



领先的网络安全人才培养平台

北京益安在线科技股份有限公司

Beijing E' An Online Technology Co.,Ltd.

主讲人

Beijing E' An Online Technology Co.,Ltd.

- **Jason(杰森)**

- 10年以上的网络安全从业经验，曾在北京多家大型上市公司，担任项目总监，北京某高校任信安专业学科带头人。

- 部分项目：

- 《华北油田数据加密》方案与实施
- 中国农业银行网银《漏洞检测与信息传输加解密》项目
- 中国工商银行北京分行《市级财政授权支付》项目
- 北京信息科技大学《网络安全建设》项目
- 北京警种学院《网络安全规划与建设》项目

- 高校项目：

- 国内重点高校**师资培训**与大四和研究生就业前**网络安全项目实训**，学生就职于启明、网康、绿盟、360、西普、联想、大唐等主流安全厂商和安全服务公司;

- 研究方向：

- 网络协议安全、系统安全及WEB安全，软硬件防护设备、服务器入侵与防护、计算机取证、追踪溯源技术、熟悉风险评估及等级保护体系。



揭秘黑客常用入侵工具与思路

WEB安全为例

- 1、信息收集 50%时间
- 2、漏洞挖掘
- 3、漏洞利用
- 4、上传木马
- 5、维持访问

信息收集

Beijing E' An Online Technology Co.,Ltd.

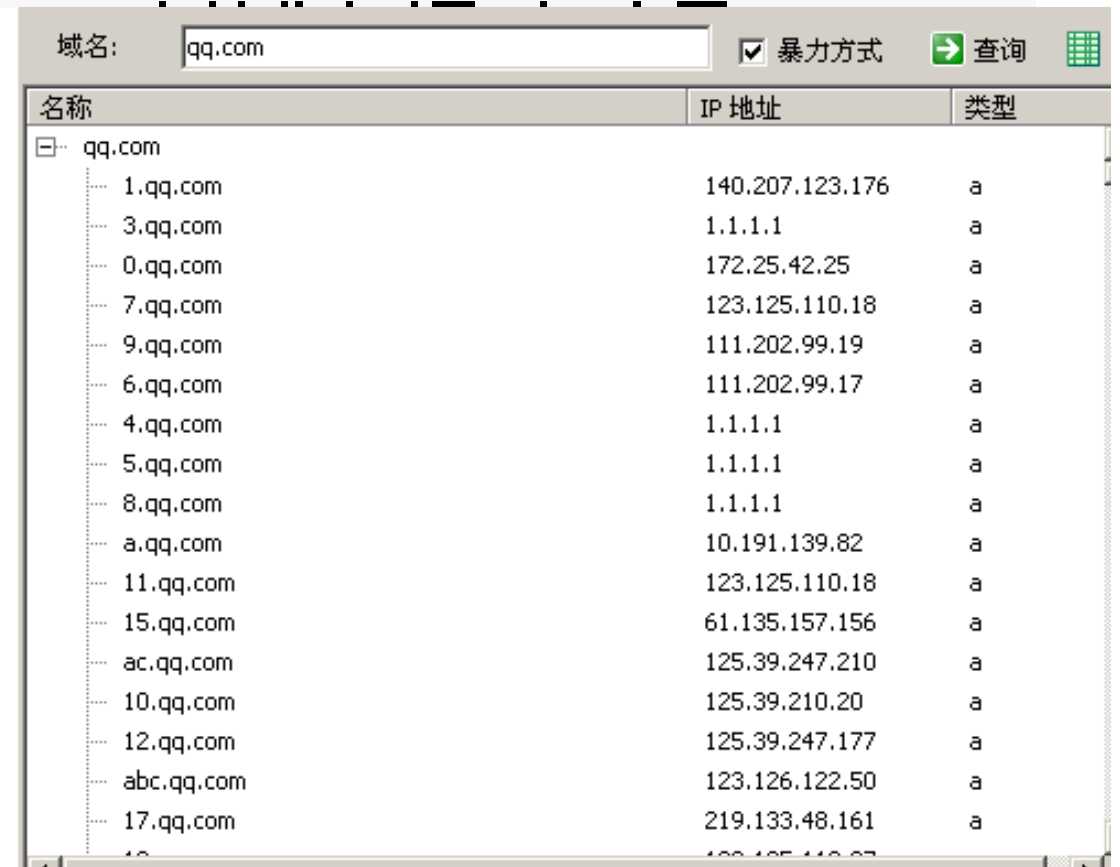
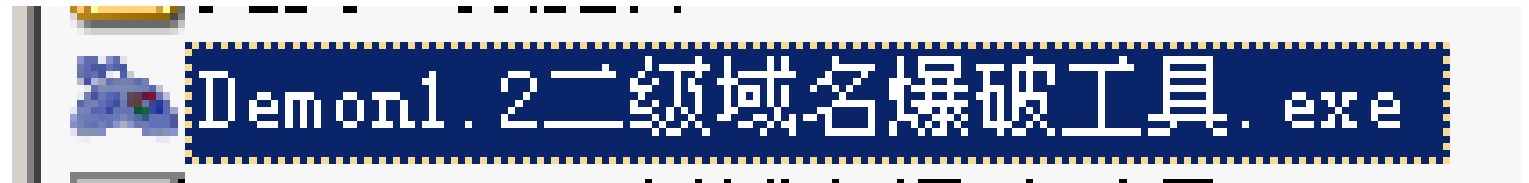
- whois收集域名信息：
 - 网站注册人、联系人、电话、邮箱、手机等
- 站长之家 <http://whois.chinaz.com>、kali
- 获取IP地址（可能有多个）
 - 真实IP可通过 子域名解析 邮件服务器IP
 - nslookup、ping、<http://ping.chinaz.com>
 - 奇云测<http://ce.cloud.360.cn/>

