# ATTACKS AND THREATS

HEZRON MWANGI
Systems Administrator
hmwangi@kenet.or.ke

10th March 2014

Some Material Borrowed From:
Merike Kaeo
merike@doubleshotsecurity.com
For: NSRC


# Securing The Network - Basic Terms

- Threat – An adversary that is motivated and capable of exploiting a vulnerability
- Vulnerability – A weakness in security procedures, network design, or implementation that can be exploited
- Risk – The possibility that a particular vulnerability will be exploited

# What Are Security Goals?

- Controlling Data / Network Access
- Protecting Information in Transit
- Ensuring Network Availability
- Preventing Intrusions
- Responding To Incidences

kenet
Kenya Education Network

# Security Properties

- Confidentiality – Access to information is restricted to those who are privileged to see it
- Integrity – Having trust that information has not been altered during its transit from sender to intended recipient
- Accountability – Non-repudiation: property of a cryptographic system that prevents a sender from denying later that he or she sent a message or performed a certain action
- Availability – Information or resources are accessible when required

# Security Services

- Authentication – Process of verifying the claimed identity of a device, user and/or application
- Authorization – Rights and permissions granted to a user, device or application that enables access to resources
- Access Control – Means by which authorized user has access to resources
- Encryption – Mechanism by which information is kept confidential
- Auditing – Process that keeps track of networked activity

# Causes of Security Related Issues

- Protocol error – No one gets it right the first time
- Software bugs – Is it a bug or feature ?
- Active attack
    - Targeting specific devices
    - BotNets
    - DDoS [amplification attacks]
- Configuration mistakes – Very common form of problem

# Passive vs Active Attacks

- Passive Attacks
  - Eavesdropping
  - Offline cryptographic attacks
- Active Attacks
  - Replay
  - Man-In-The-Middle
  - Message Insertion
  - Spoofing (device or user)
  - Denial of Service
  - Protocol specific attacks

# What Can Attackers Do?

- Eavesdrop for reconnaissance
- Send arbitrary messages (spoof IP headers and options)
- Replay recorded messages
- Modify messages in transit
- Write malicious code and trick people into running it
- Exploit bugs in software to ‘take over’ machines and use them as a base for future attacks

# Attack Motivation

- Criminal
  - Criminal who use critical infrastructure as a tools to commit crime
  - Their motivation is money
- War Fighting/Espionage/Terrorist
  - What most people think of when talking about threats to critical infrastructure
- Patriotic/Principle
  - Large groups of people motivated by cause be it national pride or a passion aka Anonymous

# Most Common Threats and Attacks

- Opportunistic
  - Port scanning to exploit known vulnerabilities
  - Password cracking
  - Phishing attacks
- Targeted Attacks
  - You have something they want
  - Amplification attacks, spear-phishing
- Advance Persistent Threat (APT)
  - Very skilled attackers aiming at specific targets
  - Will target CPU, memory, bandwidth
  - Creative BotNets

# Mistakes IT People Make

- Connecting systems to the Internet before hardening them.
- Connecting test systems to the Internet with default accounts/passwords
- Failing to update systems when security holes are found
- Using telnet and other unencrypted protocols for managing systems, routers, firewalls, and PKI.
- Giving users passwords over the phone or changing user passwords in response to telephone or personal requests when the requester is not authenticated.
- Failing to maintain and test backups.
- Running unnecessary services : ftpd, telnetd, finger, rpc, mail, rservices
- Implementing firewalls with rules that don't stop malicious or dangerous traffic incoming and outgoing.
- Failing to implement or update virus detection software
- Failing to educate users on what to look for and what to do when they see a potential security problem.

# Malicious Software (Malware) Introduction

- Malware is software used to:
  - disrupt computer operation
  - gather sensitive information
  - gain access to private computer systems.
- Malware can appear in the form of:
  - code
  - scripts
  - active content
  - other software.
- Malware is a general term used to refer to a variety of forms of hostile or intrusive software.

