



Information Assurance Network Assessment

CDT Catherine Johnston

'05, Company A-2



Agenda



- Introduction and Overview
- Tasks
- Methodology
- Lessons Learned



Introduction



Mission of ARL SLAD

White Sands Missile Range, NM

Provide survivability, lethality and vulnerability analysis and evaluation support over the entire life cycle of major Army systems; and help acquire systems that will survive and be lethal in all environments against the full spectrum of battlefield threats.

My purpose at ARL

To aid in the development of tools for use in the Information Assurance Network Assessment (IANA), in order to help active units prepare for information warfare threats.



Introduction

ARL Organization





Army Research Laboratory

Intellectual Crossroads for the Southwestern USA



New Mexico

Los Alamos ◦

◦ Santa Fe

◦ Las Vegas

★ Albuquerque

Portales ◦

Socorro ◦

WSMR

◦ Silver City

Las Cruces ◦



Army Research Laboratory

◦ El Paso

Texas

◦ Las Cruces

New Mexico State University
Physical Science Laboratory
National Aeronautics and Space Administration

White Sands Missile Range (WSMR)

Army Research Laboratory

TRADOC Analysis Center
Army Test and Evaluation Command
Naval Air Warfare Center Weapons Division (NAWCWD)
Center for Countermeasures (CCM)
High Energy Laser Systems Test Facility (HELSTF)
Troy State University

★ Albuquerque

Sandia National Laboratories
Kirtland Air Force Base
Defense Threat Reduction Agency (DTRA)
Air Force Research Laboratory (AFRL)
Air Force Operational Test & Evaluation Center (AFOTEC)
National College of Albuquerque
Southern Illinois University
University of New Mexico
Webster University

◦ Los Alamos

Los Alamos National Laboratory

◦ Santa Fe

The College of Santa Fe
Southwestern College
St. John's College

◦ Las Vegas

New Mexico Highlands University

◦ Socorro

Very Large Array (VLA) Radio Telescopes
New Mexico Institute of Mining & Technology
Energetic Materials Research and Testing Center (EMRTC)

◦ Portales

Eastern New Mexico University

◦ Silver City

Western New Mexico University

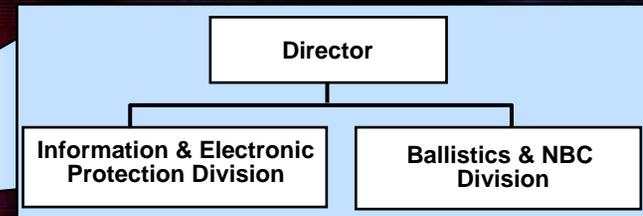
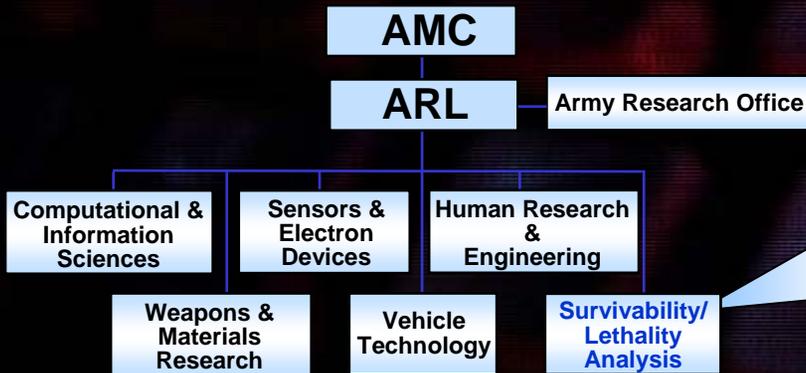
◦ El Paso

Boeing Aircraft
University of Texas at El Paso
El Paso Community College
Texas A & M University
Texas Tech University



Survivability, Lethality, Analysis Directorate (SALAD)

Introduction



Information Operations
Electronic Protection

Conventional Ballistics
Nuclear, Biological, Chemical



Tasks



- Collect information on non-operational exploits in order to determine if they can be used in the IANA
- Download exploits of interest to ARL/SLAD and identify which could be used for IANA
- Catalogue exploit information previously gathered
- Compile exploit code