whois演示：hc3333.com
端口扫描：qs68.com

信息收集

Beijing E' An Online Technology Co.,Ltd.

- 子域名爆破
- 在线子域名爆破
 - <https://phpinfo.me/domain/>



开放端口

Beijing E' An Online Technology Co.,Ltd.

- <http://tool.chinaz.com/port/>
 - qs68.com

端口扫描：
qs68.com



tool.chinaz.com/port/

站长之家 站长论坛 站长工具 站长素材 源码下载 网站排行 手机版 工具旧版 SEO工具包

China7.com
tool.chinaz.com | 站长工具

快云 快云7个月上云体验
云服务器买一送一

谋盾★无视一切大型攻击★可测证
关键词排名【1-7天上前3名】
永久免费的游戏盾，无视攻击

首页 域名/IP类 网站信息查询 SEO查询 权重查询

香港美国双线高防
多层物理安全/秒开黑科技

百万现金 诚邀技术团队加盟合作！
收购网站、域名！ QQ: 738519386

当前位置：站长工具 > 端口扫描

广告 快快网络-专家级高防安全品牌

80,8080,3128,8081,9080,1080,21,23,443,69,22,25,110,7001,9090,3389,1521,1158,2100,1433

多个端口号请用逗号隔开，例：8080,8081

开始扫描

服务+版本NMAP高级用法

Beijing E' An Online Technology Co.,Ltd.

- nmap qs68.com
- 在线NMAP
 - <http://www.webscan.cc/>

```

Initiating Parallel DNS resolution of 2 hosts. at 16:01
Completed Parallel DNS resolution of 2 hosts. at 16:01, 0.00s elapsed
NSE: Script scanning 67.198.156.48.
Initiating NSE at 16:01
Completed NSE at 16:06, 290.41s elapsed
Initiating NSE at 16:06
Completed NSE at 16:06, 0.00s elapsed
Nmap scan report for qs68.com (67.198.156.48)
Host is up (0.18s latency).
rDNS record for 67.198.156.48: 67.198.156.48.static.krypt.com
Not shown: 991 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          Microsoft ftpd
|_sslv2-drown:
80/tcp    open  http         Microsoft IIS httpd
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-iis-webdav-vuln: WebDAV is DISABLED. Server is not currently vulnerab
|_http-server-header: Microsoft-IIS/6.0
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
514/tcp   filtered shell
1025/tcp  open  msrpc        Microsoft Windows RPC
1030/tcp  open  msrpc        Microsoft Windows RPC
4444/tcp  filtered krb524
Device type: general purpose
Running: Microsoft Windows XP|7|2012
OS CPE: cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_7 cpe:/o:m
OS details: Microsoft Windows XP SP3, Microsoft Windows XP SP3 or Windows /
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=262 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE (using port 80/tcp)
    
```

