内网渗透指南

1. 内网安全检查/渗透介绍

1.1 攻击思路

有2种思路：

攻击外网服务器，获取外网服务器的权限，接着利用入侵成功的外网服务器作为跳板，攻击内网其他服务器，最后获得敏感数据，并将数据传递到攻击者，看情况安装长期后门，实现长期控制和获得敏感数据的方式；

攻击办公网的系统、办公网电脑、办公网无线等方式，一般是采用社工，实现控制办公电脑，再用获得的办公网数据，可能是内网的各种登录账号和密码，再获取办公网或者生产网的有用数据。

一般内网安全检查使用第一种思路，实际的攻击2种思路结合实现。

1.2 敏感资料/数据/信息

高管/系统管理员/财务/人事/业务人员的个人电脑
文件服务器/共享服务器
邮件服务器
OA服务器
数据库服务器

1.3 攻击过程

按照第一种思路，个人认为可以分为4个阶段：

信息收集
漏洞验证/漏洞攻击
后渗透
日志清理

第二种思路，社工的比重更大一些，本篇不多做介绍。

2 信息收集

该阶段识别内网存活的主机 IP， 运行端口扫描和漏洞扫描获取可以利用的漏洞

2.1 主机发现

使用端口扫描工具可以实现主机发现的功能，但也有些动作小的主机发现工具（Kali），可以有效的发现存活主机。自己写个 ping 的循环脚本也可以。

不受限的测试直接端口扫描了。

2.2 端口扫描

有授权的情况下直接使用 nmap 、masscan 等端口扫描工具直接获取开放的端口信息。

作为跳板机可以使用 Metasploit 做端口扫描，也可以在跳板主机上上传端口扫描工具，使用工具扫描。

入侵到服务器上也可以根据服务器的环境使用自定义的端口扫描脚本扫描端口。

python 3 的端口扫描脚本

```
# This script runs on Python 3import socket, threadingdef TCP_connect(ip, port_number, delay, output):
    TCPsock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    TCPsock.setsockopt(socket.SOL_SOCKET, socket.SO_REUSEADDR, 1)
    TCPsock.settimeout(delay)
    try:
        TCPsock.connect((ip, port_number))
        output[port_number] = 'Listening'
    except:
        output[port_number] = ''def scan_ports(host_ip, delay):
    threads = []        # To run TCP_connect concurrently
    output = {}         # For printing purposes
    # Spawning threads to scan ports
    for i in range(10000):
        t = threading.Thread(target=TCP_connect, args=(host_ip, i, delay, output))
        threads.append(t)
    # Starting threads
    for i in range(10000):
        threads[i].start()
    # Locking the script until all threads complete
    for i in range(10000):
        threads[i].join()
    # Printing listening ports from small to large
    for i in range(10000):
        if output[i] == 'Listening':
            print(str(i) + ': ' + output[i])def main():
    host_ip = input("Enter host IP: ")
    delay = int(input("How many seconds the socket is going to wait until timeout: "))
    scan_ports(host_ip, delay)
    if __name__ == "__main__":
    main()

```

有个使用 Python 端口扫描的介绍
https://thief.one/2018/05/17/1/?hmsr=toutiao.io&utm_medium=toutiao.io&utm_source=toutiao.io

Windows 下基于 Powershell 的端口扫描脚本。
https://github.com/BornToBeRoot/PowerShell_IPv4PortScanner/tree/master/Scripts

发现端口后使用客户端连接工具或者 nc 连接，获取服务端的 banner 信息。

2.3 漏洞扫描

有授权的情况下，使用绿盟极光、Nessus、Nexpose 等漏扫工具直接扫描目标，可以直接看到存活主机和主机的漏洞情况。

2.4 识别内网环境

获取目标的主机存活信息和端口开放信息后，就可以尝试分析目标的网络结构，安全防御策略。按照办公网和生产网分别说一下：

2.4.1 办公网

按照系统区分：

OA系统
邮件系统
财务系统
文件共享系统
域控
企业版杀毒系统
上网行为管理系统
内部应用监控系统

按照网络区分：

管理网段
内部系统网段
按照部门区分的网段
按照设备区分：
个人电脑
内网服务器
网络设备
安全设备

办公网的安全防护水平一般较差（相对），能绕过杀毒软件基本上就畅通无阻了，利用信任关系容易扩大攻击面，获取数据也比生产网简单。

2.4.2 生产网

按照系统区分：

业务系统
运维监控系统
安全系统

按照网络区分：

各不同的业务网段
运维监控网段
安全管理网段

根据目标开展的不同业务，对应的服务器可能存在不同的网段上，分析服务器上运行的服务和进程可以推断目标使用的运维监控管理系统和安全防护系统，可以大概推断出入侵目标的 IT 运维水平和安全防护水平，在接下来的入侵考虑采用什么样的方法。

