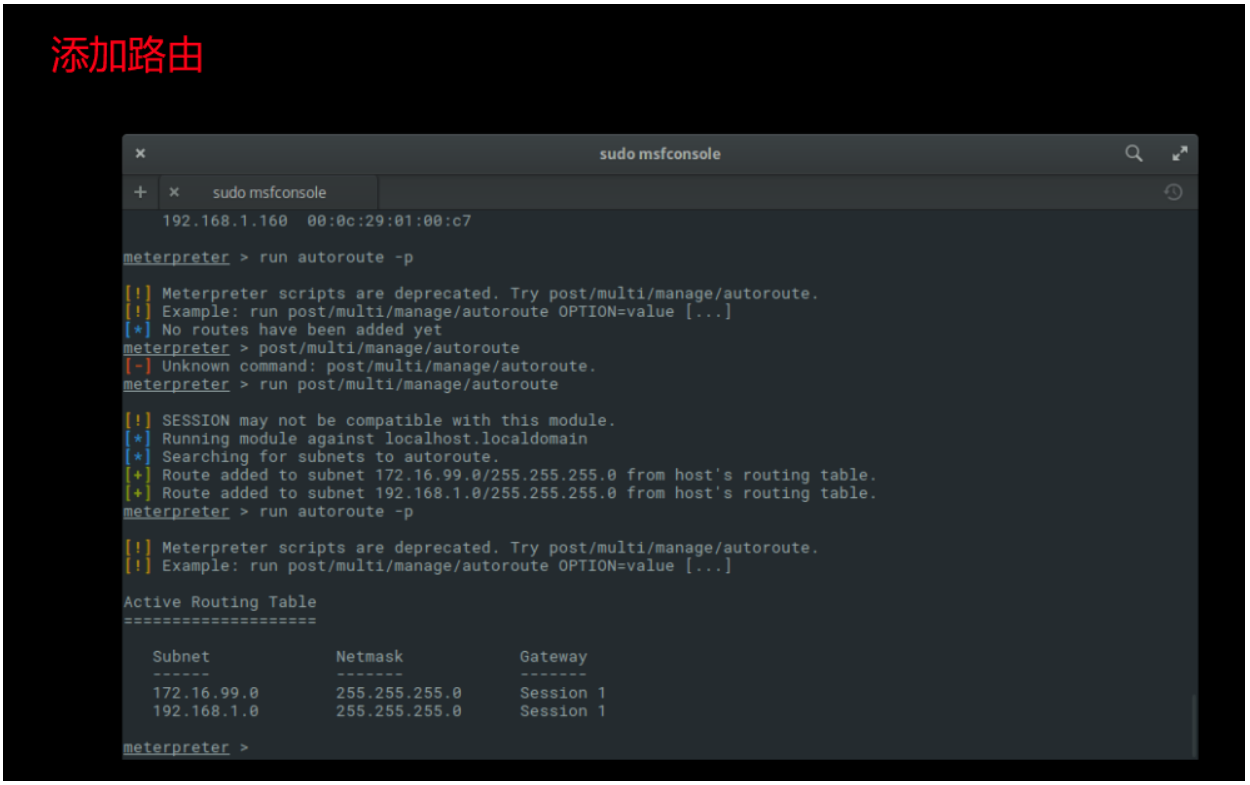


- A1对内信息搜集发现A2，并且针对A1，没有可用提权漏洞（Web非root权限），放弃提权：

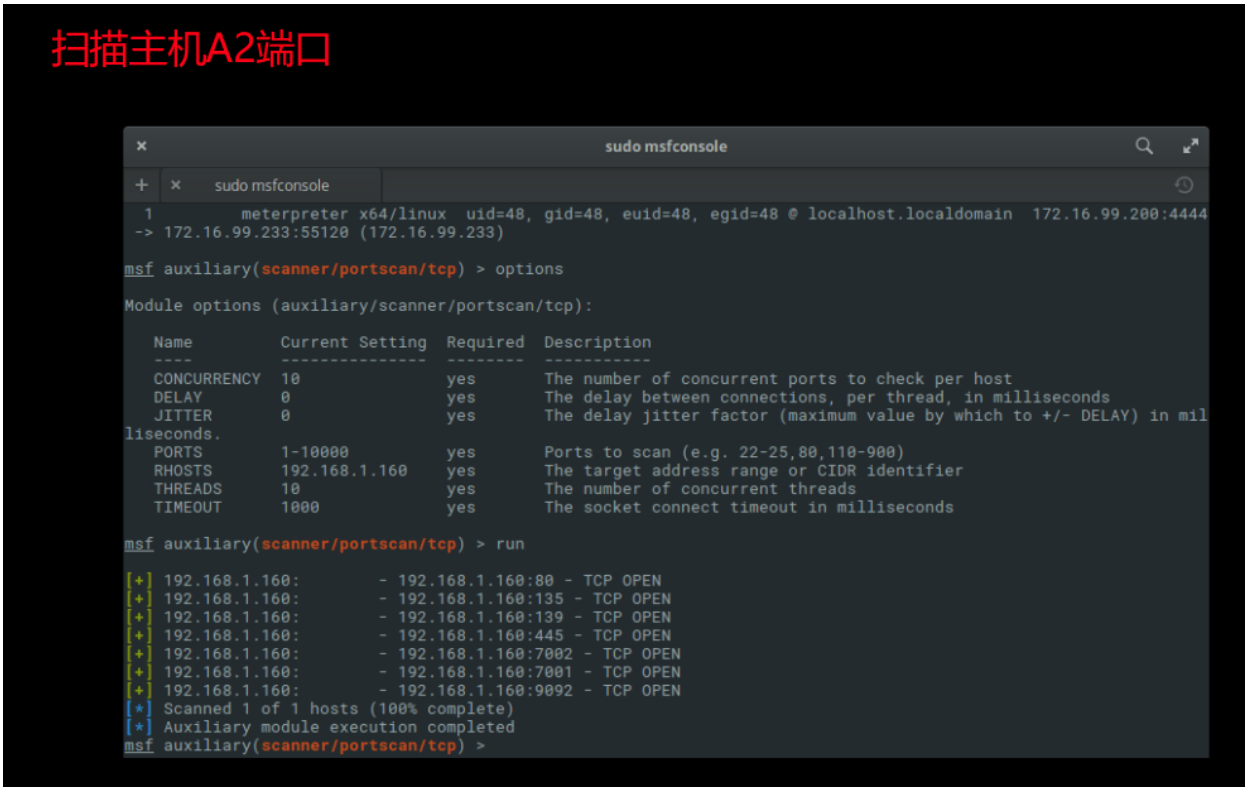
查看arp，发现内网其他主机A2

- 以A1作为跳板添加虚拟路由，并且开始做针对A2的对内信息搜集：

添加路由

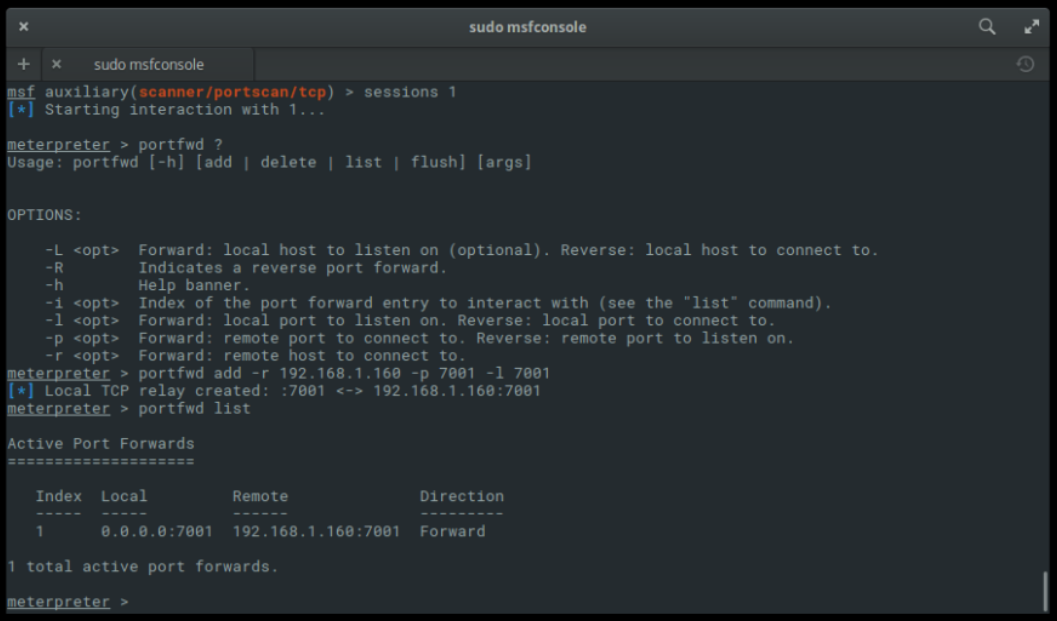