Methodology



What I did at WSMR



CDT Johnston
(kinda)

Code development
modify, compile, and test



SSARTS db

Exploit information
and source code

Yahoo, Google, hacker sites
CERT sites, vendor sites



Information Security Community



Methodology-Recon



packet storm | http://packetstormsecurity.org/ - Microsoft Internet Explorer

packet storm

about | forums | assessment | defense | papers | magazines | miscellaneous | links

Recent News Headlines

- June 22, 2004 - The Register: Apple Arms The Military
- June 22, 2004 - The Register: Microsoft Sues Over South American Drug Allegations
- June 21, 2004 - Associated Press: Merrill Lynch Put Out Of Google IPO
- June 21, 2004 - Americas Network: Cisco Plans New Software To Prevent Viruses
- June 21, 2004 - Information Week: Top 500 Supercomputers List Shows IBM A Big Winner

Consistently Random

Suggested Listening

Random Quote

Help Support Full Disclosure

Send A Donation

Featured Files

- June 18, 2004: ettercap-0.8.7.0_rc1.tar.gz (1 MD) - Ettercap NO is a network sniffer/interceptor/logger for switched LANs. It uses ARP poisoning and the man-in-the-middle technique to sniff all the connections between two hosts. Features character injec...
- June 14, 2004: hping3-alpha-1.1a.tar.gz (582 K) - hping is a network tool designed to send custom ICMP/ICMPv6 packets and to display target replies like ping. It handles fragmentation and arbitrary packet body and size, and can be used to transfer...
- June 10, 2004: framework-2.11a.tar.gz (487 K) - The Metasploit Framework is an advanced open-source platform for developing, testing, and using exploit code. This release includes 18 exploits and 27 payloads; many of these exploits are either the o...
- June 03, 2004: snort-2.1.11a.tar.gz (2 MD) - Snort is an open source network intrusion detection system, capable of performing real-time traffic analysis and packet logging on IP networks. It can perform protocol analysis, content searching, etc...

Site Updates

June 8, 2004: RSG Needs Have Been Added - RSG Needs have finally been added after many, many

Last 10 Files

- > 04002130d
- > 04002140d
- > 04002150d
- > 04002160d
- > 04002170d
- > 04002180d
- > 04002190d
- > 04002200d
- > 04002210d
- > 04002220d

Last 10 Advertisers

- > 04002100d
- > 04002110d
- > 04002120d
- > 04002130d
- > 04002140d
- > 04002150d
- > 04002160d
- > 04002170d
- > 04002180d
- > 04002190d

Last 10 Exploits

- > code.zip
- > eod-hybrid.txt
- > 04002100d
- > 04002110d
- > 04002120d
- > 04002130d
- > 04002140d
- > 04002150d
- > 04002160d
- > 04002170d

The Hacker's Choice = THC - Microsoft Internet Explorer

The Hacker's Choice

Come to where the fun's play

news | releases | papers | exploits | tools | contact | home

The Hacker's Choice

Welcome to the official THC web site. THC is an acronym for 'The Hacker's Choice' and a group of international experts involved in network and system security. THC was founded in 1995 in Germany, has published over 60 software releases and technical papers and currently is among the top ten security groups worldwide.

Recent News

- Fri, May 28, 2004
Plexwood
We like to welcome our new member Yang from the Republic of China! We are looking forward to his excellent releases and papers. Stay tuned.
- Sat, May 22, 2004
Wilkins
A Ph-Neutral special release of lysins - have fun! Now with a very nice GTK2 GUI was added (thanks to snaboblyte) and a few bugfixes -> Visit the project web site to download Win32, Palm and ARM binaries!
● releases.php
- Tue, May 18, 2004
Van Hauser
Beside that 2/3 of the THC folks will be attending ph-neutral (sorry, no picture posting, no autographs, however we accept free beer and grapes ->), we will also release lysins 4.1 on the conference - sorry with a cool GTK GUI -> Stay tuned.
● http://www.ph-neutral.org/

More about THC

The major focus of THC is to investigate and analyze common security solutions and propose concepts for circumventing security mechanisms. Such concepts range from technical papers demonstrating security aspects of loadable kernel modules to highly efficient network analysis and penetration test software.