# Malicious Software (Malware) Types

- Several types of malicious code or malware exist:
  - viruses
  - ransomware
  - worms
  - trojan horses
  - logic bombs
  - rootkits
  - keyloggers
  - spyware
  - adware
  - rogue security software
  - other malicious programs
- They usually are dormant until activated by an event the user or system initiates.

# Spread of Malware

- They can be spread by:
  - e-mail
  - sharing media
  - sharing documents and programs
  - downloading things from the Internet
  - they can be purposely inserted by an attacker.

# Malicious Software (Malware) Design

- Malware can be designed to carry out a wide range of malicious activities.
- Most malware are created to:
  - obtain sensitive information
    - credit card data
    - PIN numbers
    - credentials, etc.
  - gain unauthorized access to systems
  - carry out a profit-oriented scheme.

# How Malware Make Money

- Spyware collects personal data for the malware developer to resell to others.
- Malware redirects web traffic so that people are pointed toward a specific product for purchase.
- Malware installs back doors on systems, and they are used as proxies to spread spam or pornographic material.
- Systems are infected with bots and are later used in distributed-denial-of-service attacks.
- Malware installs key loggers, which collect sensitive financial information for the malware author to use.
- Malware is used to carry out phishing attacks, fraudulent activities, identity theft steps, and information warfare activities.

# Increase of Malware and Potency

- Environments are heterogeneous and increase in complexity.
- Everything is becoming a computer (phones, TVs, play stations, power grids, medical devices, etc.), and thus all are capable of being compromised.
- More people and companies are storing all of their data in some digital format.
- More people and devices are connecting through various interfaces (phone apps, Facebook, web sites, e-mail, texting, e-commerce, etc.).
- Many accounts are configured with too much privileged (administrative or root access).
- More people who do not understand technology are using it for sensitive purposes (online banking, e-commerce, etc.).
- The digital world has provided many ways to carry out various criminal activities with a low risk of being caught.

# Malware Components

- It is common for malware to have six main elements, although it is not necessary for them all to be in place:
  - **Insertion** - Installs itself on the victim's system.
  - **Avoidance** - Uses methods to avoid being detected.
  - **Eradication** - Removes itself after the payload has been executed.
  - **Replication** - Makes copies of itself and spreads to other victims.
  - **Trigger** - Uses an event to initiate its payload execution.
  - **Payload** - Carries out its function (that is, deletes files, installs a back door, exploits a vulnerability, and so on).

# Viruses

- A virus is a small application, or string of code, that infects software.
- The main function of a virus is to reproduce and deliver its payload, it requires a host application to do this.
- In other words, viruses cannot replicate on their own.
- A virus infects a file by inserting or attaching a copy of itself to the file.

# Viruses Cont'd

- The virus is just the “delivery mechanism.”
- It can have any type of payload (deleting system files, displaying specific messages, reconfiguring systems, stealing sensitive data, installing a sniffer or back door).
- What makes a software component an actual virus is the fact that it can self-replicate.
- If a malware cannot self-replicate, then it does not fall into the subcategory of a “virus.”

# Worms

- Worms are different from viruses in that they can reproduce on their own without a host application, and are self-contained programs.
- One of the most famous computer worms is Stuxnet, which targeted Siemens supervisory control and data acquisition (SCADA) software and equipment.
- It had a highly specialized payload that was used against Iran’s uranium enrichment infrastructures with the goal of damaging the country’s nuclear program.

# Rootkit

- A rootkit is a set of tools that is placed on a compromised system (the attacker has administrator or root user–level access) for future use.
- The first thing that is usually installed is a back-door program.
- The other common tools in a rootkit allow for credential capturing, sniffing, attacking other systems, and covering the attacker’s tracks.

# Rootkit Cont'd

- Once the rootkit is loaded, the attacker can use these tools against the system or other systems it is connected to.
- The attacker usually replaces default system tools with new compromised tools, which share the same name.
- These are referred to as “Trojaned programs”.
- They carry out the intended functionality but do some malicious activity in the background.
- This is done to help ensure that the rootkit is not detected.