扫描主机A2端口

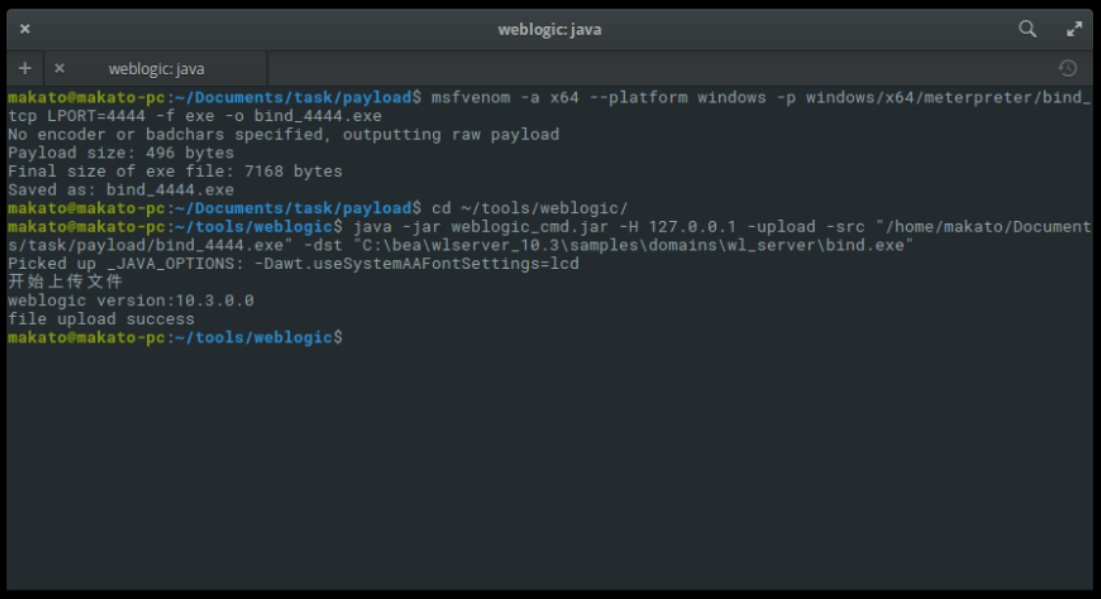


- 以A1跳板发现A2部署weblogic，并且存在漏洞。转发目标机7001至本地，利用漏洞。

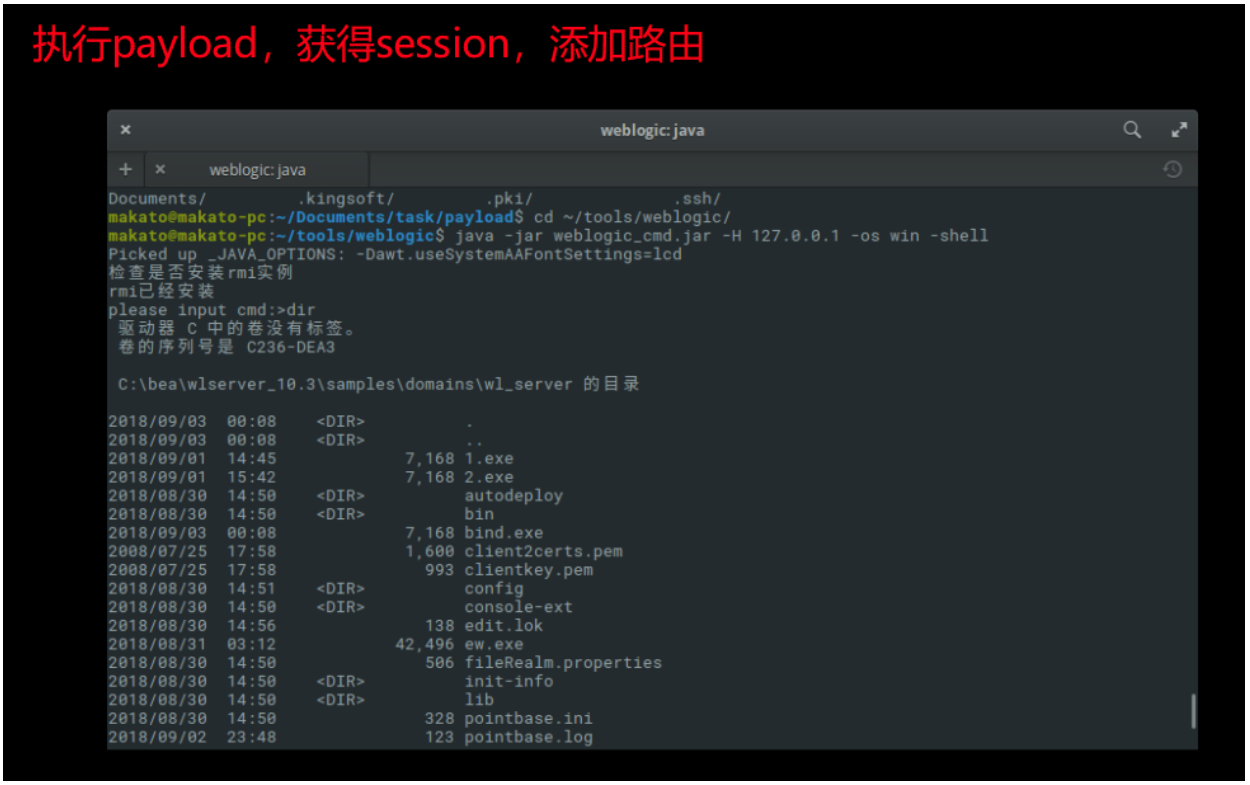
端口转发



生成payload并尝试Weblogic漏洞上传

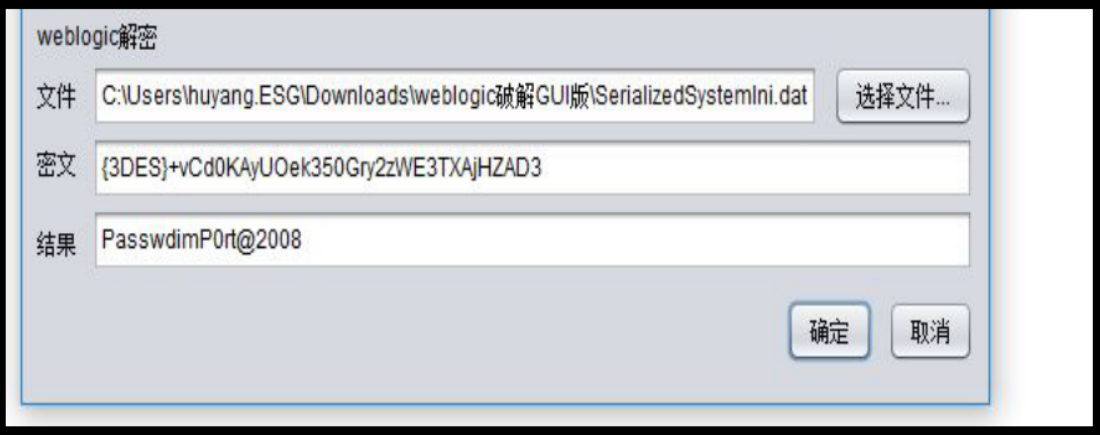


