

# Bio

- Aaron W. Bayles, [aaron.bayles@sentigy.com](mailto:aaron.bayles@sentigy.com)
- BS in Computer Science and post-graduate work in Embedded Linux Programming
- Currently working as a Senior Security Consultant for Sentigy, Inc. in Houston, Texas.
- Experience with INFOSEC spans 8 years, and includes extensive penetration testing, performing security risk assessments, and INFOSEC engineering and design for commercial and government enterprise networks.

# Overview

- What is a Vulnerability?
- What is an Exploit?
- Methodology of a Hack/Crack

# Vulnerability

- Common to all IT environments
- Allows an attacker to:
  - Impersonate another (usually privileged) user
  - Bypass restrictions for accessing data
  - Conduct a denial of service
- These characteristics taken from the Common Vulnerabilities and Exposures (CVE)

# Vulnerability Sources

- Default Configuration
  - Operating System
    - RPC DCOM
    - WINS
  - Application Level
    - MS SQL
    - Veritas BackupExec

# RPC DCOM

- RPC (Remote Procedure Call) – remote invocation, DCOM (Distributed Component Module) – code reuse
- Microsoft acknowledges vulnerability on July 16<sup>th</sup>, 2003
- Exploit code was released the same month
- Exploit used for the MS Blaster worm, which was detected first on August 11<sup>th</sup>, 2003

# RPC DCOM

- Buffer overflow is used to exploit the vulnerable interface between DCOM and RPC
- Once exploited, allows for code execution as Local System credentials
- Once you get Local System, equivalent to Administrator for the local system.
- Blaster should never have spread, as TCP 135, 139 should never pass a network perimeter

# WINS

- WINS (Windows Internet Naming Service) – uses NetBIOS to perform IP lookups
- Microsoft acknowledges vulnerability December 14<sup>th</sup>, 2004
- Vulnerable to a input validation buffer overflow
- Allows remote code execution at the Local System level

# MS SQL

- Microsoft SQL Server 2000 and associated products (MSDE, Microsoft Data Exchange)
- Vulnerability posted by NGSSoftware on July 25<sup>th</sup>, 2002
- Microsoft released patch on July 24, 2002
- Remote code execution as MS SQL service with no authentication required

# MS SQL

- Slammer worm first detected on January 25<sup>th</sup>, 2003
- Infected 75,000 hosts in 10 minutes
- Shut down multiple networks worldwide

# Mis-Configuration

- Occurs on both Operating System and Application levels

# Operating System

- Improper non-authenticated access
- Poor password policy
- Least privilege
- Vulnerable service usage

# Application Level

- Internet Information Services (IIS)
  - Directory Security/Permissions
  - Unwanted Directory Sharing
- Microsoft Word Macro Security
- Internet Explorer

# Non-Authenticated Access

- Not entirely bad, needs to exist for functions such as WWW, public information sharing
- Windows allows for non-authenticated users to enumerate shares and users
- RestrictAnonymous, RestrictAnonymousSAM, EveryoneIncludesAnonymous keys under the HKEY\_Local\_Machine registry hive

# Anonymous Access Keys

- RestrictAnonymous – when 0, (default) shares can be enumerated by non-authenticated users, this allows for an attacker to get a list of available shares
- RestrictAnonymousSAM – when 0, (non-default), local SAM accounts can be enumerated.
- EveryoneIncludesAnonymous – when 0, (non-default) anonymous users inherit permissions granted to the Everyone group (bad idea)

# Password Policy

- Poor password policies open up attack from brute force methods and guesses
- Combine RestrictAnonymousSAM with a poor password policy, then a brute force password attack can be successfully completed in seconds
- Account lockout keeps brute force attacks from being successful in a short amount of time

# Least Privilege

- The principle of least privilege should be used to enforce separation of duties among all users
- Database administrators should have different rights assigned than software engineers or system administrators
- Many times the default groups of “Administrators” are used as “catch-alls” for ease of administration.

# Vulnerable Service Usage

- Plaintext protocols
  - Telnet
  - FTP
  - LDAP
- Improper Use of Services
  - Microsoft DNS for Active Directory
  - Internet Printing Protocol (IPP)

# Internet Information Services (IIS)

- Directory Security – The Code Red worm used directory traversal (../../../../) to pass references through http to cmd.exe
- Directory Sharing – IIS allows the user to share entire folders or drives, giving execute permissions to a variety of programs that run as Local System
- Microsoft Word Macro Security – In the context of Terminal Services, users could open dangerous files, exposing the internal network to a variety of threats

# Internet Explorer (IE)

- Again, in the context of Terminal Services and thin clients, IE provides a vector to system level services (ActiveX) that are easily exploited.
- E-mail messages, malformed URLs, and cross-site scripting are multiple ways of providing malware to a Terminal Server

# What is an Exploit?

- An exploit is anything that takes advantage of a vulnerability to violate the confidentiality, integrity, and availability (CIA) of a system.
- Consists of an attack vector, and a payload
- Can be commonly known and published or a “0-day” (zero-day)

# Attack Vector

- Local
  - Must be executed by a local user to the machine, or placed locally in such a way that it is executed by a local process
  - Usually more difficult to achieve as local access to the system must be gained first, often through deception

