The Nmap Project

Fotis Hantzis aka ithilgore
sock-raw.org

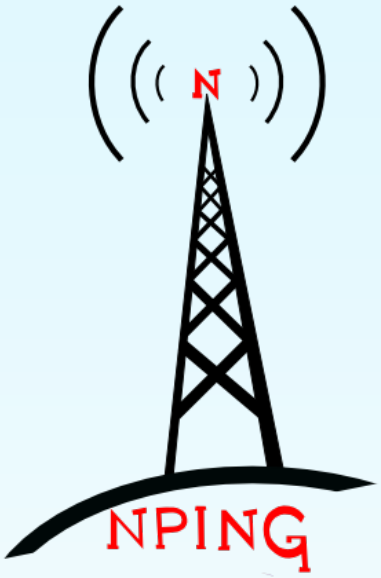
FOSSCOMM 2016

whoami

- Exploiting TCP and the Persist Timer Infiniteness (Phrack #66)
- Abusing Network Protocols (stealthy portscanning through XMPP exploitation)
- Nmap developer, Ncrack author
- Startup ventures

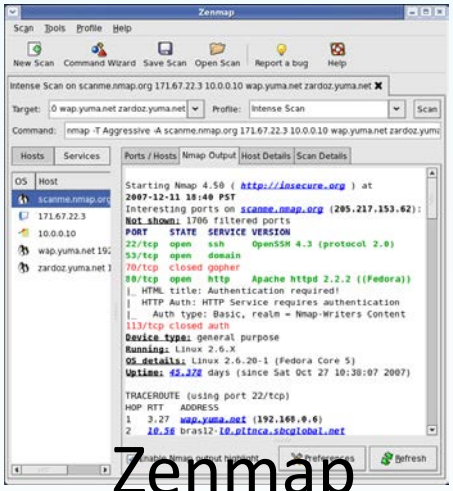
@ithilgore

http://phrack.org/issues/51/11.html#article