执行payload，获得session，添加路由



- 发现A2全补丁，放弃提权，（weblogic为user权限）对内信息刺探A2，得到weblogic相关配置文件，解密后，得到密码。

破解weblogic登录密码



- 尝试做二级跳板，以weblogic相关配置，尝试对B（域内成员）的渗透（SMB）

尝试使用weblogic用户密码登录主机B

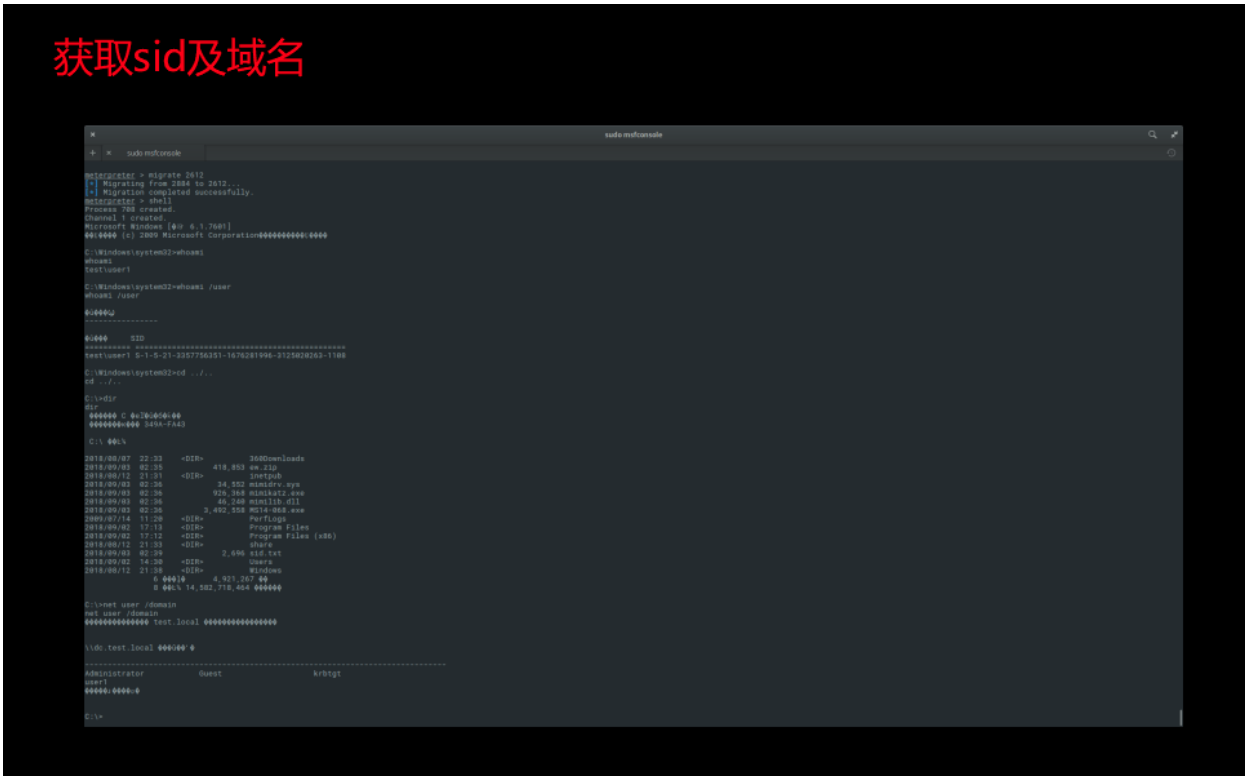