THC is a non-commercial group and all releases, papers and even this web site have been developed in the free time of the THC members.

Top Downloads



digital self defense

briefings

training

consulting

BLACK HAT

go to main Black Hat page

http://www.blackhat.com/main.html



Methodology-Recon

Microsoft Excel - listoneexploit

File Edit View Insert Format Tools Data Window Help

Type a question for help

Arial 8

D6 DOS privilege elevation, password harvesting, etc

	A	B	C	D	E	F	G	H	I	J	K	L
1	Name	Victim platform	Type	Abstract	Description							
2	Cfengine	UNIX, WWindow	remote	execute arbitrary code								
3	eznet	LINUX	local remote or both	Dos, privilege elevation, password harvesting, etc	Cryptso.dll contains a 'static' jmp esp in eZnetwork pack from v3.3 to v3.5 jumping to esp, then at esp we jump backward to finally reach the shellcode. The shellcode gives a reverse remote shell. (http://www.exploitdatabase.com/view.php?name=51 copied blurb from)							
4	fcisco	WINDOWS NT	local remote or both	DOS	By sending an oversized TACACS+ packet to CiscoSecure ACS for Windows NT Server it is possible to place the system into an unstable condition that may lead to a denial of service (http://www.cisco.com/warp/public/707/csecureacsnt-pub.shtml copied blurb from)							
5	Fpipe v2.1	WINDOWS										
6	Hydra v3.1	UNIX	local remote or both	DOS privilege elevation, password	parallelized password cracker							
7	ibm-symbolicLink	X WINDOWS										
8	jolt-exp	WINDOWS 2000										
9	manipulate_data		local	A security flaw exists in Microsoft Metadirectory Services (MMS) which may allow a malicious user to access and manipulate data within MMS that should, by design, only be accessible to MMS administrators. (change data)(copied blurb fromMicrosoft Site)								
10	mremap	Linux, SULinux	local remote or both	Dos, privilege elevation, passw	This may allow an attacker to achieve root privileges on an unpatched system, or to disrupt the kernel sufficiently that the system becomes unusable. (http://securecomputing.stanford.edu/alerts/linux-mremap-19feb2004.html blurb copied from) when a client connects to a game server to play a multiplayer game, the server can return a specially crafted server name string that is 260							

Sheet1 Sheet2 Sheet3

Ready NUM

Microsoft PowerPoint - [A...] ExploitList2 listoneexploit

12:31 PM



Methodology-the End Result



SSARTS - SLAD's Security Analysis and Reporting Tool

Search Criteria

Exploits

Remote Local

Attack Platform

Victim Platform

```
ssarts -aLinux(x86) -vCisco -e -r
```

Result Set

Name	Attack OS	Victim OS	Service	Type	Exploit	Info
cisco_brute	Linux/Redhat(x86)	Cisco IOS	Cisco IOS	remote	LAUNCH	BROWSE
cisco-dos	Linux/Redhat(x86)	Cisco IOS	Cisco IOS	remote	LAUNCH	BROWSE
cisco_ios	Linux/Redhat(x86)	Cisco IOS	Cisco IOS	remote	LAUNCH	BROWSE

Find Clear Quit Help



Lessons Learned



- Increased knowledge of information security threats
- Familiarization with Perl , Python, and C
- Increased understanding of networking and network vulnerabilities.



Thanks and Appreciation



- I would like to thank Nora Christianson and ARL SLAD for allowing me the opportunity to participate in this AIAD.



Questions

Contact Information

Catherine.johnston@usma.edu

CFShinigami@aol.com

Cell : 864-617-9570

P.O. Box 1731

West Point, NY 10997



Works Cited



- Google Images search “hacker”
- Ms. Nora Christianson