3 漏洞验证/漏洞攻击

使用端口扫描、漏洞扫描验证扫描目标开放的端口，在对应端口上开放的服务，运行该服务的软件和版本号。

如果只是使用端口扫描，只是发现开放的端口，接着使用 nc 可以获取端口上服务的 banner 信息，获取 banner 信息后需要在漏洞库上查找对应 CVE，后面就是验证漏洞是否存在。如果是使用漏洞扫描工具可以直接获取对应端口上的漏洞，后面也是验证漏洞。

安全检查一般是尽可能的发现所有漏洞，对漏洞的风险进行评估和修复。入侵的话只关注高危远程代码执行和敏感信息泄露漏洞等可以直接利用的漏洞。

漏洞验证可以找对应的 CVE 编号的 POC、EXP，利用代码在 ExploitDB 、seebug上查看或者在 github 上搜索是否有相关的漏洞验证或利用的工具。

3.1 Web

3.1.1 自定义 Web 应用

从公网直接攻击目标对外的 Web 应用，或者在授权的情况下在内网进行渗透测试，如果是入侵目的可以直接寻找注入、上传、代码执行、文件包含等高危漏洞，尝试获取系统权限，或者直接能拿到敏感数据。

允许扫描的话一般使用 WVS 直接扫描，也可以使用专门扫描特定漏洞的扫描工具如 sqlmap、XSStrike 等工具扫描特定类型的漏洞。不允许直接扫描，使用 Burp 手工慢慢找了。

3.1.2 Web 中间件

1. Tomcat

Tomcat是Apache Jakarta软件组织的一个子项目，Tomcat是一个JSP/Servlet容器，它是在SUN公司的JSWDK（Java Server Web Development Kit）基础上发展起来的一个JSP和Servlet规范的标准实现，使用Tomcat可以体验JSP和Servlet的最新规范。

端口号：8080

攻击方法：

默认口令、弱口令，爆破，tomcat5 默认有两个角色：tomcat和role1。其中账号both、tomcat、role1的默认密码都是tomcat。弱口令一般存在5以下的版本中。

在管理后台部署 war 后门文件

远程代码执行漏洞

参考：

https://paper.seebug.org/399/

http://www.freebuf.com/column/159200.html

http://liehu.tass.com.cn/archives/836

http://www.mottoin.com/87173.html

2. Jboss

Jboss 是一个运行 EJB 的 J2EE 应用服务器。它是开放源代码的项目，遵循最新的J2EE规范。从JBoss项目开始至今，它已经从一个EJB容器发展成为一个基于的 J2EE 的一个

Web 操作系统（operating system for web），它体现了 J2EE 规范中最新的技术。

端口：8080

攻击方法：

弱口令，爆破

管理后台部署 war 后门

反序列化

远程代码执行

参考：

http://www.vuln.cn/6300

http://mobile.www.cnblogs.com/Safe3/archive/2010/01/08/1642371.html

https://www.zybuluo.com/websec007/note/838374

https://blog.csdn.net/u011215939/article/details/79141624

3. WebLogic

WebLogic 是美国 Oracle 公司出品的一个 Application Server，确切的说是一个基于 JAVAEE 架构的中间件，WebLogic 是用于开发、集成、部署和管理大型分布式 Web 应用、网络应用和数据库应用的 Java 应用服务器。将Java的动态功能和 Java Enterprise 标准的安全性引入大型网络应用的开发、集成、部署和管理之中。

端口：7001，7002

攻击方法：

弱口令、爆破，弱密码一般为weblogic/Oracle@123 or weblogic

管理后台部署 war 后门

SSRF

反序列化漏洞

weblogic_uac

参考：

https://github.com/vulhub/vulhub/tree/master/weblogic/ssrf

https://blog.gdssecurity.com/labs/2015/3/30/weblogic-ssrf-and-xss-cve-2014-4241-cve-2014-4210-cve-2014-4.html

https://fuping.site/2017/06/05/Weblogic-Vulnerability-Verification/

https://bbs.pediy.com/thread-224954.htm

4. WebSphere

WebSphere 是 IBM 公司一套典型的电子商务应用开发工具及运行环境。

端口：默认端口：908*；第一个应用就是9080，第二个就是9081；控制台9090

攻击方法：

控制台登录爆破

很多内网 websphere 的控制台存在弱口令 / 默认口令，可以使用 admin/admin 以及 webshpere/webshpere 这种口令登录。 通过该口令登录控制台后，可以部署 war 包，从而获取到 WEBSHELL 。