- 获取B权限（system），尝试对内B的本身信息搜集，发现域账号（普通成员）user1.

抓取主机B的账号密码，发现域账号user1

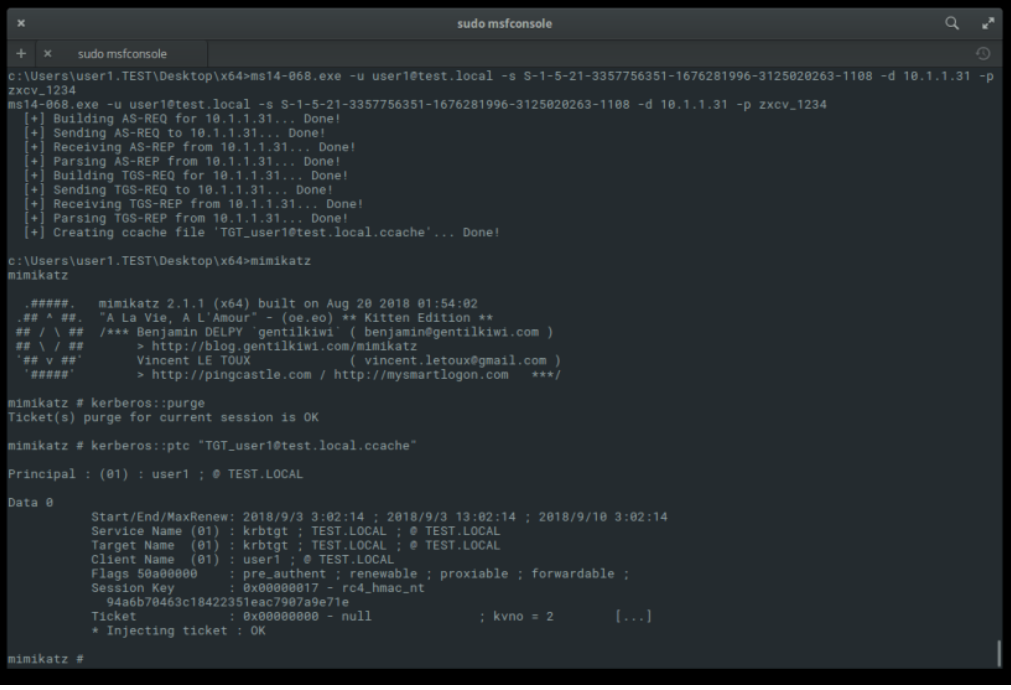
引言（2）：

渗透测试过程，提权是非核心任务，这里也不建议尝试提权，因为在实战过程中获取某个“点”的权限，过程是及其漫长以及困难的，不要因为某个大胆的尝试，而影响了整个渗透测试流程。

