

SECURITY

MORE TALES

**SEPT. 6
2018**

FROM THE

3:30pm

CRWPT

...ANALYST

GrrCON

online

Results. Guaranteed.

Jeff Man


Sr. Information Security Consultant
InfoSec Curmudgeon
Online Business Systems

@MrJeffMan

301-310-4275

jman@obsglobal.com




 Results. Guaranteed.

Apologies



This is how we did screenshots back in the day!

 Results. Guaranteed.

Important Dates in History

August 29, 1997

Skynet becomes self-aware

My 10 Years at NSA

National Security Agency

- ▀ Cryptography
- ▀ System Design & Development
- ▀ Cryptanalysis
- ▀ Fielded Systems Analysis
- ▀ Penetration Testing
- ▀ Vulnerability Assessment
- ▀ Threat Detection
- ▀ Forensics



 Results. Guaranteed.

NSA Tales v1.0

Cryptanalyst

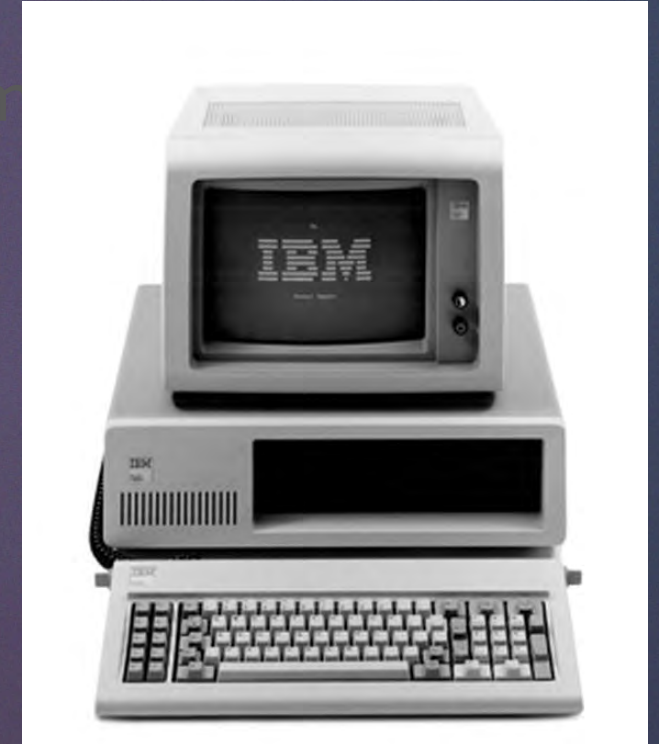
Manual Cryptosystems Branch

INFOSEC

One-Time Pad



One-Time Floppy Disc



Fielded NSA's First SW-Based Crypto System



Re-Writing the rules – “There’s no such thing as software...”



“This guy is a loose cannon”

 Results. Guaranteed.

NSA Tales v2.0

Cryptanalysis Intern
Operations



Cryptanalysis Intern

DS
DS

*The National Security Agency/
Central Security Service*

takes pleasure in presenting a Letter of Appreciation to

JEFFREY E. MAN



JUNE 1991

We want to convey our appreciation to you for your magnificent contribution to our fighting forces and the Nation during Operation Desert Shield/Storm. From the outset of Desert Shield and through the extremely successful completion of Desert Storm, you responded splendidly. Your dedication, perseverance, selflessness and professionalism were key factors in our victory.

We learned some very valuable lessons from Desert Shield/Storm, but above all we learned that hard work and self-sacrifice will always serve this Nation well.

Thank you for a job well done.

Donald L. Parsons

Donald L. Parsons
Deputy Director for Operations

W. O. Studeman

W. O. Studeman
Vice Admiral, U.S. Navy
Director



National Security Agency



Professionalization Program

JEFFREY E. MAN

is hereby certified

AS A

CRYPTANALYST

by the

CRYPTANALYSIS CAREER PANEL

EFFECTIVE THIS 23RD DAY OF AUGUST 1993

Robert Ekbar

Panel Chairperson

J. M. McConnell

J. M. McConnell
Vice Admiral, U.S. Navy
Director

 Results. Guaranteed.

NSA Tales v3.0

Fielded Systems Evaluations
Systems and Network Attack Center
The Pit

 Results. Guaranteed.

Fielded Systems Evaluations

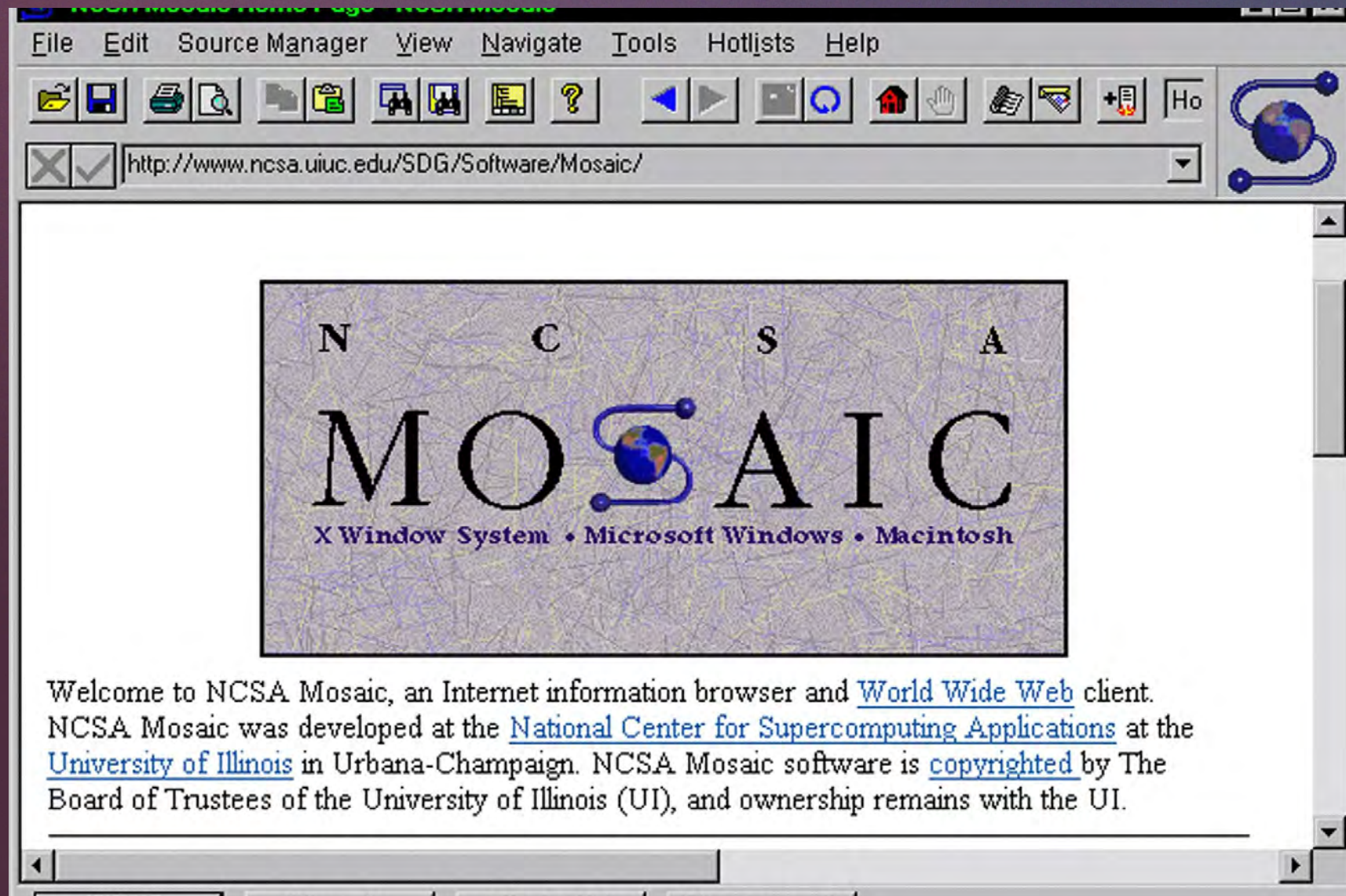
My final diversity tour as a Cryptanalysis Intern