反序列化

任意文件泄露

参考：

https://loudong.sjtu.edu.cn/?keyword=WebSphere&serverity=%E9%AB%98%E5%8D%B1

http://www.fr1sh.com/wooyun_1/bug_detail.php?wybug_id=wooyun-2013-036803

https://gist.github.com/metall0id/bb3e9bab2b7caee90cb7

5. Glassfish

3.1.3 Web 框架

1. Struts2

Struts2 是一个优雅的,可扩展的框架,用于创建企业准备的 Java Web 应用程序。出现的漏洞也着实的多每爆一个各大漏洞平台上就会被刷屏。

可利用漏洞

S2-046 CVE-2017-5638 Struts 2.3.5-2.3.31,Struts 2.5-2.5.10
S2-045 CVE-2017-5638 Struts 2.3.5-2.3.31,Struts 2.5-2.5.10
S2-037 CVE-2016-4438 Struts 2.3.20-2.3.28.1
S2-032 CVE-2016-3081 Struts 2.3.18-2.3.28
S2-020 CVE-2014-0094 Struts 2.0.0-2.3.16
S2-019 CVE-2013-4316 Struts 2.0.0-2.3.15.1
S2-016 CVE-2013-2251 Struts 2.0.0-2.3.15
S2-013 CVE-2013-1966 Struts 2.0.0-2.3.14
S2-009 CVE-2011-3923 Struts 2.0.0-2.3.1.1
S2-005 CVE-2010-1870 Struts 2.0.0-2.1.8.1

参考：

https://github.com/hktalent/myhktools

https://github.com/Lucifer1993/struts-scan

https://github.com/SecureSkyTechnology/study-struts2-s2-054_055-jackson-cve-2017-7525_cve-2017-15095

2. Spring 框架

Spring Framework 是一个开源的Java / Java EE全功能栈（full-stack）的应用程序框架，以Apache License 2.0开源许可协议的形式发布，也有.NET 平台上的移植版本。Spring Framework提供了一个简易的开发方式，这种开发方式，将避免那些可能致使底层代码变得繁杂混乱的大量的属性文件和帮助类。

可利用漏洞

CVE-2010-1622
CVE-2018-1274
CVE-2018-1270
CVE-2018-1273
反序列化
目录穿越

参考

http://www.inbreak.net/archives/377
https://www.secpulse.com/archives/71762.html
http://www.open-open.com/news/view/1225d07
https://xz.aliyun.com/t/2261
https://xz.aliyun.com/t/2252

3.1.4 Web 服务器

IIS：Windows 的 WWW 服务器
https://masterxsec.github.io/2017/06/07/IIS-write-%E6%BC%8F%E6%B4%9E%E5%88%A9%E7%94%A8/
http://www.freebuf.com/articles/4908.html
https://www.anquanke.com/post/id/85811
IIS，开启了 WebDAV，可以直接详服务器 PUT 文件
短文件名枚举漏洞
远程代码执行
提权漏洞
解析漏洞

端口：80

攻击方法参考：
Apache
解析漏洞
目录遍历

Nginx

https://www.seebug.org/vuldb/ssvid-92538

CVE-2016-1247：需要获取主机操作权限，攻击者可通过软链接任意文件来替换日志文件，从而实现提权以获取服务器的root权限。

端口：80

攻击方法：
解析漏洞
目录遍历

参考：
lighttpd

3.2 常见运维系统

一般分自动化部署和运维监控相关的的工具。漏洞可以通过搜索引擎搜索，github搜索，ExploitDB搜索，官网上的安全通告获取。

内网的通用类应用比较常见的问题是弱口令，如果一个管理员可以登录几个系统，那在这几个系统的账号、密码也基本上是一样的。

3.2.1 Gitlab

GitLab是一个利用 Ruby on Rails 开发的开源应用程序，实现一个自托管的项目仓库，可通过Web界面进行访问公开的或者私人项目。

可利用漏洞：

任意文件读取漏洞
意用户 token 泄露漏洞
命令执行漏洞

参考：
http://blog.knownsec.com/2016/11/gitlab-file-read-vulnerability-cve-2016-9086-and-access-all-user-authentication-token/
http://rinige.com/index.php/archives/577/

3.2.2 Jenkins

Jenkins是一种跨平台的持续集成和交付的应用软件，它便于不断稳定地交付新的软件版本，并提高你的工作效率。这款开发运维工具还让开发人员更容易把项目的变化整合起来，并使用大量的测试和部署技术。

可利用漏洞：

远程代码执行漏洞
反序列化漏洞
未授权访问漏洞
登录入口爆破

参考
https://www.cnblogs.com/backlion/p/6813260.html
https://www.anquanke.com/post/id/86018
https://paper.seebug.org/199/

3.2.3 Puppet

Puppet Enterprise专门管理基础设施即代码(IAC)，在这种类型的IT基础设施配置过程中，系统用代码而不是脚本流程来自动构建、管理和配置。由于它是代码，整个过程易于重复。Puppet有助于更容易控制版本、自动化测试和持续交付，可以更快速地响应问题或错误。

可利用漏洞，很少公开的POC

反序列化
远程命令执行

3.2.4 Ansible

Ansible是一种配置和管理工具，面向客户端的软件部署和配置，支持Unix、Linux和Windows。它使 用JSON和YAML，而不是IAC，根本不需要节点代理就可以安装。它可以通过OpenStack在内部系统上使用，也可以在亚马逊EC2上使用。

可利用漏洞

远程代码执行

3.2.5 Nagios

Nagios是一款开源的电脑系统和网络监视工具，能有效监控Windows、Linux和Unix的主机状态，交换机路由器等网络设置，打印机等。在系统或服务状态异常时发出邮件或短信报警

第一时间通知网站运维人员，在状态恢复后发出正常的邮件或短信通知。

可利用漏洞

代码执行

SQLi

参考

http://www.bugku.com/thread-87-1-1.html
http://www.mottoin.com/93936.html

3.2.6 Zabbix

Zabbix 是一款强大的开源分布式监控系统，能够将SNMP、JMX、Zabbix Agent提供的数据通过WEB GUI的方式进行展示.