爆破

Beijing E' An Online Technology Co.,Ltd.

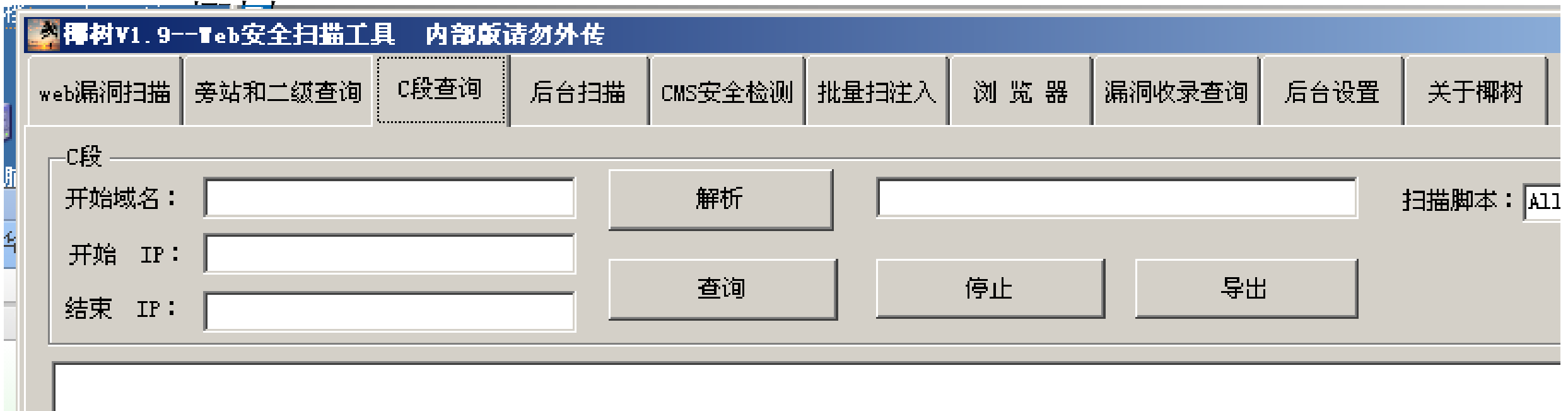
敏感端口21可做爆破 Hydra 九头蛇
系统口令爆破
数据库爆破



旁站、C段

Beijing E' An Online Technology Co.,Ltd.

- 在线工具
- <http://www.webscan.cc/>



扫描工具

Beijing E' An Online Technology Co.,Ltd.

awvs, appscan, burp, 御剑, 破壳, 椰树, safe3wvs,
wwwscan

- 注入工具：啊D, 明小子, 穿山甲, 萝卜头, sqlmap, NBIS
- 端口扫描工具：尖刀端口扫描, nmap, zenmap

Sqlmap使用命令

Beijing E' An Online Technology Co.,Ltd.

- --tables //猜数据库
- --columns //-T表名
- --dump -T //表名 -C"账号, 密码"
- --dump-all //列所有表的内容
- --current-user //查看当前用户
- --dbs //猜数据库
- --D 表名 -tables
- --D 表名 -T列名 -columns //

WEB渗透相关工具

Beijing E' An Online Technology Co.,Ltd.