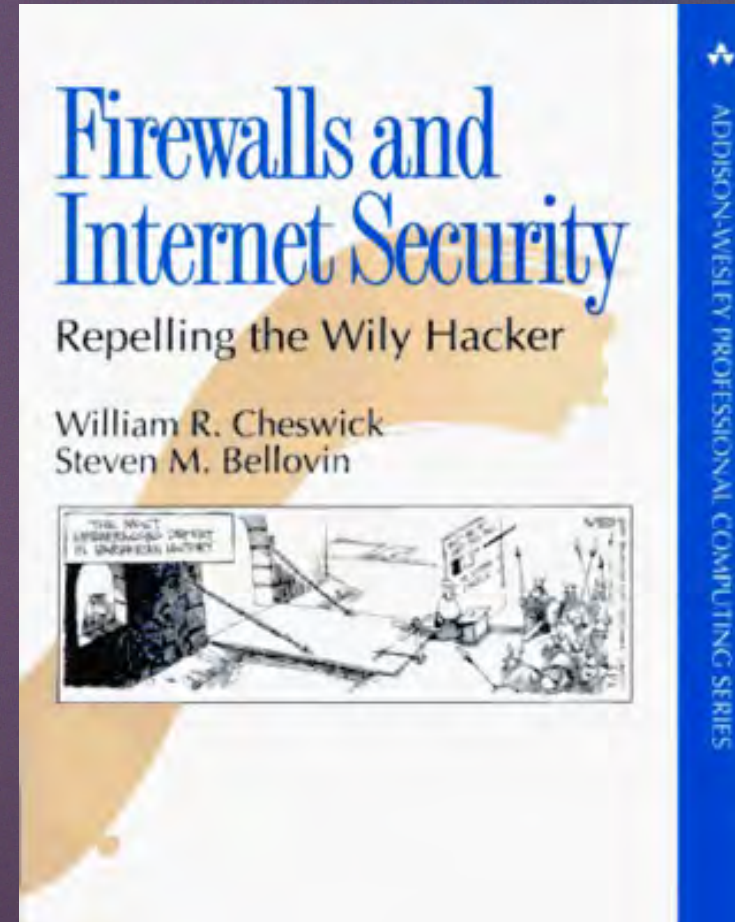
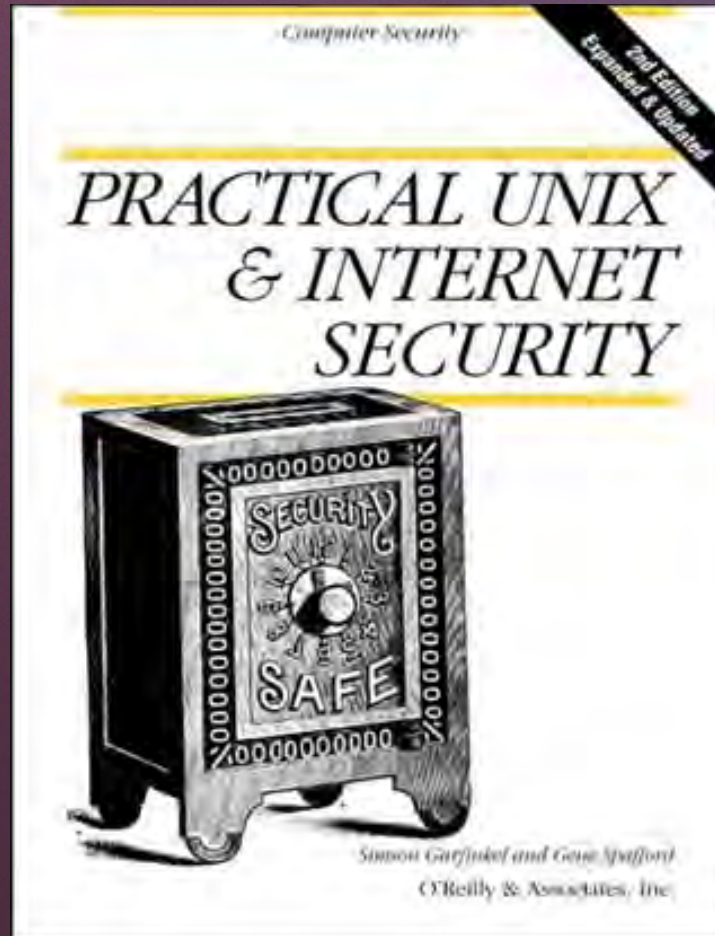


Security evaluations of fielded cryptosystems

January 23, 1993

NCSA MOSAIC initial release (and the world changed)





In the beginning...it was Internet Security (not Cyber)

 Results. Guaranteed.

We Assembled a Team

“If I could just hire me 50 of those hacker kids, we’d have something special...”

- Deputy Director for InfoSec (DDI)

 Results. Guaranteed.

Systems & Network Attack Center (SNAC)

NSA Center of Excellence for Computer and Network Security

C4 – The Systems & Network Attack Center (SNAC)

- ▀ Evolution of Fielded Systems Evaluations
- ▀ Formed to be a center of excellence for vulnerability research
- ▀ Developed initial attack and penetration testing methodologies used by NSA Red Teams
- ▀ Performed Vulnerability & Threat Assessments for all Classified networks within the DOD

Road Trip

We visited the Air Force Information Warfare Center to learn how to setup operations

online

Results. Guaranteed.



Our hosts and mentors...

online

Results. Guaranteed.



...and founders of one of the first commercial Internet security companies

online

San Antonio

Results. Guaranteed.



online

Results. Guaranteed.



Our biggest takeaway

 Results. Guaranteed.

We Developed a Methodology

Ground Rules (a.k.a. 'red tape')

- ▀ Our activities could be construed as active attacks against U.S. systems
 - ▀ Technically violated the NSA Charter as the activity is illegal
 - ▀ There were ways to accomplish the mission, but there were rules
- ▀ All activity had to be pre-approved by multiple levels of management up to and including the deputy director
- ▀ Gathering 10-15 signatures took weeks/months
- ▀ Permission had to be obtained before starting any activities

Vulnerability & Threat Assessment Methodology

- ▀ Conduct Reconnaissance
 - ▀ Identify target network (IP address range, Network subnet)
 - ▀ Identify users, investigate user habits, behaviors, etc.
- ▀ Initial Discovery
 - ▀ Pingscan, traceroute, strobe, network mapping, portscanning
- ▀ Develop attack strategies
- ▀ Execute attacks
- ▀ Report findings

What We Did Not Have

We Didn't have...

- Google
- Nessus
- Metasploit
- Nmap
- Wireshark
- SANS
- NAT'ing
- WiFi
- Burp Suite
- Kali Linux
- Snort
- OWASP
- SQLmap
- CME

 Results. Guaranteed.