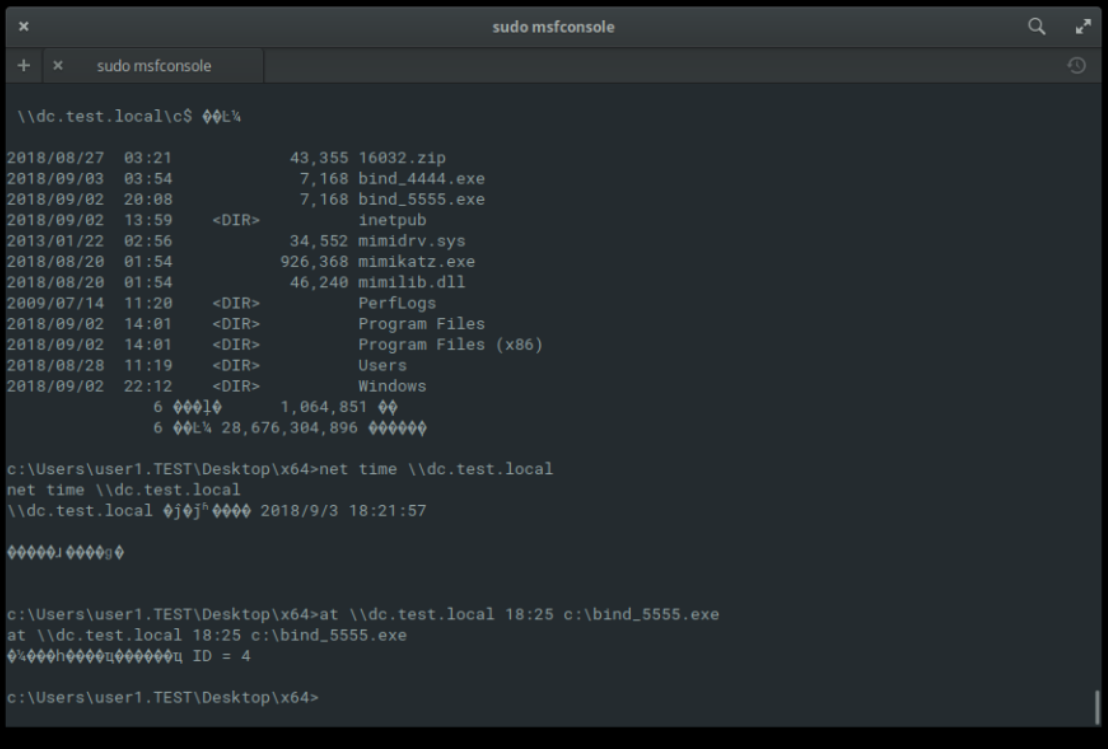
- 尝试三级跳板，尝试获取sid，以及域控对内相关IP，尝试越权，获取域控权限。