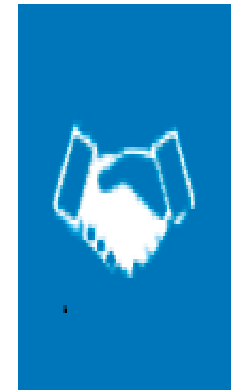
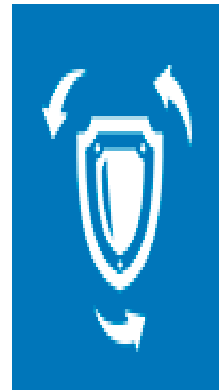
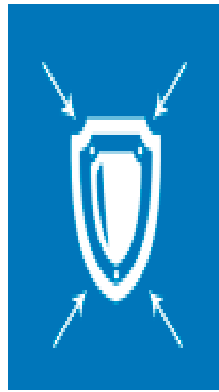
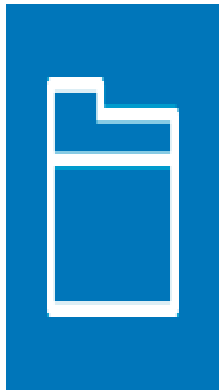
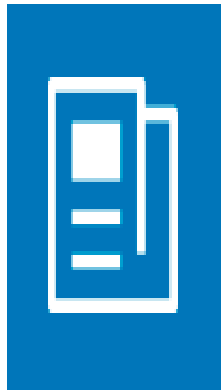
- AWVS、sqlmap、Burp、nessus、Appscan等相关工具的使用
- 目标：了解该类工具的用途和使用场景

网络大咖中级-快速掌握渗透技能

说明	工具名称	工具简介
协议安全	cain	ARP欺骗、中间人攻击、DNS欺骗、明文密码嗅探等
	阿拉丁UDP攻击器V2.1	UDP洪水攻击 (DOS攻击)
	Wireshark	抓包、嗅探
系统安全	DUBrute 2.2	破解3389神器
	hydra-8.1-windows版本	爆破神器支持多种协议
	nmap	扫描与漏洞审计
	Scanport	扫描端口
	lansee	局域网查看
	Ntscan	可破解系统密码
	Xcan	漏洞扫描
病毒与后门查杀	GetHashes	获取Windows用户密码的Hash值
	Gh0st	远控后门
	灰鸽子	远控后门
	蓝茵防火墙压力测试	远控后门&可实现DDOS

病毒与后门查杀	Gh0st	远控后门
	灰鸽子	远控后门
	蓝茵防火墙压力测试	远控后门&可实现DDOS
KALI	arp spopf	ARP欺骗、中间人攻击、DNS欺骗、明文密码嗅探等
	hydra	爆破神器支持多种协议
	MS10-020漏洞利用模块	蓝屏攻击
	MS11-050漏洞利用模块	拿系统SHELL
	MS10-018漏洞利用模块	拿系统SHELL
	MS17-010漏洞利用模块	拿系统SHELL
	Nmap&l漏洞扫描模块	拿系统SHELL
WEB安全	MD5破解	破解
	啊D注入工具	注入
	网页木马	WEBSHELL
	提权	提权
	御剑	WEB扫描

Beijing E' An Online Technology Co.,Ltd.



商务沟通

了解需求，确定测试意向，签订合作合同。
(1-2个工作日)

收集材料

系统账号、稳定的测试环境、业务流程等。
(1个工作日)

模拟攻击

自动化扫描 手动测试
(1-5个工作日)

漏洞校验与复测

对测试发现的漏洞进行验证
(1-3个工作日)

专业安全报告

漏洞基本描述 危险级别
重现方法 网络特征 修复建议.....

项目验收

专家讲解 客户反馈 交付验收报告
(1个工作日)

进入“安全交流圈”

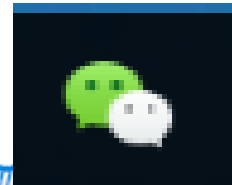
Beijing E' An Online Technology Co.,Ltd.