# Rootkit Cont'd

- Rootkits and their payloads have many functions, including concealing other malware (password-stealing key loggers and computer viruses).
- A rootkit might also install software that allows the compromised system to become a zombie for specific botnets.
- Rootkits can reside:
  - At the user level of an operating system.
  - At the kernel level.
  - In a system’s firmware.
  - In a hypervisor of a system using virtualization.

# Rootkit Detection

- Can be difficult because the rootkit may be able to subvert the software that is intended to find it.
- Detection methods include:
  - behavioral-based methods.
  - signature-based scanning.
  - memory dump analysis.
  - Removal can be complicated, especially in cases where the rootkit resides in the kernel.
- Reinstallation of the operating system may be the only available solution to the problem.

# Spyware

- Spyware is a type of malware that is covertly installed on a target computer to gather sensitive information about a victim.
- The gathered data may be used for malicious activities, e.g.,
  - identity theft
  - Spamming
  - fraud, etc.
- Spyware can also gather information about a victim's online browsing habits, which are then often used by spammers to send targeted advertisements.

# Spyware Cont'd

- It can also be used by an attacker to direct a victim’s computer to perform tasks such as:
  - installing software,
  - changing system settings,
  - transfer browsing history,
  - logging key strokes,
  - taking screenshots, etc.

# Adware

- Adware is software that automatically generates (renders) advertisements.
- The ads can be provided through
  - pop-ups,
  - user interface components,
  - screens presented during the installation of updates of other products.
- The goal of adware is to generate sales revenue, not carry out malicious activities, but some adware use invasive measures, which can cause security and privacy issues.

# Botnets

- A “bot” is short for “robot” and is a piece of code that carries out functionality for its master, who could be the author of this code.
- Bots allow for simple tasks to be carried out in an automated manner in a web-based environment.
- While bot software can be used for legitimate purposes (i.e., web crawling), it can be used in a malicious manner.

# Botnets Cont'd

- The bot can send a message to the hacker indicating that a specific system has been compromised.
- When a hacker has a collection of these compromised systems, it is referred to as a botnet (network of bots).
- The hacker can use all of these systems to carry out powerful distributed-denial-of-service (DDoS) attacks or even rent these systems to spammers.
- The owner of this botnet (commonly referred to as the bot herder) controls the systems remotely, usually through the Internet Relay Chat (IRC) protocol.

# How Botnets are used

- A hacker sends out malicious code that has the bot software as its payload.
- Once installed, the bot logs into an IRC or web server that it is coded to contact. The server then acts as the controlling server of the botnet.
- A spammer pays the hacker to use these systems and sends instructions to the controller server, which causes all of the infected systems to send out spam messages to mail servers.

# How Botnets are used Cont'd

- Botnets can be used for
  - spamming,
  - brute force and DDoS attacks,
  - click fraud,
  - fast flux techniques,
  - the spread of illegal material.
- The traffic can pass over IRC or HTTP and even be tunneled through Twitter, instant messaging, and other common traffic types.
- The servers that send the bots instructions and manage the botnets are commonly referred to as command-and-control (C&C) servers, and they can maintain thousands or millions of computers at one time.

# Logic Bombs

- A logic bomb executes a program, or string of code, when a certain set of conditions are met.
- The logic bomb software can have many types of triggers that activate its payload execution, as in time and date or after a user carries out a specific action.
- For example, many times compromised systems have logic bombs installed so that if forensics activities are carried out the logic bomb initiates and deletes all of the digital evidence.
- This thwarts the investigation team’s success and helps hide the attacker’s identity and methods.

# Trojan Horses

- A Trojan horse is a program that is disguised as another program.
- Trojan horses are one of the fastest growing malware types in the world.
- A Trojan horse can
  - set up a back door,
  - install keystroke loggers,
  - implement rootkits,
  - upload files from the victim’s system,
  - install bot software,
  - perform many other types of malicious acts.
- They are commonly used to carry out various types of online banking fraud and identity theft activities.