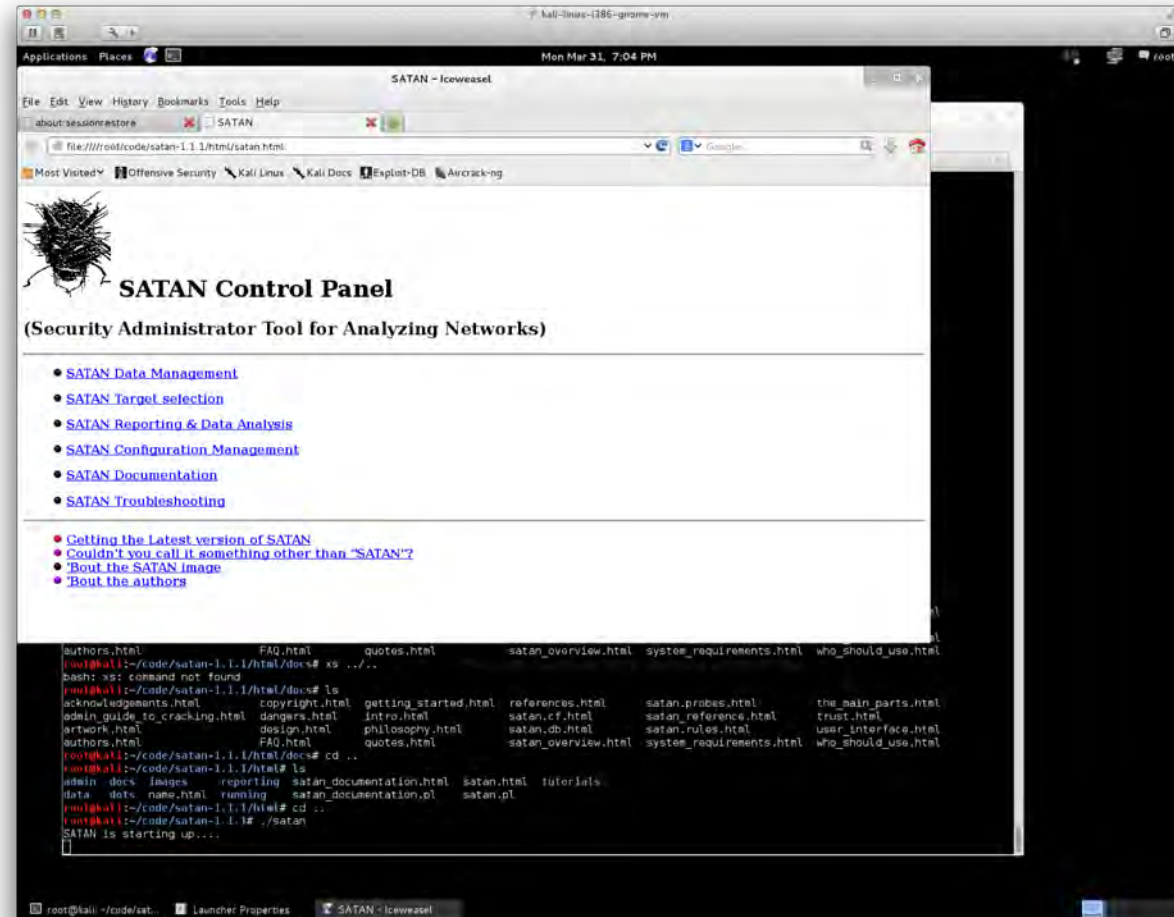
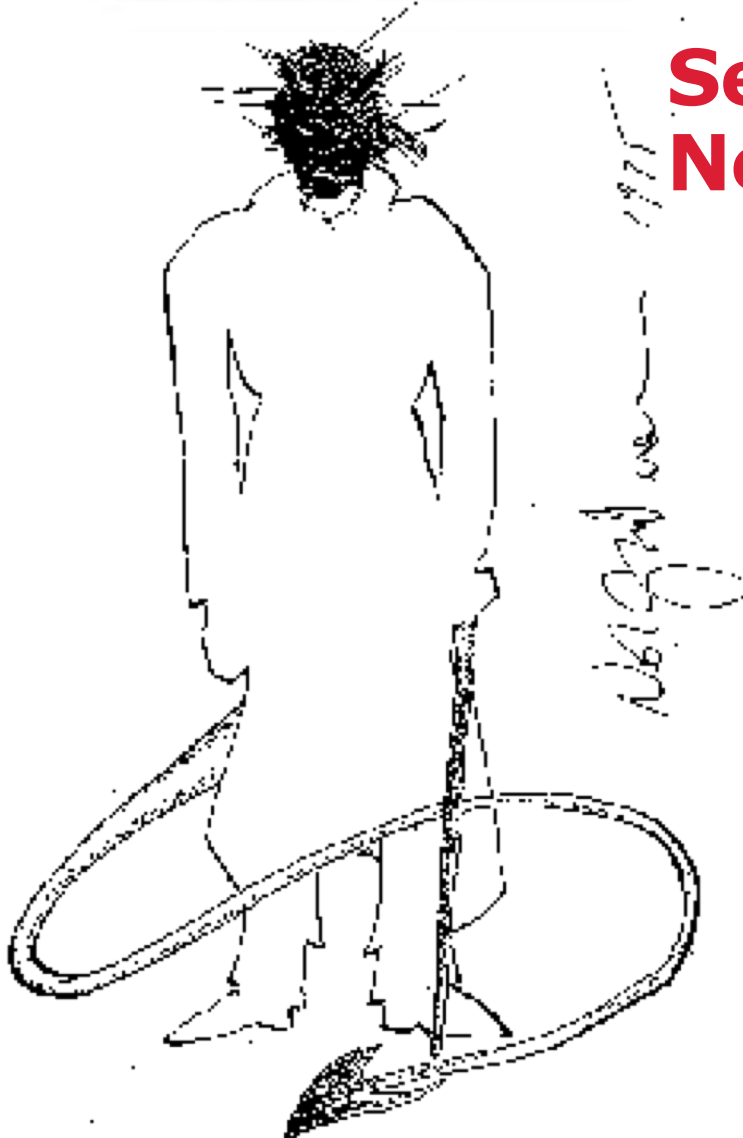
Tradecraft

We used to have to hack systems uphill in the snow!

DISCLAIMER

What you are about to see is likely still classified as "TOP SECRET"
(don't tell anyone I showed this to you)

Security Administrator Tool for Analyzing Networks (SATAN) – released 1995



November 5, 1993

BugTraq created by Scott Chasin
(taken over by Aleph One in May 1996)

Vulnerability Discussion Groups

List: [bugtraq](#)
Subject: [Re: NT floppy driver makes risky assumptions](#)
From: [Aleph One <aleph1 \(\) DFW ! NET>](#)
Date: [1998-09-19 1:35:17](#)
[\[Download message RAW\]](#)

I'll spare everyone from the deluge of replies to this thread. To summarize many people could not reproduce the problem while quite a few could obtain the dreaded BSoD under NT with all kind of floppies (Sun and Solaris boot disks, Mac disks, floppies with lots of CRC errors, etc).

Some people commented the problems went away with SP3, other continue to experience them. Some blamed it on antivirus scanners that read the disk when it is inserted.

If you have a disk with which you can reproduce the problem under SP3 with different types of hardware mail it to Microsoft along with a description of you hardware.

Aleph One / aleph1@dfw.net

<http://underground.org/>

KeyID 1024/948FD6B5

Fingerprint EE C9 E8 AA CB AF 09 61 8C 39 EA 47 A8 6A B8 01

[\[prev in list\]](#) [\[next in list\]](#) [\[prev in thread\]](#) [\[next in thread\]](#)

(CERT) Advisories

CERT(sm) Advisory CA-96.13
July 4, 1996

Topic: ID4 virus, Alien/OS Vulnerability

Concerning the attack on Earth.America.IndependenceDay@SolarSystem:

The CERT Coordination Center has received reports of weaknesses in Alien/OS that can allow species with primitive information sciences technology to initiate denial-of-service attacks against MotherShip(tm) hosts. One report of exploitation of this bug has been received.