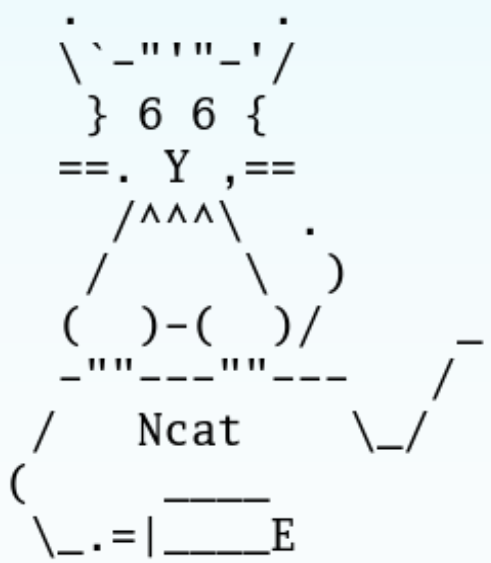
Ndiff

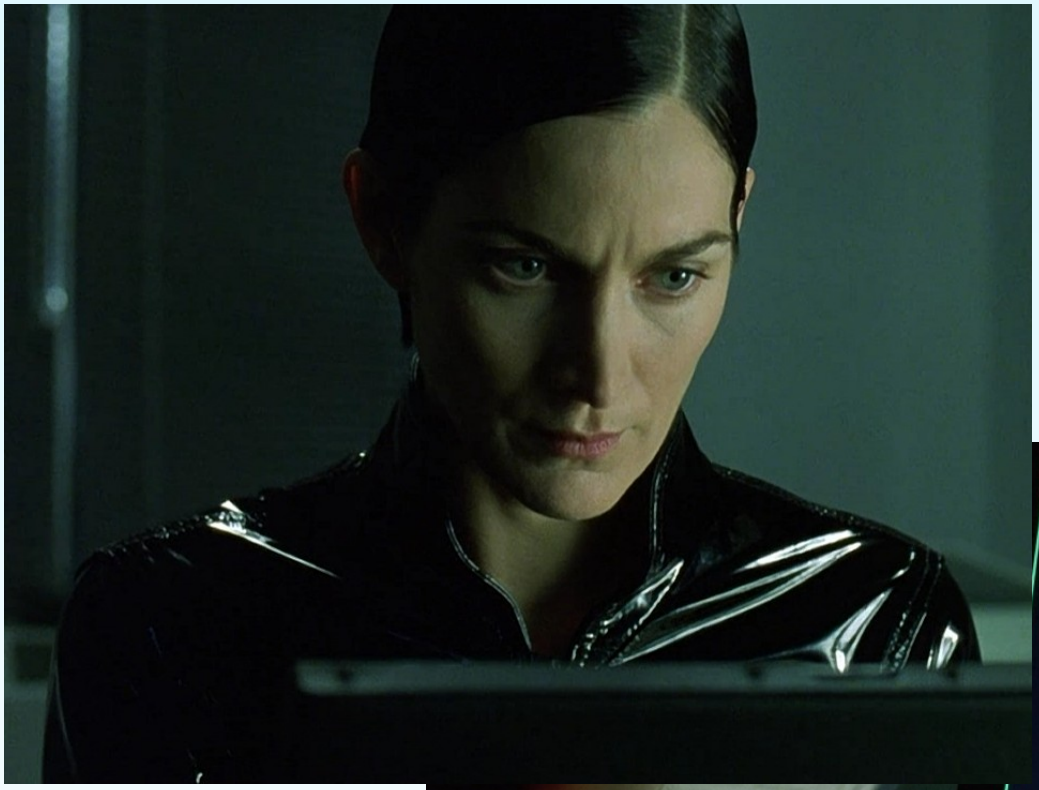
NSE



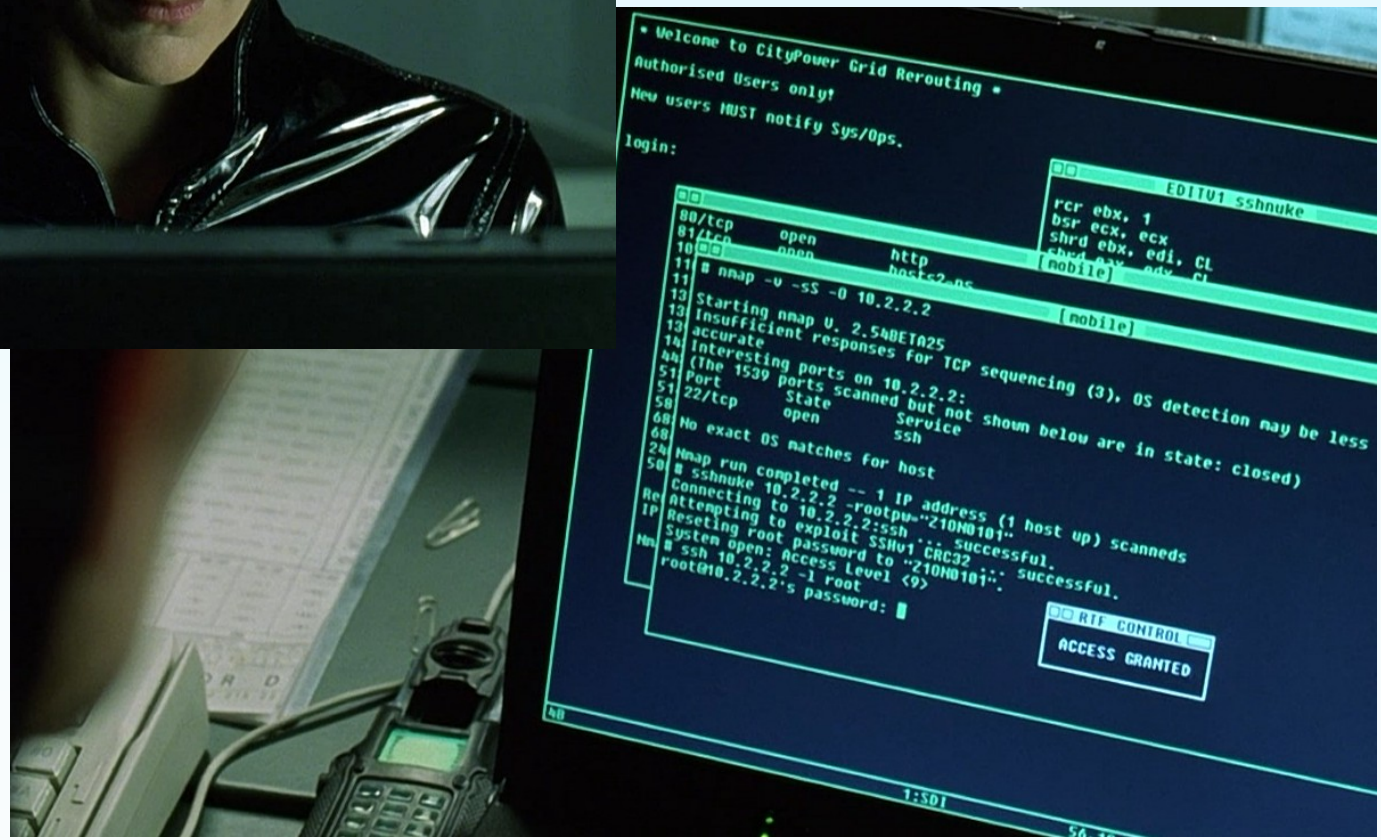
Zenmap

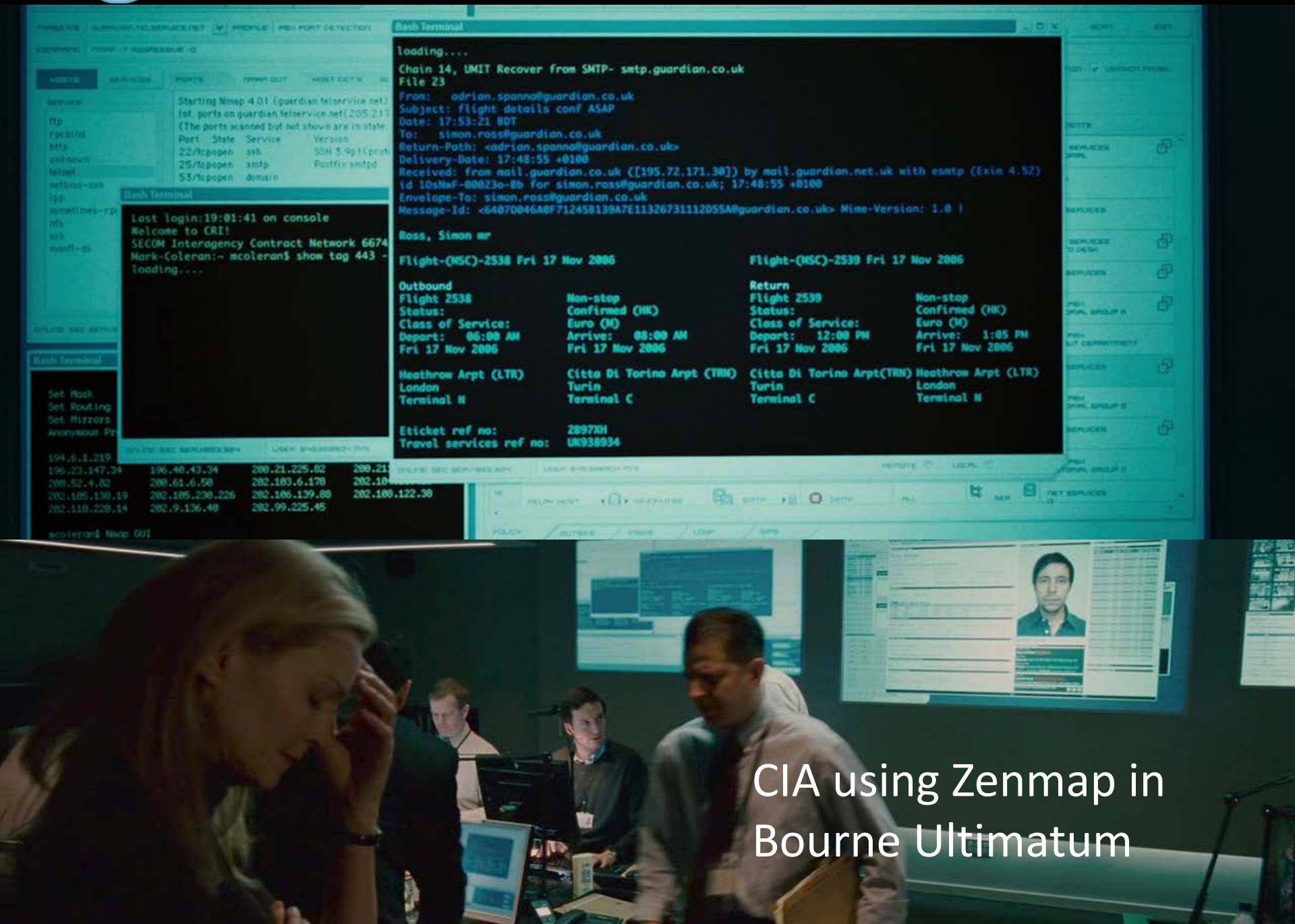
Npcap





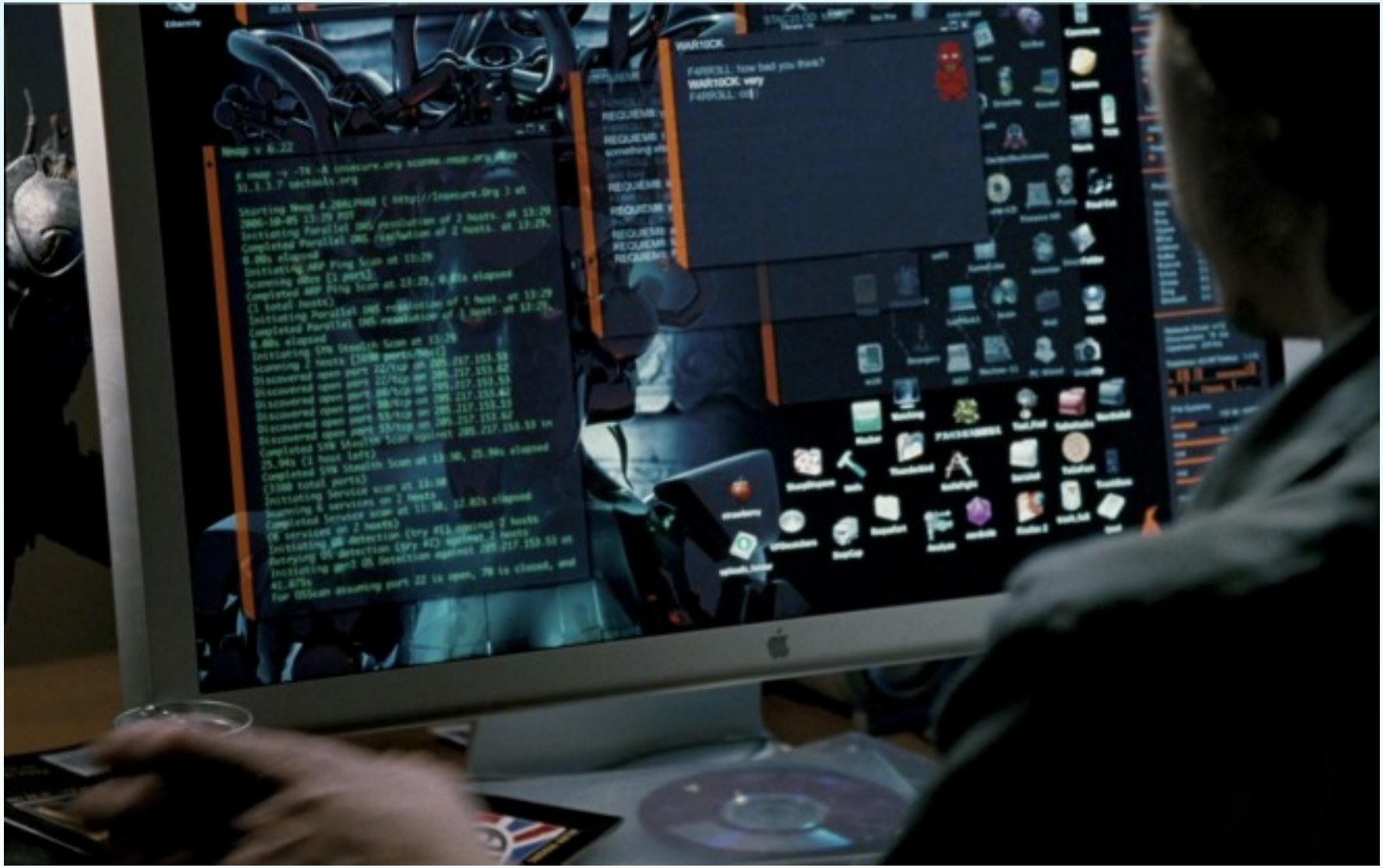
Trinity uses Nmap in Matrix Reloaded





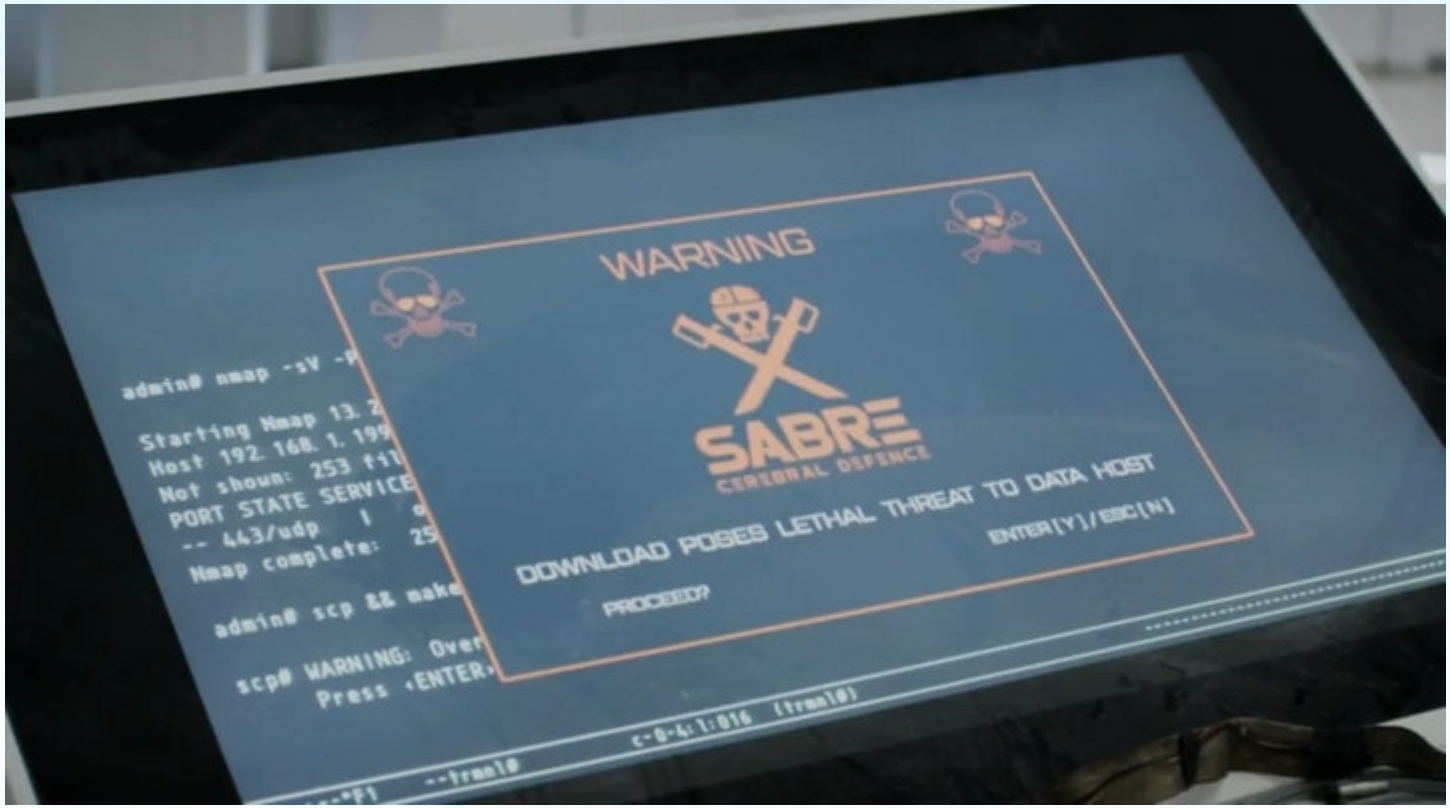
CIA using Zenmap in Bourne Ultimatum

Die Hard 4



And many more:
http://nmap.org/movies