可利用漏洞（具体参考 ExploitDB）：

远程代码执行

SQLi

shell 命令注入

认证绕过

默认账户与密码，默认口令 admin/zabbix，或者是guest/空

参考

https://blog.csdn.net/ytuo1223/article/details/45937981
http://vinc.top/2017/04/18/zabbix%E6%BC%8F%E6%B4%9E%E6%80%BB%E7%BB%93/
http://www.mottoin.com/87570.html

3.2.7 Cacit

Cacti是一套基于PHP,MySQL,SNMP及RRDTool开发的网络流量监测图形分析工具。

可利用漏洞

任意代码执行

SQLi

登录爆破

默认密码admin/admin

参考：

http://wooyun.jozxing.cc/static/bugs/wooyun-2011-02674.html

3.2.8 Splunk

Splunk Enterprise 可以从任何来源监控和分析机器数据，以提供操作智能，从而优化您的 IT、安全和业务绩效。Splunk Enterprise 具有直观的分析功能、机器学习、打包应用程序和开放式 API，是一个灵活的平台，可从重点用例扩展到企业范围的分析主干。

可利用漏洞

信息泄露

命令注入

服务端请求伪造

参考

Exploit DB 搜索

3.3 常见 Web 应用

还有常见邮件应用、CMS 应用，在搜索引擎上查找对应的漏洞，利用已知漏洞进行攻击。

3.3.1 邮件系统

一部分是使用腾讯企业邮箱、阿里企业邮箱的，很难有可利用的漏洞，另外一种是能独立部署的邮件系统，政企常用的邮箱应用：

Coremail

亿邮

35互联

TurboMail

Exchange

IBM Lotus

3.3.2 CMS 应用

3.4 数据库/缓存/消息服务

3.4.1 MySQL数据库

默认端口：3306

攻击方法：

爆破：弱口令

身份认证漏洞：CVE-2012-2122

拒绝服务攻击

Phpmyadmin万能密码绕过：用户名：‘localhost’@’@”密码任意

提权

参考：

https://www.seebug.org/appdir/MySQL

http://www.waitalone.cn/mysql-tiquan-summary.html?replytocom=390

https://xz.aliyun.com/t/1491

3.4.2 MSSQL数据库

默认端口：1433（Server 数据库服务）、1434（Monitor 数据库监控）

攻击方法：

爆破：弱口令/使用系统用户

注入

参考：

https://www.anquanke.com/post/id/86011

3.4.3 Oracle数据库

默认端口：1521（数据库端口）、1158（Oracle EMCTL端口）、8080（Oracle XDB数据库）、210（Oracle XDB FTP服务）

攻击方法：

爆破：弱口令

注入攻击；

漏洞攻击；

参考：

https://www.leiphone.com/news/201711/JjzXFp46zEPMvJod.html

3.4.4 PostgreSQL数据库

PostgreSQL是一种特性非常齐全的自由软件的对象－关系型数据库管理系统，可以说是目前世界上最先进，功能最强大的自由数据库管理系统。包括kali系统中msf也使用这个数据库；浅谈postgresql数据库攻击技术 大部分关于它的攻击依旧是sql注入，所以注入才是数据库不变的话题。

默认端口：5432

攻击方法：

爆破：弱口令：postgres postgres

缓冲区溢出：CVE-2014-2669

参考：

http://drops.xmd5.com/static/drops/tips-6449.html

https://www.secpulse.com/archives/69153.html

3.4.5 MongoDB数据库

MongoDB，NoSQL数据库；攻击方法与其他数据库类似

默认端口：27017

攻击方法：

爆破：弱口令

未授权访问；github有攻击代码

参考：

http://www.cnblogs.com/LittleHann/p/6252421.html

http://www.tiejiang.org/19157.html

3.4.6 Redis数据库

Redis是一个开源的使用c语言写的，支持网络、可基于内存亦可持久化的日志型、key-value数据库。关于这个数据库这两年还是很火的，暴露出来的问题也很多。特别是前段时间暴露的未授权访问。