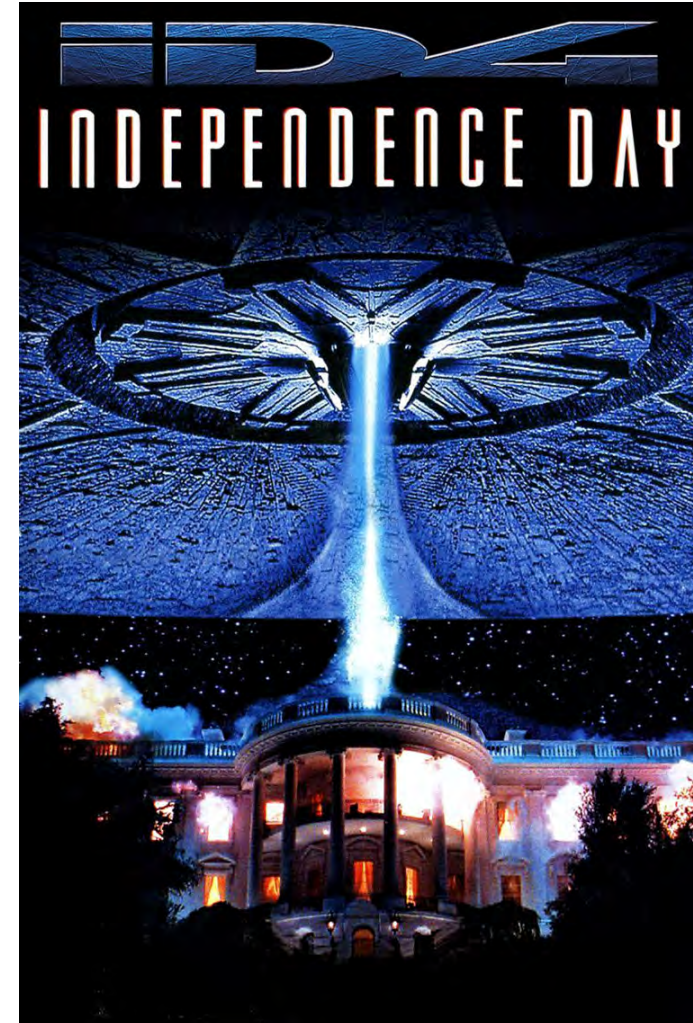
When attempting takeover of planets inhabited by such races, a trojan horse attack is possible that permits local access to the MotherShip host, enabling the implantation of executable code with full root access to mission-critical security features of the operating system.

The vulnerability exists in versions of EvilAliens' Alien/OS 34762.12.1 or later, and all versions of Microsoft's Windows/95. CERT advises against initiating further planet takeover actions until patches are available from these vendors. If planet takeover is absolutely necessary, CERT advises that affected sites apply the workarounds as specified below.

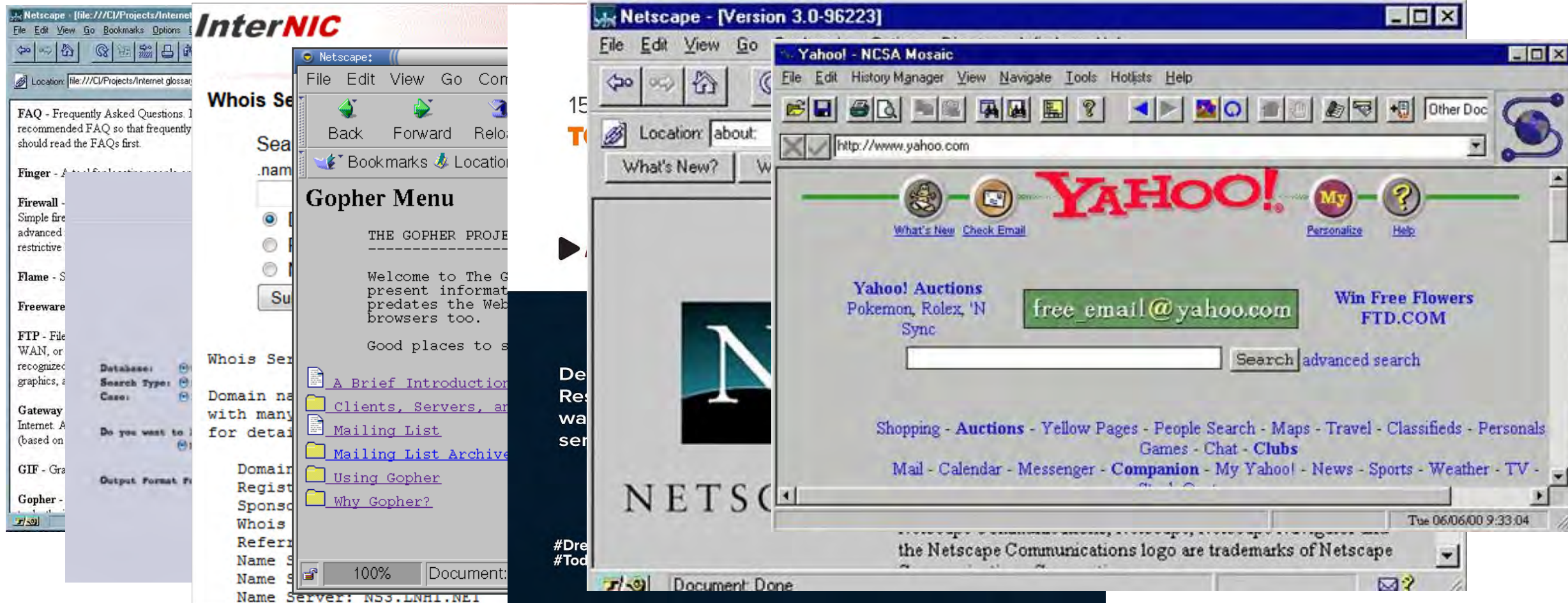
As we receive additional information relating to this advisory, we will place it in

ftp://info.cert.org/pub/cert_advisories/CA-96.13.README

We encourage you to check our README files regularly for updates on advisories that



Open Source Collection



Target Acquisition

strobe(1) - Linux man page List of Class A Networks

Name

strobe - Super optimised TCP port surveyor

Synopsis

strobe [-vVmdbepPAtnSilfsaM] [host1 ... [h

Description

strobe is a network/security tool that locates and describes all listening tcp ports on a (remote) host or on many hosts in a bandwidth utilisation maximising, and process resource minimising manner.

strobe approximates a parallel finite state machine internally. In non-linear multi-host mode it attempts to apportion bandwidth and sockets among the hosts very efficiently. This can reap appreciable gains in speed for multiple distinct hosts/routes.

On a machine with a reasonable number of sockets, *strobe* is fast enough to port scan en

Source: [ARIN](#), [RIPE](#), [APNIC](#)

Compilation: [Adrian Turttschi](#)

Click [here](#) to go back to main overview page.