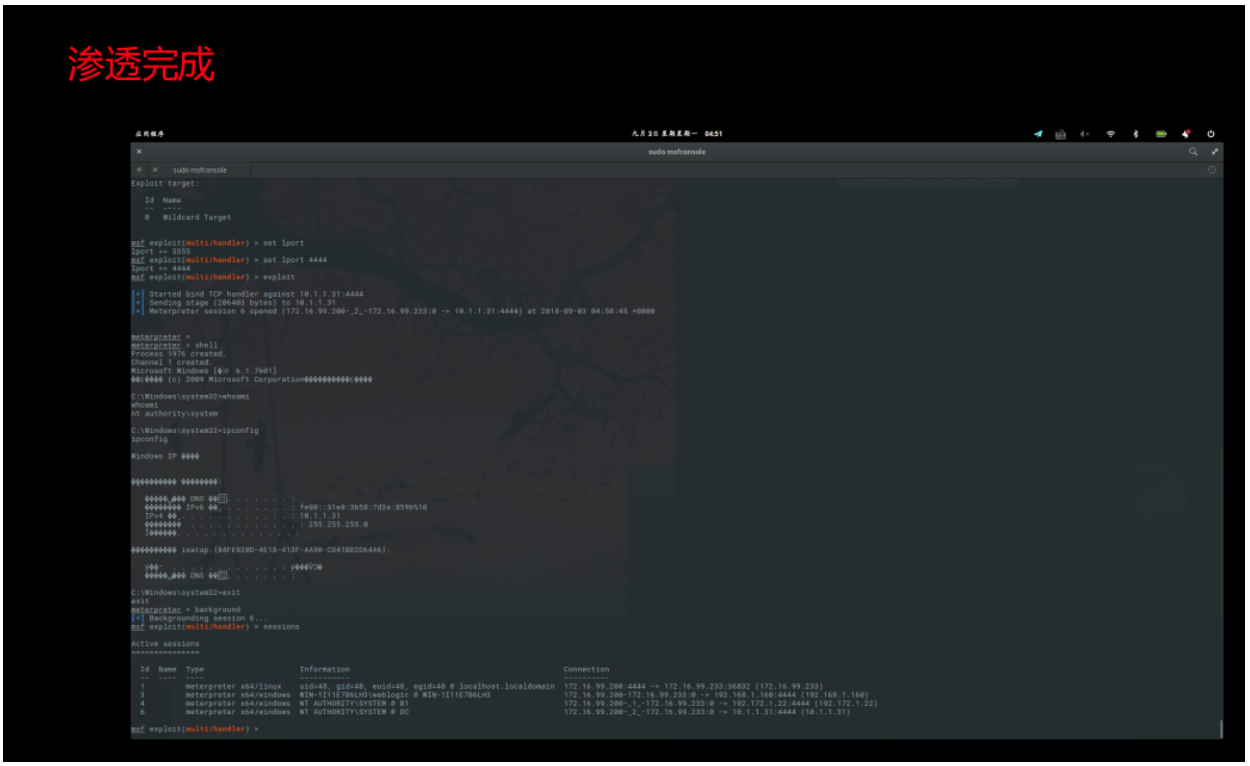


利用user1生成票据并注入内存



查看C主机时间，at执行命令





并没有结束：

在得到域控后，对主机C对内信息搜集，得到域控administrator密码，尝试用该密码ssh--->A1，成功，root权限。

广告（你需要背下来的广告词）：只要是“一个人”设置的密码“群”，一定有大的规律，只要是“一个行业”设置的密码“群”一定有规律可寻。

引言（4）：

渗透的本质是信息搜集，而要把信息搜集发挥最大效果，一定是离不开“线索关联”，而信息搜集，无论是对内，对外，更或者是主动信息搜集，被动信息搜集。如何把目标A与B的信息搜集，整理后做“线索关联”是一个非常有趣的工作。

后者的话：

APT攻击三大要素，既：

- **攻击手段复杂，持续时间长，高危害性**

APT攻击主要分类为两大类，既：

- **高级持续渗透 ， 即时渗透**

3.1 APT攻击的概念

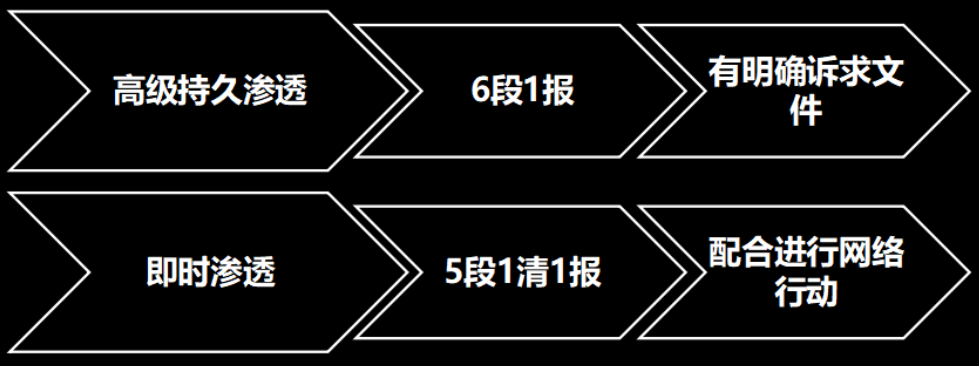
高级持续性威胁（英文缩写APT），既攻击手段复杂（Advanced）、持续时间长（Persistent）、高危害性（Threat）。APT是黑客以窃取目标数据或文件为目的，并且该数据具有“涉我”属性。针对目标所发动的网络行动是一种有组织。有规划，并且是蓄谋已久的恶意网络间谍行为。这种行为往往经过长期的经营与策划，并具备高度的隐蔽性，针对性，长期，有计划性和组织性地窃取“涉我”数据或文件。而APT攻击，又往往伴随着传统的人力情报分析。

注：“涉我”这里指目标数据或文件与攻击者有关联或特殊用途，攻击者可用该数据或文件产生价值。

3.2 APT攻击的手法

APT的攻击手法复杂且多样性，并随着目标发生变化而改变攻击行动计划。

（如：目标工作人员作息改变，地域时差等）



3.3 APT攻击的流程

高级持续渗透攻击

在高级持续渗透测试中，基本符合PTES的渗透测试执行标准，主要分为6段1报。既：

- 高级持续渗透攻击
  - 前期交互阶段
  - 情报收集阶段
  - 威胁建模阶段
  - 漏洞分析阶段
  - 渗透攻击阶段
  - 后渗透攻击阶段
  - 报告编写

3.3 APT攻击的流程

即时针对渗透攻击

在即时目标渗透测试中，主要分为5段1清1报。既：

- 即时目标渗透攻击
  - 前期交互阶段
  - 情报收集阶段
  - 威胁建模阶段
  - 漏洞分析阶段
  - 渗透攻击阶段
  - 清理攻击痕迹
  - 报告编写