攻击方法：

爆破：弱口令

未授权访问+配合ssh key提权；

参考：

http://www.alloyteam.com/2017/07/12910/

3.4.7 SysBase数据库

默认端口：服务端口5000；监听端口4100；备份端口：4200

攻击方法：

爆破：弱口令

命令注入：

3.4.8 DB2 数据库

默认端口：5000

攻击方法：

安全限制绕过：成功后可执行未授权操作（CVE-2015-1922）

参考：

http://23.94.222.93/bug_detail.php?wybug_id=wooyun-2015-0113071

3.5 常见服务/协议

3.5.1 FTP 服务

FTP服务：ftp服务我分为两种情况，第一种是使用系统软件来配置，比如IIS中的FTP文件共享或Linux中的默认服务软件；第二种是通过第三方软件来配置，比如Serv-U还有一些网上写的简易ftp服务器等；

默认端口：20（数据端口）；21（控制端口）；69（tftp小型文件传输协议）

攻击方式：

爆破：ftp的爆破工具有很多，这里我推荐owasp的Bruter 以及msf中ftp爆破模块；

匿名访问：用户名：anonymous 密码：为空或任意邮箱

嗅探：ftp使用明文传输技术（但是嗅探给予局域网并需要欺骗或监听网关）

后门 vsftp

远程溢出

跳转攻击

3.5.2 NFS 服务

NFS（Network File System）即网络文件系统，是FreeBSD支持的文件系统中的一种，它允许网络中的计算机之间通过TCP/IP网络共享资源。在NFS的应用中，本地NFS的客户端应用可以透明地读写位于远端NFS服务器上的文件，就像访问本地文件一样。如今NFS具备了防止被利用导出文件夹的功能，但遗留系统中的NFS服务配置不当，则仍可能遭到恶意攻击者的利用。

攻击方法

未授权访问

参考

http://www.freebuf.com/articles/network/159468.html

http://www.vuln.cn/6368

3.5.3 Samba服务

Samba是linux和unix系统上实现SMB/CIFS协议的一个免费软件，由服务器和客户端程序构成。而SMB是局域网支持共享文件和打印机的一种通信协议，为局域网内不同计算机之

间提供文件及打印机等资源的共享服务。

攻击方法

远程代码执行

弱口令

未授权访问（public）

参考

http://www.91ri.org/17114.html

3.5.4 SSH 服务

SSH 是协议，通常使用 OpenSSH 软件实现协议应用。SSH 为 Secure Shell 的缩写，由 IETF 的网络工作小组（Network Working Group）所制定；SSH 为建立在应用层和传输层基础上的安全协议。SSH 是目前较可靠，专为远程登录会话和其它网络服务提供安全性的协议。利用 SSH 协议可以有效防止远程管理过程中的信息泄露问题。

端口：22

攻击方法：

爆破

后门

漏洞：28退格漏洞、OpenSSL漏洞

参考

https://cloud.tencent.com/developer/article/1078187

3.5.5 Telnet 服务

Telnet协议是TCP/IP协议族中的一员，是Internet远程登陆服务的标准协议和主要方式。它为用户提供了在本地计算机上完成远程主机工作的能力。在终端使用者的电脑上使用telnet程序，用它连接到服务器。终端使用者可以在telnet程序中输入命令，这些命令会在服务器上运行，就像直接在服务器的控制台上输入一样。可以在本地就能控制服务器。

默认端口：21

攻击方法：

爆破

嗅探

3.5.6 Windows 远程连接

默认端口：3389

攻击方法

爆破

Shift粘滞键后门：5次shift后门

利用ms12-020攻击3389端口

3.5.7 VNC服务

VNC（Virtual Network Computing），为一种使用RFB协议的显示屏画面分享及远程操作软件。此软件借由网络，可发送键盘与鼠标的动作及即时的显示屏画面。

默认端口：5900+桌面ID（5901；5902）

攻击方式：

爆破：弱口令

认证口令绕过：

拒绝服务攻击：（CVE-2015-5239）

权限提升：（CVE-2013-6886）

3.5.8 SMTP协议

smtp：邮件协议，在linux中默认开启这个服务，可以向对方发送钓鱼邮件！

默认端口：25（smtp）、465（smtps）

攻击方式：

爆破：弱口令

未授权访问

3.5.9 POP3协议

默认端口：109（POP2）、110（POP3）、995（POP3S）

攻击方式：

爆破；弱口令

未授权访问；

3.5.10 DNS服务

默认端口：53

攻击方式：

区域传输漏洞

3.5.11 IMAP协议

默认端口：143（imap）、993（imaps）

攻击方式：

爆破：弱口令

配置不当

3.5.12 SNMP协议

默认端口：161

攻击方式:

爆破：弱口令

3.5.13 DHCP服务

默认端口：67&68、546（DHCP Failover做双机热备的）

攻击方式：

DHCP劫持；

3.6 云环境

3.6.1 VMware

使用 VMware vCloud 可将现有数据中心内的虚拟基础架构资源池化，并将其作为基于目录的服务交付。通过与云计算基础架构的最佳平台 VMware vSphere 配合使用，VMware vCloud Director 可为客户提供构建安全的私有云，从而改变 IT 部门交付和管理基础架构服务以及用户访问和使用这些服务的方式。