On this page: Networks 1.0.0.0 through 127.0.0.0

Netnumber	Organization	Net Hand
1.0.0.0	IANA	RESERVED-9
2.0.0.0	Internet Assigned Numbers Authority	IANA
3.0.0.0	General Electric Company	NET-GE-INTEI
4.0.0.0	BBN Planet	NET-SATNET
5.0.0.0	Internet Assigned Numbers Authority	IANA
6.0.0.0	Army Information Systems Center	NET-YPG-NET
7.0.0.0	Defense Information Systems Agency	NET-DISANET
8.0.0.0	Bolt Beranek and Newman Inc.	NET-BBN-NET
9.0.0.0	IBM Corporation	NET-IBM
10.0.0.0	IANA	RESERVED-6
11.0.0.0	DoD Intel Information Systems	NET-DODIIS
12.0.0.0	AT&T ITS	NET-ATT
13.0.0.0	Xerox Palo Alto Research Center	NET-XEROX-3
14.0.0.0	Public Data Network	NET-PDN
15.0.0.0	Hewlett-Packard Company	NET-HP-INTEI

nslookup(1) - Linux man page

Name

nslookup - query Internet name servers interactively

Synopsis

nslookup [-option] [name | -] [server]

Description

Nslookup is a program to query Internet domain name servers. **Nslookup** has two modes: interactive and non-interactive. Interactive mode allows the user to query name servers for information about various hosts and domains or to print a list of hosts in a domain. Non-interactive mode is used to print just the name and requested information for a host or domain.

July 15, 1991

Public release of Crack v2.7a by Alec Muffett

/etc/passwd

```
root:KgQw/rmKNmxyM:0:0:Super-User:/:/bin/csh
shutdown:wYPdZi5U5dyXA:0:0:Shutdown Login:/etc/admin:/etc/admin/shutdown.sh
lp::9:9:Print Spooler Owner:/var/spool/lp:/bin/sh
guest:NpS96PKTr2Wxk:998:998:Guest Account:/usr/people/guest:/bin/csh
schererm:kQUyPBUDdW76s:1110:20:[REDACTED]:/usr/people/schererm:/bin/csh
brownm:n2j8d2EH03YOE:1112:20:[REDACTED]:/usr/people/brownm:/bin/csh
fedex:wxr1V5TIqMSjE:1111:20:[REDACTED]:/usr/people/fedex:/bin/tcsh
anderson:Nv5ydoMxfPkhc:1114:20:David Anderson:/usr/people/anderson:/bin/csh
keyop:xDLAtPt4gxBtw:1116:20:keyop:/usr/people/keyop:/bin/csh
scalesa:3lTO.pjG9bfUk:1117:20:[REDACTED]:/usr/people/scalesa:/bin/csh
sommersb:O9aw6JWELmaQ:1118:20:[REDACTED]:/usr/people/sommersb:/bin/csh
tkirk:uP0MwSptZoN3.:1119:20:[REDACTED]:/usr/people/tkirk:/bin/tcsh
backup:P3QV2/CJ.gXuM:1120:20:[REDACTED]:/usr/local/backup:/bin/csh
```

Set User ID (SUID)

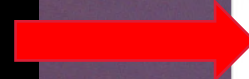
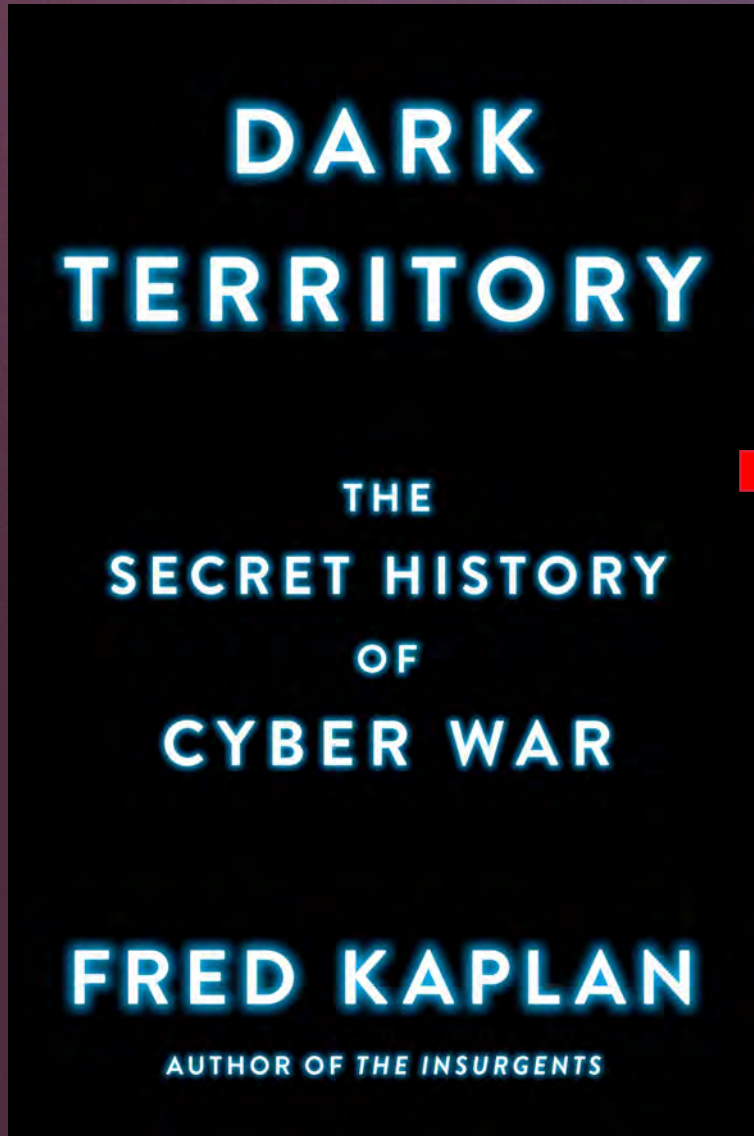
```
aaronkili@tecmint ~ $ find . -perm /4000
./backup.sh
./update.sh
./diskusage.sh
aaronkili@tecmint ~ $ ls -l backup.sh
-rwsrwx--- 1 aaronkili aaronkili 0 Aug  3 22:06 backup.sh
aaronkili@tecmint ~ $ ls -l update.sh
-rwsrws--- 1 aaronkili aaronkili 0 Aug  3 22:06 update.sh
aaronkili@tecmint ~ $ ls -l diskusage.sh
-rwsrws--- 1 aaronkili aaronkili 20 Aug  3 22:04 diskusage.sh
aaronkili@tecmint ~ $
```


We Needed Our Own Space

Origins of the “PIT”



ISSO was relocated near BWI Airport (FANX III)



CONTENTS

<u>CHAPTER 1</u>	<u>"Could Something Like This Really Happen?"</u>	<u>1</u>
<u>CHAPTER 2</u>	<u>"It's All About the Information"</u>	<u>21</u>
<u>CHAPTER 3</u>	<u>A Cyber Pearl Harbor</u>	<u>39</u>
<u>CHAPTER 4</u>	<u>Eligible Receiver</u>	<u>57</u>
<u>CHAPTER 5</u>	<u>Solar Sunrise, Moonlight Maze</u>	<u>73</u>
<u>CHAPTER 6</u>	<u>The Coordinator Meets Mudge</u>	<u>89</u>
<u>CHAPTER 7</u>	<u>Deny, Exploit, Corrupt, Destroy</u>	<u>107</u>
<u>CHAPTER 8</u>	<u>Tailored Access</u>	<u>119</u>
<u>CHAPTER 9</u>	<u>Cyber Wars</u>	<u>145</u>
<u>CHAPTER 10</u>	<u>Buckshot Yankee</u>	<u>171</u>
<u>CHAPTER 11</u>	<u>"The Whole Haystack"</u>	<u>191</u>
<u>CHAPTER 12</u>	<u>"Somebody Has Crossed the Rubicon"</u>	<u>203</u>
<u>CHAPTER 13</u>	<u>Shady RATs</u>	<u>221</u>
<u>CHAPTER 14</u>	<u>"The Five Guys Report"</u>	<u>237</u>
<u>CHAPTER 15</u>	<u>"We're Wandering in Dark Territory"</u>	<u>265</u>