网络安全专属



公众号



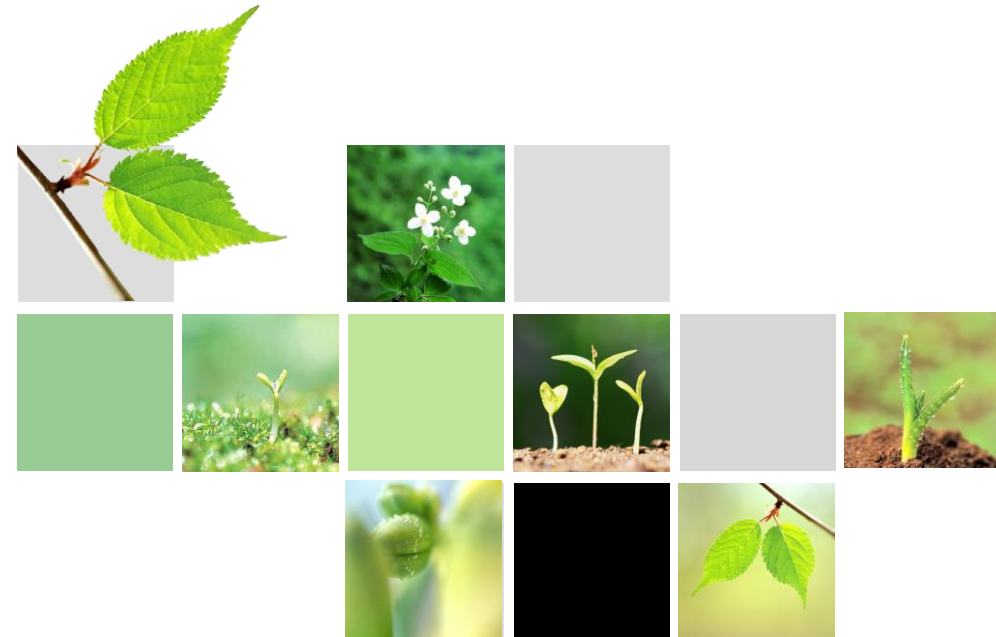
APP

谢谢观看!

Beijing E' An Online Technology Co.,Ltd.

QQ / 微信 : 2708 33442

邮件 : wanggang@51ean.com



更多课程访问 www.51ean.com

The screenshot displays the website's navigation and main content. On the left, a blue sidebar menu is highlighted with a red box and a red arrow pointing to the '学习指南' (Learning Guide) item. The main banner features a Super Mario Bros. theme with the text 'LEVEL 1 GET SECURITY 领你入门' and '网络安全大咖养成记 YOU STARTED'. Below the banner, there are four promotional tiles: '安全意识' (Security Awareness), '等保培训' (Information Security Training), '认证课程' (Certification Courses), and '新人注册' (New User Registration). On the right, there are sections for '近期集训' (Recent Training) and '新闻资讯' (News & Information).

学习指南 菜单项：

- 网络安全
- 安全管理
- 大数据
- 云计算
- 开发技术
- 移动安全
- 工控安全
- DevOps
- 安全意识
- 厂商课

网站导航：首页 | 课程库 | 集训营 | 新手入门 | 职业路径 ^{HOT} | 资讯 | 技术问答 | 合作伙伴

LEVEL 1 GET SECURITY 领你入门
网络安全大咖养成记 YOU STARTED
目标+计划+指导+态度=成功

近期集训

网络安全大咖养成记，火热进行中

新闻资讯

- 信息安全快讯2017年6月第2期
- Linux恶意软件将树莓派设备变成...
- 智能吸管问世，可检测饮料当中是...
- 研究人员发现了某个针对树莓派的...
- 提醒：在朋友圈转发这类信息，最...

安全意识 网络安全大揭秘

等保培训 保障国家信息安全

认证课程 权威认证 官方授权

新人注册 注册领取新人专享大礼包

邀请返利 好友学习，我拿奖金

北京益安在线科技股份有限公司

Beijing E' An Online Technology Co.,Ltd.