# Antivirus Software

- Traditional antivirus software uses signatures to detect malicious code.
- The signature is a fingerprint created by the antivirus vendor. It's a sequence of code that was extracted from the virus itself.
- An antivirus software package has an engine that uses these signatures to identify malware.
- The antivirus software scans files, e-mail messages, and other data passing through specific protocols, and then compares them to its database of signatures.
- When there is a match, the antivirus software can quarantine the file, attempt to clean the file (remove the virus), provide a warning message dialog box to the user, and/or log the event.

# Antivirus Detection Types

- **Signature-based/fingerprint** detection - is an effective way to detect malicious software, but there is a delayed response time to new threats.
- **Heuristic detection** - analyzes the overall structure of the malicious code, evaluates the coded instructions and logic functions, and looks at the type of data within the virus or worm.
- It has a type of "*suspiciousness counter*," which is incremented as the program finds more potentially malicious attributes.
- This allows antivirus software to detect unknown malware, instead of just relying on signatures.

# Antivirus Detection Types Cont'd

- **Behavior blocking** - actually allows the suspicious code to execute within the operating system unprotected and watches its interactions with the operating system, looking for suspicious activities.
- **Immunizers** – Products with this type of functionality would make it look as though a file, program, or disk was already infected.
- An immunizer attaches code to the file or application, which would fool a virus into “thinking” it was already infected.

# Antimalware Programs

- Antivirus software is not enough.
- Certain administrative, physical, and technical controls must be deployed and maintained.
- There should be standards outlining what type of antivirus software and antispyware software should be installed and how they should be configured.
- Antivirus information and expected user behaviors should be integrated into the security-awareness program.

# security-awareness program

- Every workstation, server, and mobile device should have antimalware software installed.
- An automated way of updating antivirus signatures should be deployed on each device.
- Users should not be able to disable antivirus software.
- A preplanned malware eradication process should be developed and a contact person designated in case of an infection.
- All external disks (USB drives and so on) should be scanned automatically.

# security-awareness program Cont'd

- Backup files should be scanned.
- Antivirus policies and procedures should be reviewed annually.
- Antivirus software should provide boot virus protection.
- Antivirus scanning should happen at a gateway and on each device.
- Virus scans should be automated and scheduled. Do not rely on manual scans.
- Critical systems should be physically protected so malicious software cannot be installed locally.

# Social engineering

- Social engineering refers to psychological manipulation of people into performing actions or divulging confidential information.
- In a social engineering attack, an attacker uses human interaction (social skills) to obtain or compromise information about an organization or its computer systems.
- A type of confidence trick for the purpose of information gathering, fraud, or system access.

# Social engineering Cont'd

- Phishing is a form of social engineering. Phishing attacks use email or malicious websites to solicit personal information by posing as a trustworthy organization.
- Phishing attacks may also appear to come from other types of organizations, such as charities.

# avoid being a victim

- Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about employees or other internal information.
- Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information.
- Do not reveal personal or financial information in email, and do not respond to email solicitations for this information. This includes following links sent in email.
- Don't send sensitive information over the Internet before checking a website's security.

# avoid being a victim cont'd

- Pay attention to the URL of a website.
- If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly.
- Information about known phishing attacks is also available online from groups such as the Anti-Phishing Working Group (http://www.antiphishing.org)
- Install and maintain anti-virus software, firewalls, and email filters to reduce some of this traffic.
- Take advantage of any anti-phishing features offered by your email client and web browser.

# If You Are The victim

- If you believe you might have revealed sensitive information about your organization, report it to the appropriate people within the organization, including network administrators. They can be alert for any suspicious or unusual activity.
- If you believe your financial accounts may be compromised, contact your financial institution immediately and close any accounts that may have been compromised. Watch for any unexplainable charges to your account.
- Immediately change any passwords you might have revealed.
- Watch for other signs of identity theft.

# Q&A.

?

kenet
Kenya Education Network

kenet
Kenya Education Network

---

# THANK YOU!