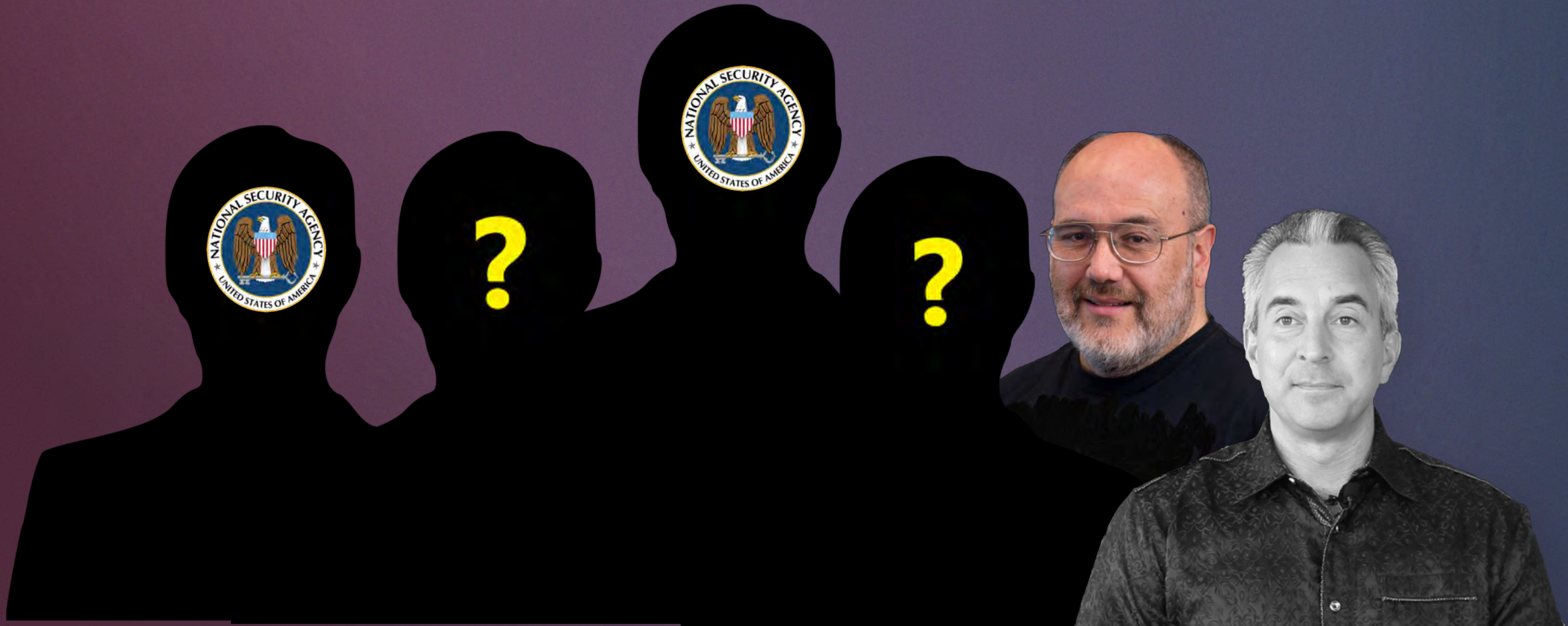
mander's personal computer, sending him false information, thus distorting his view of the battlefield and leading him to make bad decisions, which, in a real war, could have meant defeat.

The NSA had a similar group called the Red Team. It was part of the Information Assurance Directorate (formerly called the Information Security Directorate), the defensive side of the NSA, stationed in FANEX, the building out near Friendship Airport. During its most sensitive drills, the Red Team worked out of a chamber called The Pit, which was so secret that few people at NSA knew it existed, and even they couldn't enter without first passing through two combination-locked doors. In its workaday duties, the Red Team probed for vulnerabilities in new hardware or software that had been designed for the Defense Department, sometimes for the NSA itself. These systems had to clear a high bar to be deemed secure enough for government purchase and installation. The Red Team's job was to test that bar.

Minihan's idea was to use the NSA Red Team in the same way

online

Results. Guaranteed.



The Pit – was really a team of hackers

Growing Pains

The SNAC had its problems (and we were one of them)



National Security Agency | Central Security Service
Defending our Nation. Securing the Future.



[About Us](#) [What We Do](#) [News & Features](#) [Resources For ...](#) [Join our Team](#) [Doing Business With Us](#)

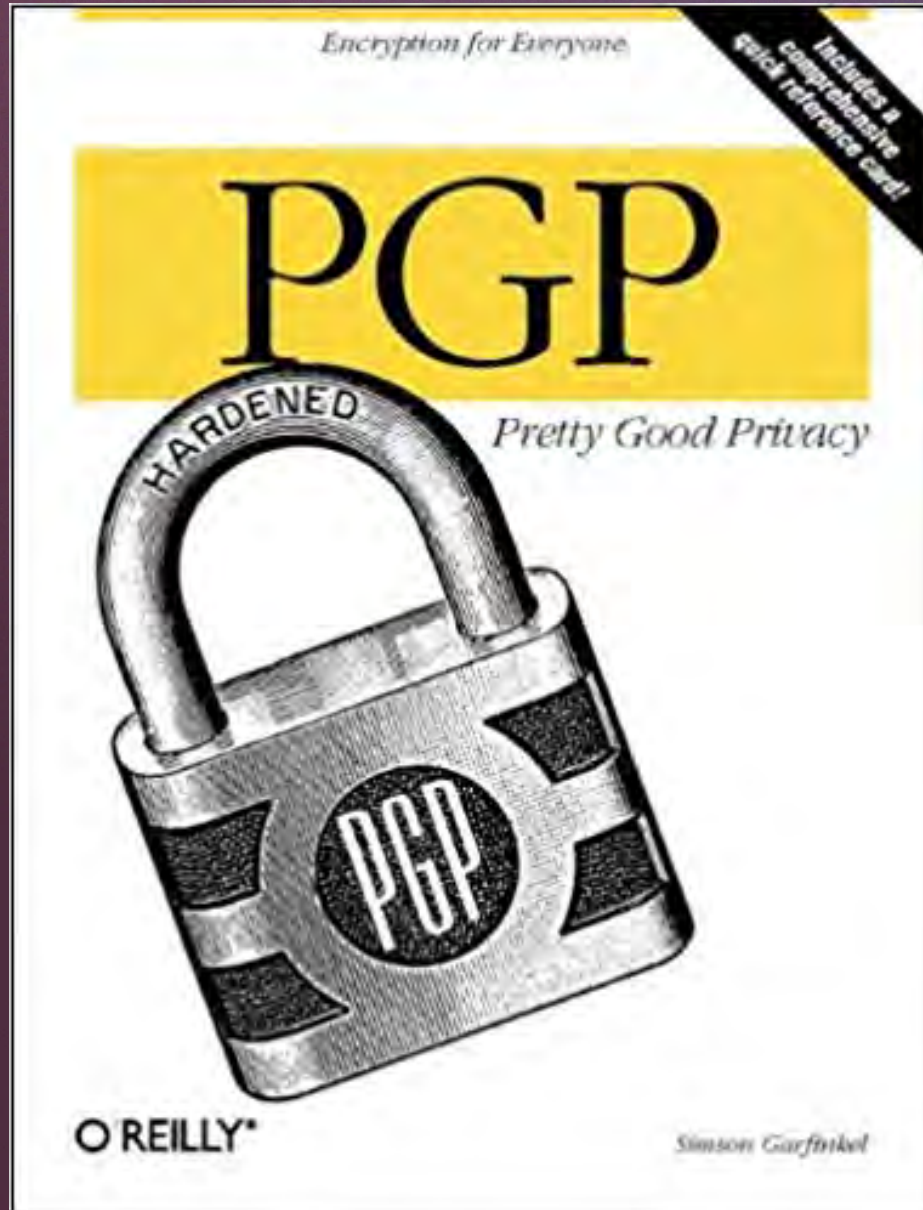
[NSA.gov](#) > [What We Do](#) > [Information Assurance](#)

Information Assurance

The Information Assurance (IA) mission at the National Security Agency (NSA) serves a role unlike that of any other U.S. Government entity. National Security Directive (NSD) 42 authorizes NSA to secure National Security Systems, which includes systems that handle classified information or are otherwise critical to military or intelligence activities. IA has a pivotal leadership role in performing this responsibility, and partners with government, industry, and academia to execute the IA mission.

