网络对抗原理与技术

——课程介绍

尹钰　yinyu@xidian.edu.cn

关于我

一直在干一件事

2003-2010 西电 - 信息安全

2010-2012 阿里巴巴

2013-2014 艺龙

2015-2016 豌豆荚

2017- ? @# ￥ #% ￥ @

关于这门课

沉淀、实践、探索

必修 => 选修
40 => 20
16 => 24

网络安全

对抗

原理与技术

都讲些什么

网络对抗原理与技术

安全时事分析（2）

方法论 与 体系规划 （2）

网络攻击技术（6）

网络防御体系及其组件（10）

实验（24）

展开点说

网络攻击技术

漏洞原理与利用

渗透路径

扫描与嗅探

拒绝服务攻击

展开点说

网络防御体系

网络安全域划分与隔离

网络准入

认证、授权、审计

入侵检测技术

应用安全对抗

业务安全对抗

合作与产业化

展开点说

实验

漏洞

攻击

AAA

IDS / WAF

成绩

客观、真实

平时成绩	15%
实验	30%
考试	55%

情景画面

反常规、不对称

对手：黑客精英 ✗

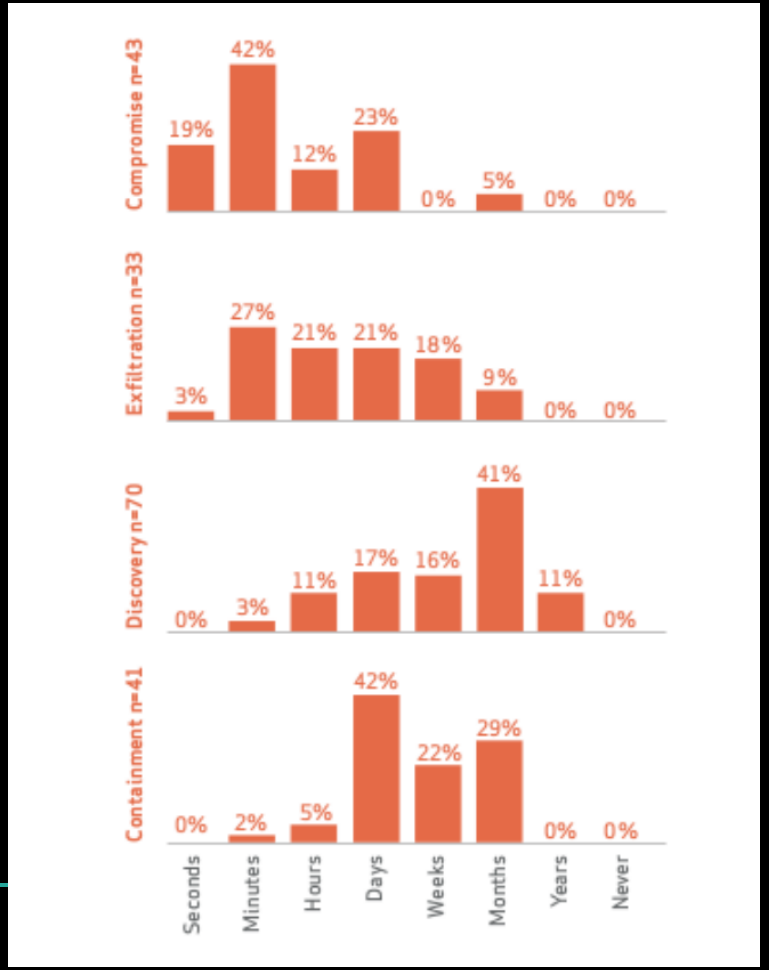
我方：严阵以待 ✗

形式：两军对垒 ✗

比拼：技术、灵感、资源 ✗

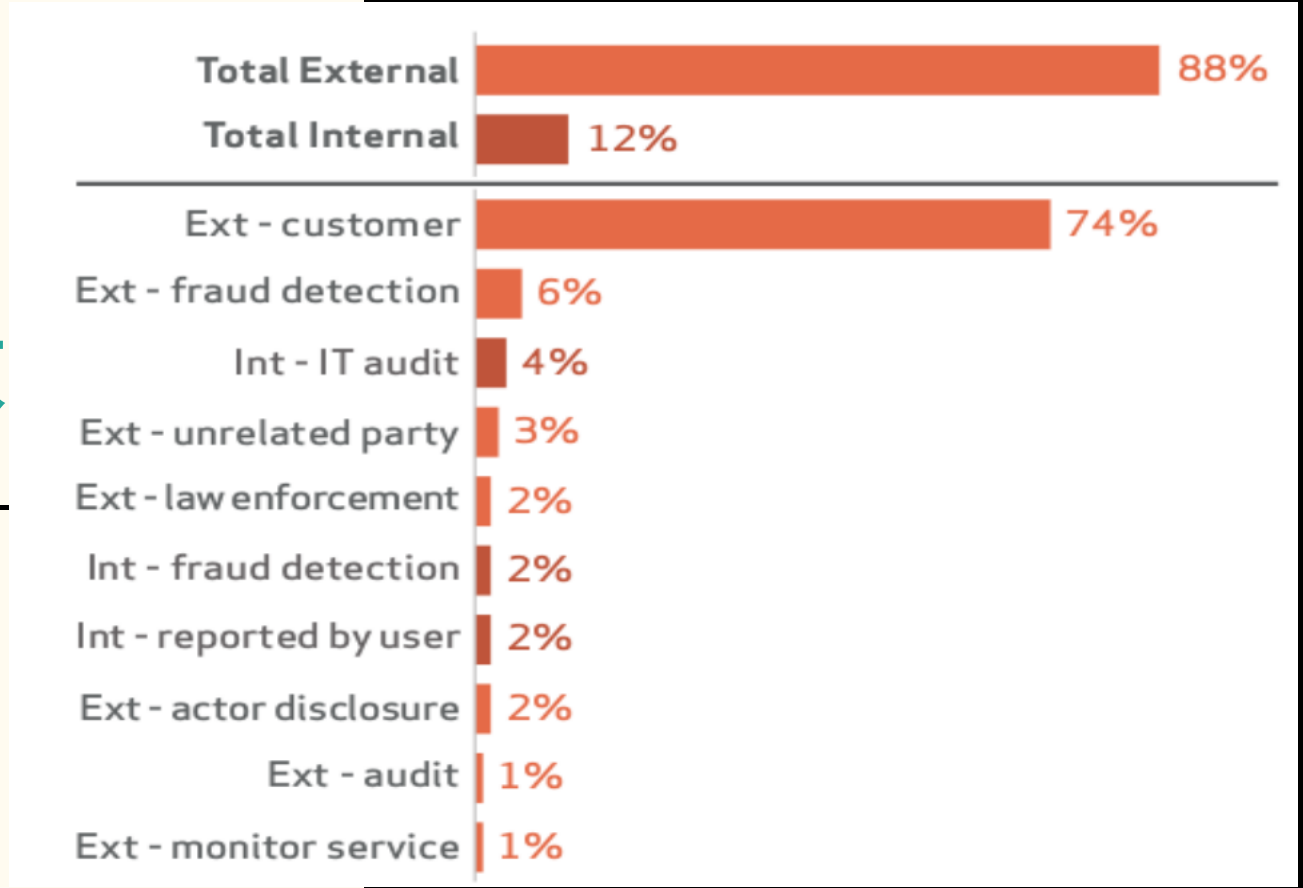
现 状

和想象的不太一样

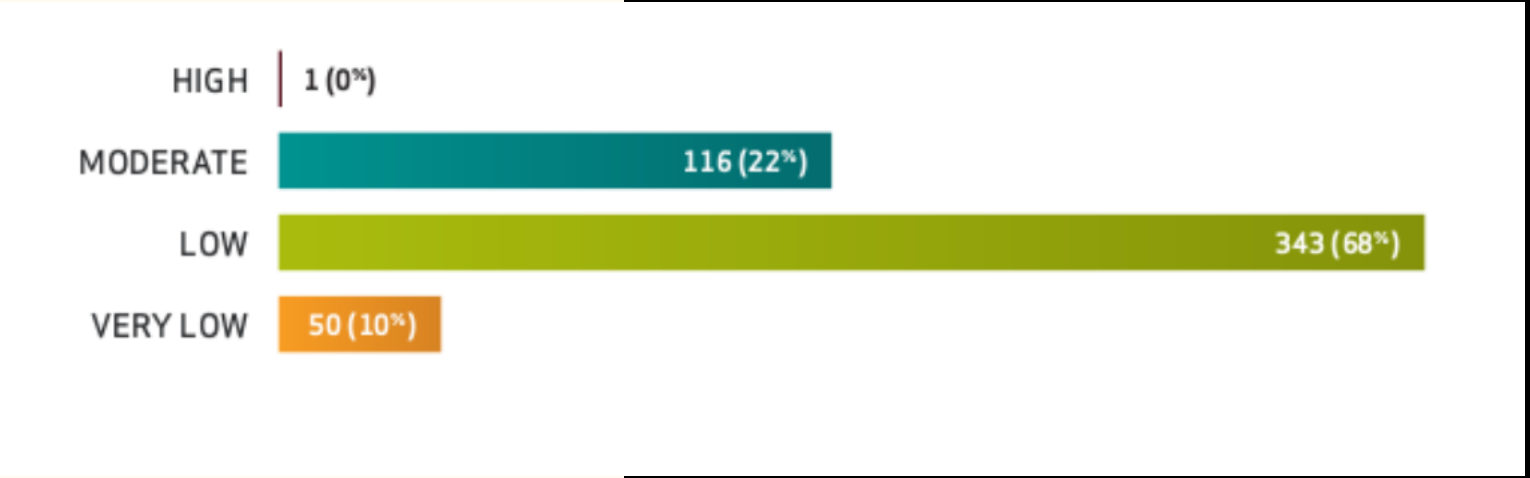

Compromise n=43
19%
42%
12%
23%
0%
5%
0%
0%
Exfiltration n=33
3%
27%
21%
21%
18%
9%
0%
0%
Discovery n=70
0%
3%
11%
17%
16%
41%
11%
0%
Containment n=41
0%
2%
5%
42%
22%
29%
0%
0%
Seconds
Minutes
Hours
Days
Weeks
Months
Years
Never

现 状

和想象的不太-


Total External
88%
Total Internal
12%
Ext - customer
74%
Ext - fraud detection
6%
Int - IT audit
4%
Ext - unrelated party
3%
Ext - law enforcement
2%
Int - fraud detection
2%
Int - reported by user
2%
Ext - actor disclosure
2%
Ext - audit
1%
Ext - monitor service
1%

和杰



对抗思路

不对称

攻——尖、刁、准、快、藏

侦察　　漏洞

工具　　缺陷

路径　　持久化

防——严、密、序、厚、敏

发现　　处置

引导　　规范

两个概念

经常被弄混

弱点

- 漏洞
- 配置不当
- 设计缺陷

攻击

- 扫描
- 渗透
- DDoS/Anti-DDoS

漏洞挖掘

SDL

ACL

入侵检测

应急响应

Q & A