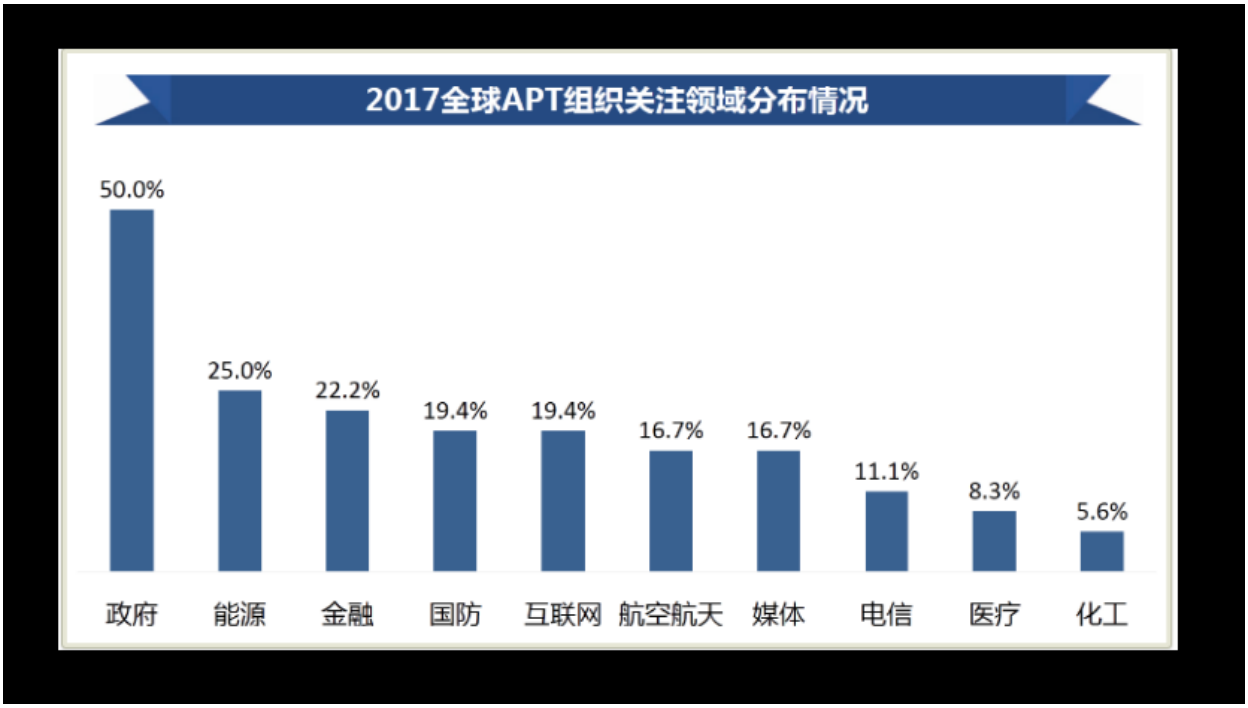
APT两大类攻击核心诉求区别：

3.4 APT攻击的诉求

持久渗透以时间换空间为核心的渗透，以最小化被发现，长期把控权限为主的渗透测试。

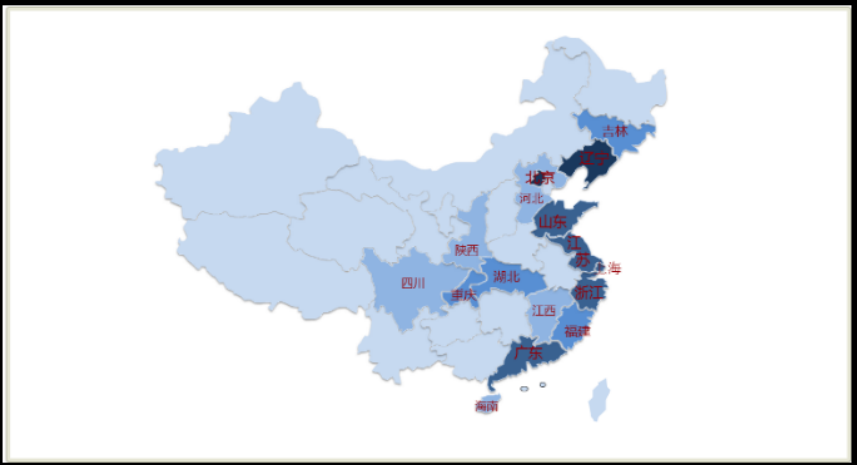
即时目标渗透则相反，放大已知条件，关联已知线索，来快速入侵，以达到诉求。

在做调研之前，作者一直以为越发达的城市，或者越政治中心的城市是发生攻击的高发地，但是在调研后，打破了我之前的想法，于是作者深入调研原因究竟，以便更好的了解企业安全建设的规划。



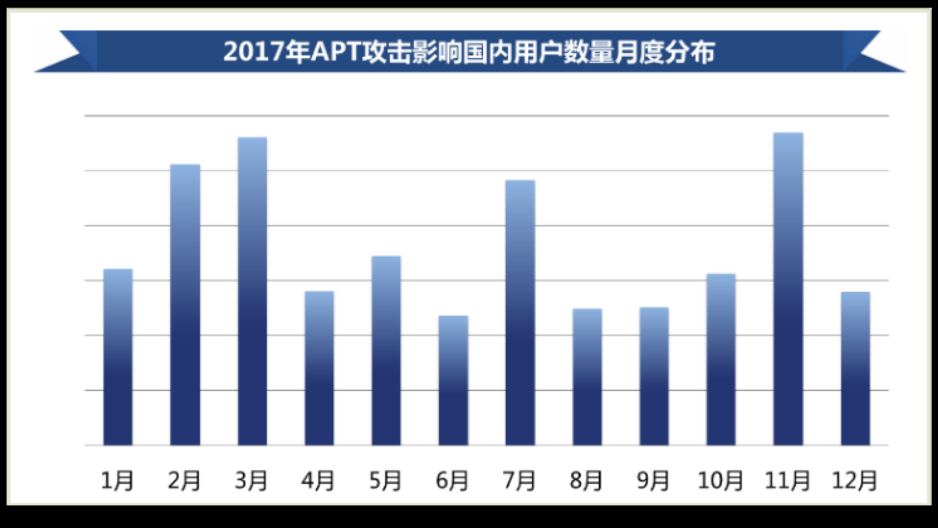
3.5 APT攻击的对象

根据第三方的统计显示（不含港澳台地区）：2017年，国内受APT攻击最多的地区是辽宁和北京，其次是山东、江苏、上海、浙江和广东。关于APT攻击在中国境内的分布情况，详见下图（不含港澳台地区）。



3.5 APT攻击的对象

下图给出了2017年以来，APT攻击影响中国境内用户数量的月度分布情况，3月和11月是APT组织比较活跃的两个月份。



在针对政府机构的攻击中，APT组织除了会攻击一般的政府机构外，还有专门针对公检法的攻击。

在针对能源行业的攻击中，APT组织重点关注的领域依次是：石油、天然气和核能。针对能源行业的攻击，对国家安全具有很大的影响。

在针对金融行业的攻击中，APT组织最为关注的是银行，其次是证券、互联网金融等。还有部分APT组织会关注到与虚拟数字货币（如比特币、门罗币等）相关的机构或公司。针对金融机构的攻击大多会利用安全漏洞。针对ATM自动取款机的攻击也一直延续了2016年的活跃状态。