June 5, 1991

Pretty Good Privacy by Phil Zimmerman released



“All hands on deck!”

**'TOP'
SECRET'**

Primary Attack Tool...

```
Yongs-MacBook-Air:~ mkyong$ ping google.com
PING google.com (74.125.135.139): 56 data bytes
64 bytes from 74.125.135.139: icmp_seq=0 ttl=53 time=49.050 ms
64 bytes from 74.125.135.139: icmp_seq=1 ttl=53 time=47.191 ms
64 bytes from 74.125.135.139: icmp_seq=2 ttl=53 time=45.751 ms
64 bytes from 74.125.135.139: icmp_seq=3 ttl=53 time=46.413 ms
64 bytes from 74.125.135.139: icmp_seq=4 ttl=53 time=44.589 ms
64 bytes from 74.125.135.139: icmp_seq=5 ttl=53 time=10.068 ms
64 bytes from 74.125.135.139: icmp_seq=6 ttl=53 time=46.189 ms
^C
--- google.com ping statistics ---
7 packets transmitted, 7 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 10.068/41.322/49.050/12.822 ms
Yongs-MacBook-Air:~ mkyong$
```

...the Ping Command!

We Had to Talk to the Lawyers

Streamlining the Process

- ▀ Show us/Teach us all of your attack tools
- ▀ AGC(I) to maintain a catalog of all the tools
- ▀ Submit list of tools to be used for the penetration test to be performed
- ▀ AGC(I) blesses the list of tools to be used based on prior knowledge

online

Results. Guaranteed.



TOOL
TIME

Demonstrate tools, techniques, methodology

 Results. Guaranteed.

We Were in Demand

Copyright 1998 Indigo Publications
Intelligence Newsletter
September 17, 1998
SECTION: BUSINESS INTELLIGENCE; UNITED STATES; N. 342
LENGTH: 523 words
HEADLINE: The Hidden Cost of Asking NSA's Help
BODY:

The National Security Agency is being asked increasingly by the government's civilian branches to simulate attacks on their computer systems to evaluate threats even though such tests are in blatant contravention of the country's Computer Security Act, according to officials in Washington. The law assigns responsibility for threat assessments to the National Institute of Standards and Technology (NIST), a civilian agency, and not to NSA, an intelligence organization that answers to the Pentagon.

The practice has stirred concern among many who are familiar with NSA's methods of eavesdropping and breaking into computer systems and who underline the danger of giving the NSA access to systems containing intimate personal details of millions of American citizens, and to many financial institutions and companies.

Word got out. We were in demand.

The Honorable Emmett Paige, Jr.
Assistant Secretary of Defense (C3I)
The Pentagon
Washington, DC 20301

Dear Mr. Paige:

For the past several weeks, officials of the Department of Justice have been discussing with representatives of the Defense Information Systems Agency (DISA) and the National Security Agency (NSA) a strategy for testing the vulnerability of the Department of Justice (DOJ) sensitive computer systems to unauthorized access. As you know, I am strongly committed to ensuring the security of our Justice systems. A systematic testing and assessment of our current vulnerabilities will help us meet this objective.

Therefore, I am formally requesting that DISA and NSA work with us to provide a vulnerability assessment on the security posture of DOJ sensitive systems and network connectivity to include the System Network Architecture (SNA) and Virtual Telecommunications Access Method (VTAM). I am requesting that the assessment begin with the testing and evaluation of the security configurations in the Financial Management Information System, which is used by several components within DOJ.

Department of Justice request for a vulnerability assessment.

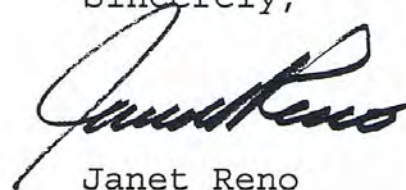
The Honorable Emmett Paige

2

I have enclosed a copy of the banner that is displayed when users log onto the system, as well as a description of the TCP/IP and network connectivity (including SNA and VTAM), to assist the project team in sizing the effort.

Thank you for your attention to this matter.

Sincerely,



Janet Reno

Enclosures

cc: [REDACTED], Chief
Information Systems Security Countermeasures
Defense Information Systems Agency

Director
Chief of Security Analysis Organization
ISSO, National Security Agency



NATIONAL SECURITY AGENCY
FORT GEORGE G MEADE MARYLAND 20755-6000



21 August 1996

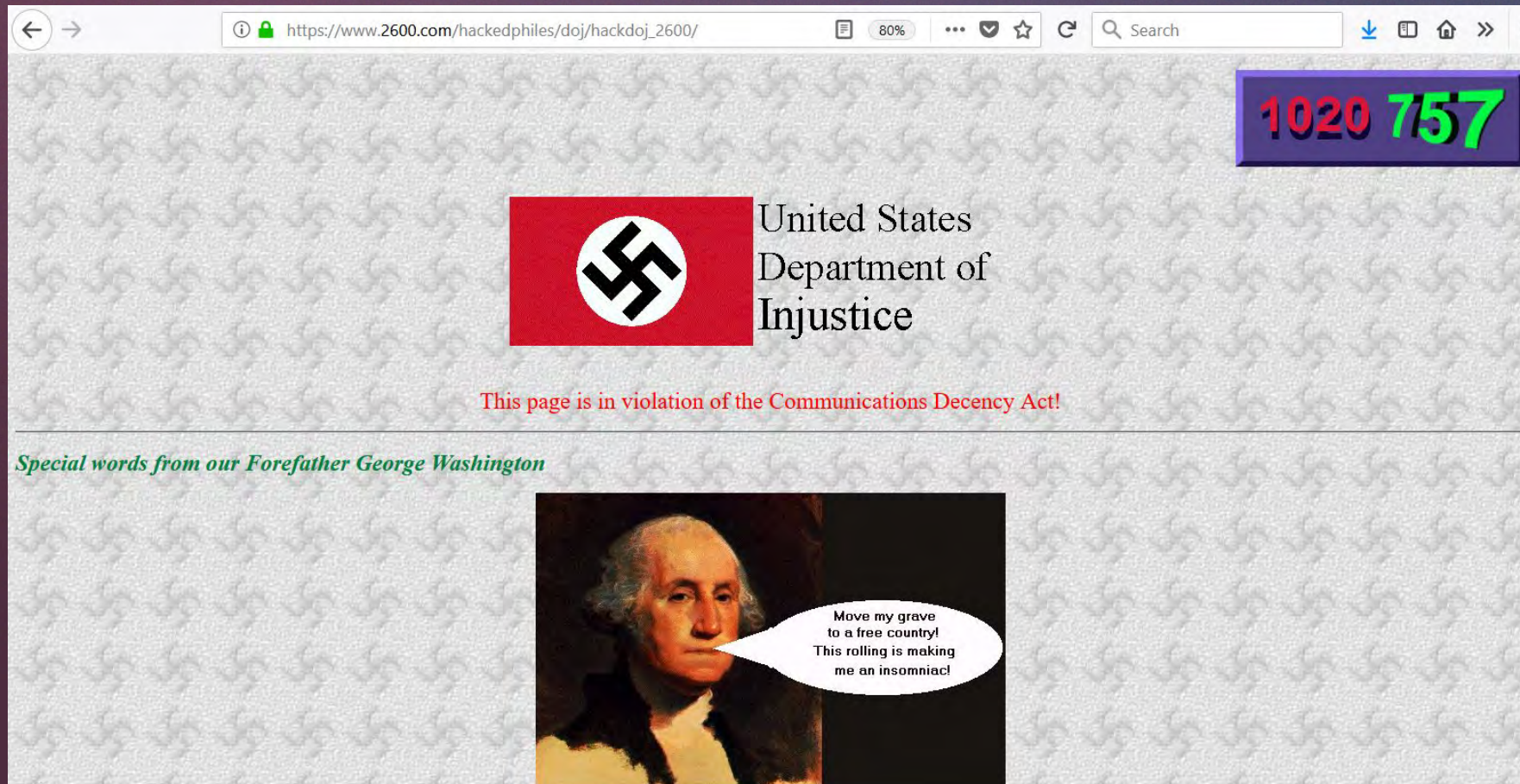
MEMORANDUM FOR ASSISTANT SECRETARY OF DEFENSE FOR COMMAND,
CONTROL, COMMUNICATIONS, AND INTELLIGENCE