# Attack Vector

- Remote
  - Must be executed by sending data to a remote port or host, such that the data is executed exploiting a vulnerability
  - Primary mitigation is to block access to critical services from non-trusted hosts

# Payload

- What is executed when an exploit succeeds
- Usually consists of commands translated into hexadecimal shellcode
- Combining multiple payload types create “blended threats”
  - Virus that uses a remote vulnerability to infect local system resources
  - Worm that is created to spread to other machines
  - Rootkit that is left behind to facilitate future access

# Common Exploit Types

- Buffer Overflow
  - “Stack Smashing” – sending excessive information to a buffer that is not properly bounded, overflowing malicious data into executable memory space
- Race Conditions
  - Occurs when multiple processes are competing for the same resource, first one to the resource wins, possible to inject payload into a trusted memory space
- File System Permissions
  - Improper permission checking can allow links from un-trusted sources to trusted sources to be created.

# Tools for Testing and Detecting Vulnerabilities

- Same tools used by penetration testers, as well as system crackers
- ISS Internet Scanner
- eEye Retina
- Foundstone Enterprise
- Nessus / Tenable
- Metasploit

# Vulnerability Scanners

- Internet Scanner, Retina, and Foundstone are enterprise class products that allow the Security personnel to manage known vulnerabilities and exposures
- In conjunction with proper Risk Management and Exposure Mitigation, critical part of the INFOSEC process

# Tools for Creating and Testing Exploits

- Nessus, Tenable, and Metasploit have the capabilities to use 0-day exploits that are written by community members, or written by the Security personnel themselves
- Metasploit is a tool that is a framework for combining common attack vectors and payloads in a Perl environment
- Metasploit has found a large following in the penetration testing community and allows for INFOSEC neophytes to access an environment for creating and detecting new exploits and vulnerabilities

# Demonstrations

- Enumerate
  - Nessus Scan
  - Nessus Result Analysis
- Exploit
  - MetaSploit Framework
    - Msfconsole
    - Msfweb
    - Msfcli
  - Brute force of Administrator Account
- Compromise
  - Adding User Accounts
  - Rootkit
  - Process Hiding

# Windows Server 2003 Protections

- Kerberos Authentication – Tim McGuffin presented a talk on Kerberos and Server 2003, D7.
- Network Access Quarantine Control
- Public Key Infrastructure (PKI)
- Security Configuration Wizard (SCW) – Introduced in Windows 2003 SP1
- Windows 2003 Stack Protection

# Kerberos Authentication

- Default authentication for Server 2003
- More efficient authentication
- Only send credentials to one server, single-signon
- Encrypted authentication
- Interoperability with other authentication mechanisms

# Network Access Quarantine Control

- Validates Service Pack and patch level
- Checks for anti-virus software and signature dates
- Split-routing disabled
- Firewall status
- Any policy-configurable option, i.e. password-protected screensaver active

# PKI

- Multiple authentication mechanisms
- Integration with strong encryption services
  - Internet Protocol Security (IPSec)
  - Point-to-point Tunneling Protocol (PPTP)
  - Secure Sockets Layer/Transport Layer Security (SSL/TLS)
  - Encrypted File System (EFS)
- Trusted network connectivity
- Confidential e-mail

# Security Configuration Wizard (SCW)

- Disable unneeded services and IIS plugins
- Block ports
- Import security templates
- Implement role-based security policies, i.e. Domain Controllers, Web Servers, Database Servers
- Implemented in Server 2003 SP1

# Windows 2003 Stack Protection

- Valid security attempt, but flawed implementation
- Designed to prevent buffer overflows by using a “canary” value that is written on the return address of valid data. If the buffer is overwritten, so is canary.
- Canary value is checked against lookup when function is called. If values don’t match, no function called.
- David Litchfield of Next Generation Security released paper in September of 2003 detailing how to defeat stack based protection.

<http://www.nextgenss.com/papers/defeating-w2k3-stack-overflow.pdf>

# Conclusions

- As with anything, proper Windows Server 2003 security is a process, not a destination
- Weak passwords and vulnerable remote services are primary targets
- New tools have been released with Server 2003 to improve the security configurations
- Security administrators should routinely audit their own systems, using the same tools that hackers use

# Questions and Answers

- Questions?

# Links

- RPC-DCOM <http://www.microsoft.com/technet/security/bulletin/MS03-026.msp>
- CVE <http://www.cve.mitre.org>
- WINS <http://www.microsoft.com/technet/security/bulletin/MS04-045.msp>
- Code Red  
<http://www.microsoft.com/technet/security/bulletin/MS01-033.msp>
- ISS Internet Scanner  
[http://www.iss.net/products\\_services/enterprise\\_protection/vulnerability\\_assessment](http://www.iss.net/products_services/enterprise_protection/vulnerability_assessment)
- eEye Retina <http://www.eeye.com/html/products/retina/index.html>
- Foundstone Enterprise <http://www.foundstone.com/products/enterprise.htm>

# Links Cont'd

- Nessus <http://www.nessus.org/>
- Tenable <http://www.tenablesecurity.com/products/newt.shtml>
- Metasploit <http://www.metasploit.org>
- Paper Describing 2003 Stack Protection Defeat - <http://www.nextgenss.com/papers/defeating-w2k3-stack-protection.pdf>