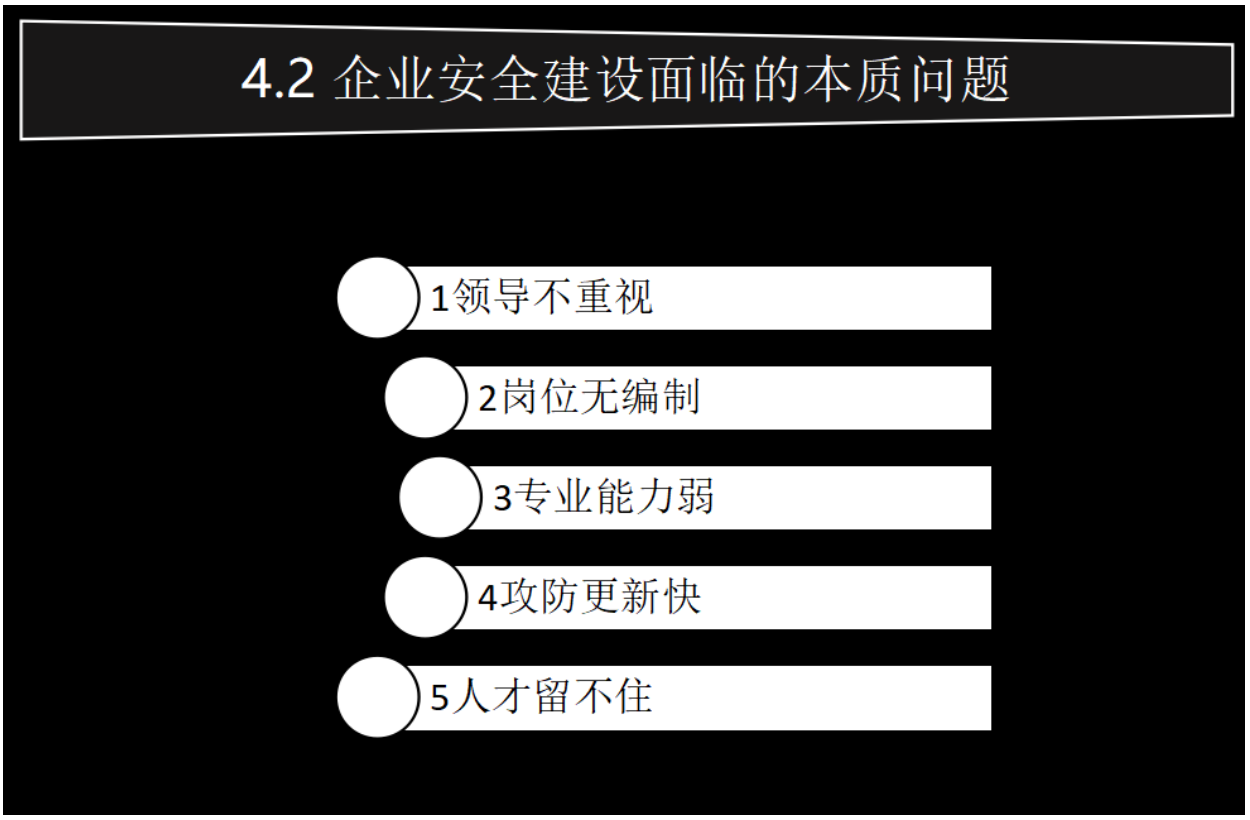
还有一点值得注意：APT组织的攻击虽然具有很强的针对性，但其攻击目标也并不一定是单一的。有的APT组织只攻击特定国家特定领域的目标（仅从目前已经披露的情况看），但也有很多APT组织会对多个国家的不同领域目标展开攻击。上图给出了2017年全球各国研究机构发布的APT研究报告中，披露APT组织攻击目标的所属国家、领域数量分析。

引言（5）：

目前市场上的企业网络安全规划与建设大部分存在统一实施方案，或者是模板方案。而非针对特定行业，特定客户群体来制定针对方案。而不同行业，不同背景的企业安全规划方案也一定是不相同的。如传统行业（医药，食品，汽车）对待企业安全的建设是起跑阶段。如金融行业（证券，银行，保险）对待企业安全的建设是规划与实施阶段。如互联网行业（某度，某巴，某鹅）对待企业安全建设是自研或商业化阶段。为了更好的了解，所以如上制图，更能清楚的看到，未来企业网络安全对待企业发展的重要性，以及特定行业特定规划方案，特定行业特定防御对象。如某X企业安全预算为100万，是否应该针对该企业，行业，地理位置，做防御预算倾斜，并且留有10%-15%的资金量做2月，3月，11月攻击高发期的预案资金等。

总结：

由于信息化，自动化的办公，企业成本的考虑，传统的“以点打面”的点会越来越分散与难以集中管理，如跨国办公，移动办公等。那么可预知的攻击方式将会以人为突破口的事越来越多。安全的本质又不能仅仅靠预算与设备的投入而杜绝，尤其是在未来的大型甲方公司，都会有着自己的安全团队，那么如何把网络安全发展成未来甲方公司的企业文化，将会是一个漫长的过程。而近些年无论是国内还是国外的官方部门开始重视网络安全，但是效果不明显，这里做一个总结，同样部分也适用于企业：



- Micropoor