SUBJECT: Testing the Vulnerability of the Department of Justice Sensitive
Computer Systems - INFORMATION MEMORANDUM

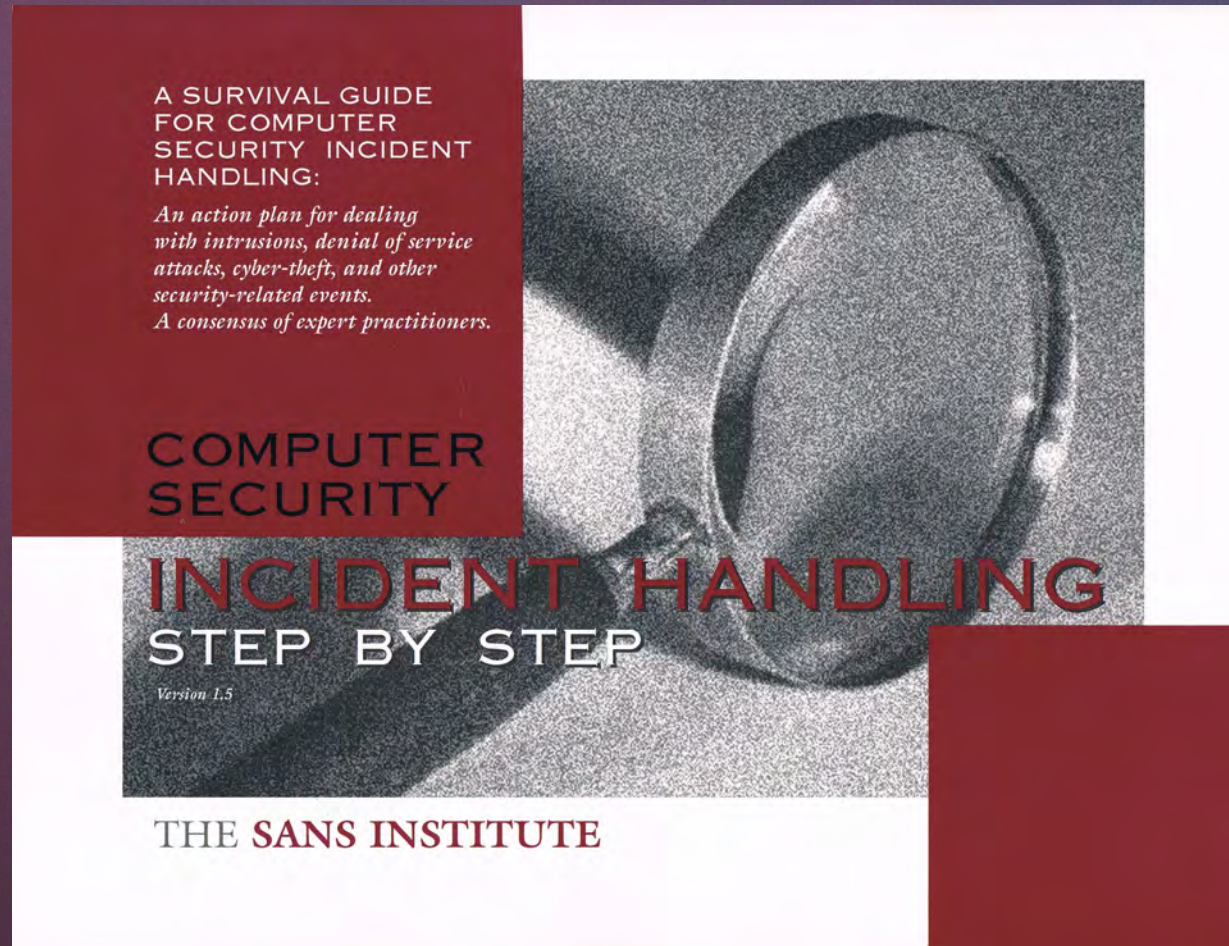
This is in response to the letter from the Attorney General, dated 30 July 1996, formally requesting that NSA support a vulnerability assessment of the security posture of the Department of Justice (DOJ) sensitive computer systems and networks. NSA accepts the request to support DOJ's efforts, beginning with the testing and evaluation of the security configurations in the Financial Management Information System (FMIS).

Analysts from our Systems and Network Attack Center (SNAC) are prepared to conduct "insider" penetration testing this month in accordance with the provisions of the National Telecommunications and Information Systems Security Directive (NTISSD) No. 600, Communications Security (COMSEC) Monitoring, to evaluate the effectiveness of the security configurations in the target DOJ network. The point of contact for this effort is Mr. Jeffrey Man, [REDACTED]

KENNETH A. MINIHAN
Lieutenant General, USAF
Director, NSA



But then this happened...



Lessons learned led to early frameworks for handling incidents

 Results. Guaranteed.

Epilogue

June 9-13, 1997

First joint DoD Red Team Exercise named “Eligible Receiver”

Eligible Receiver '97

FUTURE TENSE THE CITIZEN'S GUIDE TO THE FUTURE. MARCH 7 2016 5:56 AM

FROM SLATE, NEW AMERICA, AND ASU

Inside "Eligible Receiver"

The NSA's disturbingly successful hack of the American military.



By Fred Kaplan



During its most sensitive drills, the Red Team worked out of a chamber called the Pit, which was so secret that few people at NSA knew it existed.

Saul Loeb/Getty Images




<https://www.eiseverywhere.com/ehome/265447/symposiumagenda/>

September 1, 1997

Nmap is first released in Phrack magazine



The Pit still gets together...and sometimes we exchange gifts!

 Results. Guaranteed.

Want to learn more?

I'm around (for now).



Host on Paul's Security Weekly



I'm also a Jedi Master



The Cabal of the Curmudgeons



Phreaker.life Anhackronisms

 Results. Guaranteed.

Questions? Comments?

Will tell more stories for drinks or cigars....

online

Results. Guaranteed.

Jeff Man

Sr. Information Security Consultant
InfoSec Curmudgeon
Online Business Systems

@MrJeffMan

301-310-4275

jman@obsglobal.com