Elysium



> 1000 students

$5.000 stipends

3 – 4 months

~ 150 open source organizations

Past Nmap GSoC Accomplishments

- Nping – generic packet crafting tool
- Ncat – the modern netcat
- Npcap – packet sniffing library (WPF)
- Ncrack – network auth cracking tool
- NSE – Nmap Scripting Engine
- Zenmap – GUI for Nmap
- Ndiff – diff for network scans

http://nmap.org/ncrack

High speed network authentication cracking tool

Ncrack's Main Features

- Intelligent Core Engine
- Service Recognition through Nmap (-oN, -oX)
- Fine-grained timing control (cl, CL, to, cd, at, T1-T5)
- Built-in username/password lists
- Session stop/resume
- Modular architecture
- Nsock based (asynchronous)

Ncrack modules

- SSH – custom opensshlib based on OpenSSH
- RDP – extremely hard protocol by MS
- SMB
- SIP

Contributions

- Telnet
- FTP
- HTTP (basic/digest)
- PostgreSQL
- MySQL
- VNC
- POP3
- Redis

New Ncrack 0.5 release

- New modules:
  Redis, PostgreSQL, MySQL, SIP, HTTP digest
- pairwise user/pass iteration
- proxy support
- New opensshlib based on OpenSSH 7.1

https://nmap.org/ncrack
https://github.com/nmap/ncrack

Ncrack modules TODO list:

- CVS, SVN
- Microsoft SQL
- HTTP Form
- IMAP
- SNMP
- LDAP
- XMPP
- Rsync, Rlogin

https://nmap.org/ncrack/devguide.html

Greek Nmap Developers

- **George Chatzisofroniou**: NSE scripts, GSoC 2013
- **Evangelos Deirmetzoglou**: Ncrack modules
- **Fotis Hantzis**: Ncrack author, Nmap dev,
  GSoC: {2009, 2010} - student
  2016 - mentor

Thanks for watching!
Follow me: @ithilgore

http://sock-raw.org
http://nmap.org
http://nmap.org/ncrack
http://github.com/nmap/ncrack

Questions?