一般组织中很多独立安装的 Esxi 形式的私有云，或独立部署的虚拟化系统。

端口（很多）：
https://kb.vmware.com/s/article/2115330
https://kb.vmware.com/s/article/2081930

漏洞
主机逃逸
CVE-2017-5638

参考：
https://paper.seebug.org/348/
http://www.freebuf.com/articles/system/141179.html
http://www.mottoin.com/100651.html
http://www.52bug.cn/%E9%BB%91%E5%AE%A2%E6%8A%80%E6%9C%AF/4375.html
https://twitter.com/VMwareSRC
https://loudong.sjtu.edu.cn/?keyword=vmware&serverity=%E9%AB%98%E5%8D%B1&page=1
https://www.vmware.com/cn/security/hardening-guides.html

3.6.2 OpenStack

OpenStack是基础设施即服务（IaaS）软件，让任何人都可以自行创建和提供云计算服务。此外，OpenStack也用作创建防火墙内的“私有云”（Private Cloud），提供机构或企业内各部门共享资源。

漏洞，有漏洞但是POC基本没有。检查时候可以参考安全的配置实践。
权限绕过漏洞
信息泄露
代码执行漏洞

参考：
https://loudong.sjtu.edu.cn/?keyword=openstack&serverity=%E9%AB%98%E5%8D%B1
https://docs.openstack.org/liberty/zh_CN/install-guide-obs/environment-security.html
http://www.freebuf.com/news/topnews/107203.html

3.6.3 Docker

Docker是一个开放源代码软件项目，让应用程序布署在软件容器下的工作可以自动化进行，借此在Linux操作系统上，提供一个额外的软件抽象层，以及操作系统层虚拟化的自动管理机制[1]。Docker利用Linux核心中的资源分脱机制，例如cgroups，以及Linux核心名字空间（name space），来创建独立的软件容器（containers）。这可以在单一Linux实体下运作，避免引导一个虚拟机造成的额外负担。Linux核心对名字空间的支持完全隔离了工作环境中应

用程序的视野，包括进程树、网络、用户ID与挂载文件系统，而核心的cgroup提供资源隔离，包括CPU、内存、block I/O与网络。从0.9版本起，Dockers在使用抽象虚拟是经由libvirt的LXC与systemd – nspawn提供界面的基础上，开始包括libcontainer函数库做为以自己的方式开始直接使用由Linux核心提供的虚拟化的设施。

安全问题（很少有漏洞的POC，安全检查也是基于最佳实践和官方安全建议进行）：

CVE-2015-3630 1.6.0 Docker Libcontainer 安全绕过漏洞
CVE-2015-3627 1.6.1 Libcontainer和Docker Engine 权限许可和访问控制漏洞
CVE-2015-3630 1.6.1 Docker Engine 安全绕过漏洞
CVE-2014-9358 1.3.3 Docker 目录遍历漏洞
CVE-2014-9357 1.3.2 Docker 权限许可和访问控制漏洞
CVE-2014-6408 1.3.1 Docker 权限许可和访问控制漏洞
CVE-2014-5277 1.3.0 Docker和docker-py 代码注入漏洞

内核漏洞（Kernel exploits） 容器是基于内核的虚拟化，主机（host）和主机上的所有容器共享一套内核。如果某个容器的操作造成了内核崩溃，那么反过来整台机器上的容器都会受到影响。

拒绝服务攻击（Denial-of-service attacks） 所有的容器都共享了内核资源，如果一个容器独占了某一个资源（内存、CPU、各种ID），可能会造成其他容器因为资源匮乏无法工作（形成DoS攻击）。

容器突破（Container breakouts） Linux的namespace机制是容器的核心之一，它允许容器内部拥有一个PID=1的进程而在容器外部这个进程号又是不一样的（比如1234）。现在问题在于如果一个PID=1的进程突破了namespace的限制，那么他将会在主机上获得root权限。
有毒镜像（Poisoned images） 主要是考虑到镜像本身的安全性，没太多好说的。

参考：
https://toutiao.io/posts/2y9xx8/preview
http://www.yunweipai.com/archives/21610.html
http://www.91ri.org/15837.html
https://blog.csdn.net/ruidu_doer/article/details/53401523
https://loudong.sjtu.edu.cn/?keyword=docker&serverity=%E9%AB%98%E5%8D%B1
http://dockone.io/article/150
http://www.dockerinfo.net/docker/docker%E5%AE%89%E5%85%A8
https://blog.waterstrong.me/docker-security/

3.7 大数据

3.7.1 Elsaticsearch

Elasticsearch 是一个分布式的搜索和分析引擎，可以用于全文检索、结构化检索和分析，并能将这三者结合起来。Elasticsearch 基于 Lucene 开发，现在是使用最广的开源搜索引擎之一，Wikipedia、Stack Overflow、GitHub 等都基于 Elasticsearch 来构建他们的搜索引擎。

默认端口：9200（）、9300（）

攻击方法：

未授权访问；

远程命令执行；
文件遍历；
低版本webshell植入；

参考
http://www.freebuf.com/sectool/38025.html
https://www.secpulse.com/archives/5401.html

3.7.2 hadoop

Hadoop是一个开源的框架，可编写和运行分布式应用处理大规模数据，是专为离线和大规模数据分析而设计的，并不适合那种对几个记录随机读写的在线事务处理模式。

Hadoop=HDFS（文件系统，数据存储技术相关）+ Mapreduce（数据处理），Hadoop的数据来源可以是任何形式，在处理半结构化和非结构化数据上与关系型数据库相比有更好的性能，具有更灵活的处理能力，不管任何数据形式最终会转化为key/value，key/value是基本数据单元。用函数式变成Mapreduce代替SQL，SQL是查询语句，而Mapreduce则是使用脚本和代码，而对于适用于关系型数据库，习惯SQL的Hadoop有开源工具hive代替。 Hadoop就是一个分布式计算的解决方案。

参考：
https://tech.meituan.com/hadoop-security-practice.html
https://zhuanlan.zhihu.com/p/33525241
https://www.anquanke.com/post/id/85343
https://www.cloudera.com/documentation/cdh/5-0-x/CDH5-Security-Guide/cdh5sg_hadoop_security_intro.html

3.7.3 Hive

Hive是Hadoop家族中一款数据仓库产品，Hive最大的特点就是提供了类SQL的语法，封装了底层的MapReduce过程，让有SQL基础的业务人员，也可以直接利用Hadoop进行大数据的操作。

参考：
https://cwiki.apache.org/confluence/display/Hive/Security
https://www.cnblogs.com/yejibigdata/p/6394719.html

3.7.4 Sqoop

Apache Sqoop（SQL-to-Hadoop） 项目旨在协助 RDBMS 与 Hadoop 之间进行高效的大数据交流。用户可以在 Sqoop 的帮助下，轻松地把关系型数据库的数据导入到 Hadoop 与其相关的系统 (如HBase和Hive)中；同时也可以把数据从 Hadoop 系统里抽取并导出到关系型数据库里。除了这些主要的功能外，Sqoop 也提供了一些诸如查看数据库表等实用的小工具。

参考
https://sqoop.apache.org/docs/1.99.7/security.html

3.7.5 HBase

HBase建立在HDFS之上，提供高可靠性、高性能、列存储、可伸缩、实时读写的数据库系统。它介于NoSQL和RDBMS之间，仅能通过行键(row key)和行键序列来检索数据，仅支持单行事务(可通过Hive支持来实现多表联合等复杂操作)。主要用来存储非结构化和半结构化

的松散数据。与Hadoop一样，HBase目标主要依靠横向扩展，通过不断增加廉价的商用服务器，来增加计算和存储能力。

参考：
https://www.cloudera.com/documentation/enterprise/5-6-x/topics/admin_hbase_security.html
http://www.cloudera.com/documentation/cdh/5-1-x/CDH5-Security-Guide/cdh5sg_hbase_security.html

3.7.6 Spark

Spark是UC Berkeley AMP lab所开源的类Hadoop MapReduce的通用的并行计算框架，Spark基于map reduce算法实现的分布式计算，拥有Hadoop MapReduce所具有的优点；但不同于MapReduce的是Job中间输出和结果可以保存在内存中，从而不再需要读写HDFS。

参考：
http://cwiki.apachecn.org/pages/viewpage.action?pageId=2887905

4 后渗透

4.1 提权

SecWiki 总结了：
https://github.com/SecWiki/windows-kernel-exploits
https://github.com/SecWiki/linux-kernel-exploits

4.2 域攻击

通常域内渗透的过程

确定目标系统和应用程序
识别潜在的漏洞
利用漏洞获得初始访问
提升权限
定位域管理进程或者获取远程系统上的本地身份验证令牌
通过本地管理员的密码Hash，破解密码，使用mimikatz工具抓取密码验证运行在远程系统上的域名管理进程
迁移域管理进程
创建一个域管理员

假设到这里已经从外网或内网利用漏洞入侵到到一台服务器，并且通过提权获取了主机管理员权限，接下来要做的工作是获取域管理员权限，并找到敏感数据。

通常会使用到的工具：

Empire
PowerUp
PowerView

一般熟练使用一种就够用了，以 Empire 为例：

Empire 和 Metasploit 的使用原理是一样的，都是先设置一个监听，然后去生成一个木马，然后在目标主机运行该木马，我们的监听就会连接上反弹回来的代理。

参考：
https://www.anquanke.com/post/id/87328
http://www.4hou.com/technology/4704.html

域渗透另外一个工具 mimikatz，用于抓 Windows 密码

参考：
http://www.mottoin.com/98506.html
https://zhuanlan.zhihu.com/p/34991269

4.3 建立后门/端口转发

参考：
http://www.zerokeeper.com/experience/network-port-forwarding-and-penetration.html
https://1sparrow.com/2018/01/20/%E7%AB%AF%E5%8F%A3%E8%BD%AC%E5%8F%91%E6%80%BB%E7%BB%93/
http://drops.xmd5.com/static/drops/tools-15000.html

端口转发及代理类工具

LCX：windows下面的端口转发软件。

sockscap：主要针对windows平台的端口转发和代理转发。

proxifier：跨平台的端口转发和代理工具，适用windows，linux，Macos平台，代理转发利器

Rsscoks：＊nix平台下的端口转发和代理工具，配合proxychains好用到不行。

Proxychains：＊nix平台下老牌的socks代理工具，一般的系统都会自带，谁用谁知道。

ssh proxy：通过ssh做端口代理和转发，一般＊nix系统都自带。

netcat：socat，hping，在很多情况下可以做端口转发和数据代理转发。

metasploit：metasploit的后渗透模块中有不少代理模块和端口转发模块。

在中转服务器上下载端口转发工具（加密压缩）：

能连接互联网下载

通过 mstsc 的磁盘加载

通过入口服务器中转

通过远程控制软件上传

4.4 传输文件

4.4.1 文件打包

关于打包

Rar文件打包，压缩d:\data\目录下所有2013-01-01后修改的doc文件，100M/包密码为Pass，-x为排除选项

rar.exe a-r -v100m new.rar -ta20130101000000 -hpPass -n*.doc -x*.exe d:\data\

7z加密，压缩d:\data下所有文件，密码为Pass，分卷100M/包

7z.exe a c:\xx.7z -pPass -mhe d:\data -v100m

Linux用 tar 打包文件是可以加密码，要跟openssl结合使用。

tar –zcvf – pma|openssl des3 –salt –k password | dd of=pma.des3

使用 tar 对加密文件解压：
dd if=pma.des3 |openssl des3 –d –k password|tar zxf –

4.4.2 文件传输

几个思路

使用端口转发直接传送数据；
搭建 FTP、HTTP 协议；
上传到云端再下载；

4.5 制作后门/木马程序

一般用Matisploit 的 msfvenom

参考：
https://github.com/rapid7/metasploit-framework/wiki/How-to-use-msfvenom
https://www.offensive-security.com/metasploit-unleashed/msfvenom/

SET 也可以生成后门程序，另外也可以关注一下最新的 Office、PDF 的漏洞

5 日志清理

这部分对于安全检查、或授权渗透测试工作不是重点，通常也不考虑。

在做日志清理前需要了解以下的内容：

攻击和入侵很难完全删除痕迹，没有日志记录本身就是一种入侵特征；
删除或清理入侵系统的本地日志不代表删除了痕迹，在网络设备、安全设备、集中化日志系统上仍然留存记录；
留存的后门本身会有攻击者的信息；
使用的代理或跳板可能会被反向入侵;
在操作前检查是否有管理员登录；
删除上传的工具，使用磁盘覆写的功能删除；

Windows日志类型

web日志：IIS、Apache以及其它web日志
操作日志：3389登录列表、最近访问文件、IE等浏览器访问日志、文件访问日志
登陆日志：系统应用日志-安全日志等
攻击前和状态还原，尽量保持一致

Linux操作日志

Linux历史操作

unset HISTORY HISTFILE HISTSAVE HISTZONE HISTORY HISTLOG;
export HISTFILE=/dev/null;

SSHD登陆记录
删除~/.ssh/known_hosts中记录
修改文件时间戳
touch －r 原文件要修改文件

删除临时使用文件，尤其是tmp目录logtamper

6 工具和其他

内网使用工具渗透的一些原则

使用适合自己的工具，工具没必要收集太多，够用就行；

能根据实际情况编写适用的工具；

不能确保安全的工具均要在虚拟机中运行（很多捆绑病毒木马）；

做安全检查的话，尽量使用 GitHub 上开源的工具。

工具介绍

个人习惯使用 kali 自带工具，特定 POC 先从 Github 上搜索。

推荐一个工具介绍的网站：https://www.kitploit.com/

渗透注意事项

检查内网监控防范系统
谨慎使用ARP软件和大面积扫描软件
使用目标网络中无空闲机器，作为打包对象
使用内网大流量机器作为传输对象，如wsus服务器、视频会议系统
使用临时机器打包、数据传输，不要使用已控机器，可利用wmi脚本或wmic远程操作
禁止使用psexec.exe
打包时避开用户工作时间
控制卷包大小<100M
选择用户常用压缩软件
错峰下载数据
控制传输流量
清除所有操作日志
登录主机前先看看管理员是否在

感谢大佬们的总结

http://www.91ri.org/15441.html
https://paper.seebug.org/126/
https://paper.seebug.org/409/
DC010 上海站 演讲ppt《5内网渗透思路（陈小兵）.pdf》