قـــــــســــــم الامـــــــــــــــن الـــــــــــــــــــــــســيبرانـــــــــــــــــي

Department of Cyber Security

Subject:

Malicious codes

Class:

THIRD

Lecturer:

Dr. Suha Alhussieny

Lecture: (8)

Model, Recent Worm Attacks

Worm Countermeasures

There is considerable overlap in techniques for dealing with viruses and worms. Once a worm is resident on a machine, antivirus software can be used to detect it.

let us consider the requirements for an effective worm countermeasure scheme:

- **Generality:** The approach taken should be able to handle a wide variety of worm attacks, including polymorphic worms.
- **Timeliness:** The approach should respond quickly so as to limit the number of infected systems and the number of generated transmissions from infected systems.
- **Resiliency:** The approach should be resistant to evasion techniques employed by attackers to evade worm countermeasures.
- **Minimal denial-of-service costs:** The approach should result in minimal reduction in capacity or service due to the actions of the countermeasure software. That is, in an attempt to contain worm propagation, the countermeasure should not significantly disrupt normal operation.
- **Transparency:** The countermeasure software and devices should not require modification to existing (legacy) OSs, application software, and hardware.
- **Global and local coverage:** The approach should be able to deal with attack sources both from outside and inside the enterprise network.

Countermeasure Approaches

A. Signature-based worm scan filtering: This type of approach generates a worm signature, which is then used to prevent worm scans from entering a network / host. This approach is vulnerable to the use of polymorphic worms: Either the detection software misses the worm or, if it is sufficiently sophisticated to deal with polymorphic worms, the scheme may take a long time to react.

B. Filter-based worm containment: This approach is similar to class A but focuses on worm content rather than a scan signature. The filter checks a message to determine if it contains worm code. This approach can be quite effective but requires efficient detection algorithms and rapid alert dissemination.

NETWORK-BASED WORM DEFENSE

The key element of a network-based worm defense is worm monitoring software. Consider an enterprise network at a site, consisting of one or an interconnected set of LANs. Two types of monitoring software are needed:

➢ **Ingress monitors:**

These are located at the border between the enterprise network and the Internet.They can be part of the ingress filtering software of a border router or external firewall or a separate passive monitor.A honeypot can also capture incoming worm traffic.

Note: In computer terminology, a **honeypot** is a computer security mechanism set to detect, or, in some manner, counteract attempts at unauthorized use of information systems. A honeypot is a computer system for trapping hackers or tracking unconventional or new hacking methods. Honeypots are designed to purposely deceive hackers and identify malicious activities performed over the Internet.

➢ **Egress monitors:**

These can be located at the egress point of individual LANs on the enterprise network as well as at the border between the enterprise network and the Internet. In the former case, the egress monitor can be part of the egress filtering software of a LAN router or switch. As with ingress monitors, the external firewall or a honeypot can house the monitoring software.

(Figure 4) shows an example of a worm countermeasure architecture .

The system works as follows (numbers in figure refer to numbers in the following list):

1. Sensors deployed at various network locations detect a potential worm. The sensor logic can also be incorporated in IDS sensors.

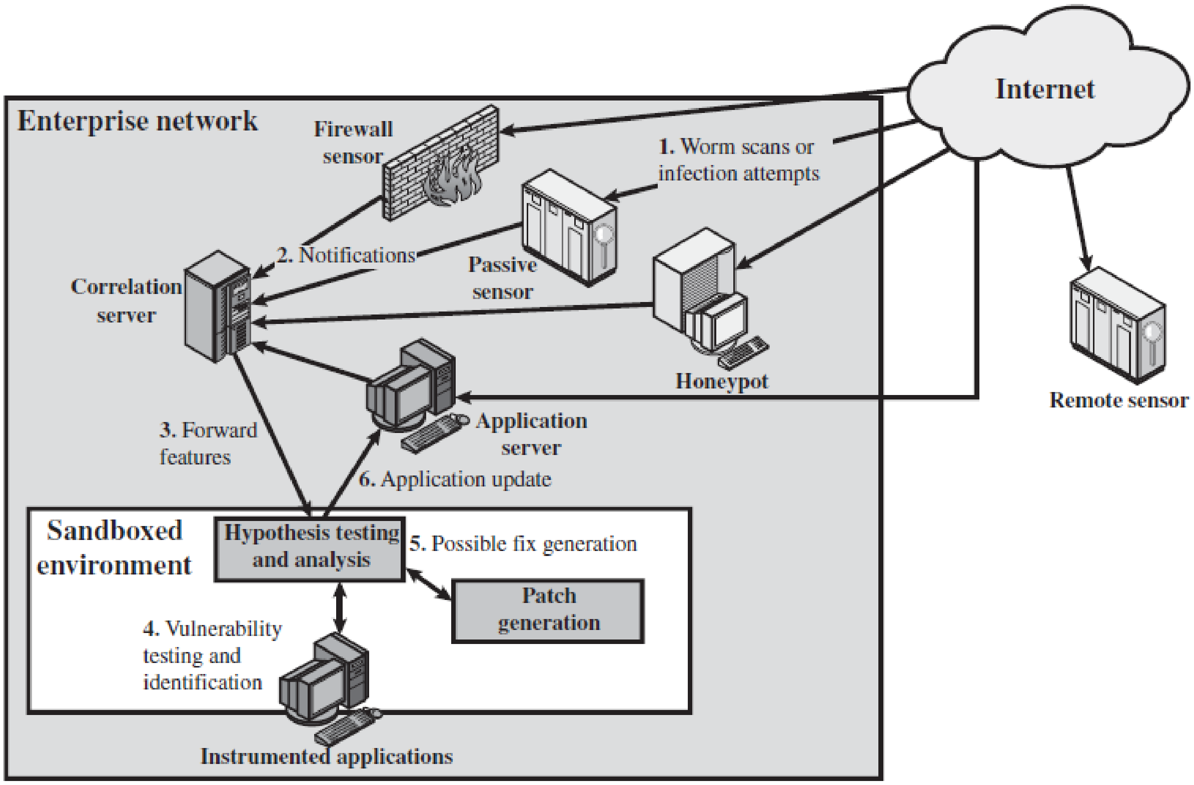
2. The sensors send alerts to a central server that correlates and analyzes the incoming alerts.The correlation server determines the likelihood that a worm attack is being observed and the key characteristics of the attack.

3. The server forwards its information to a protected environment, where the potential worm may be sandboxed for analysis and testing.

4. The protected system tests the suspicious software against an appropriately instrumented version of the targeted application to identify the vulnerability.

5. The protected system generates one or more software patches and tests these.

6. If the patch is not susceptible to the infection and does not compromise the application’s functionality, the system sends the patch to the application host to update the targeted application.



(Figure 4) Placement of Worm Monitors

H.W/

Q1. Which phase of worm propagation is characterized by exponential growth?

A. Slow finish phase B. Initial phase C. Middle phase D. Dormant phase E. Scanning phase

Q2. Which factor does NOT influence the speed of worm propagation?

A. Mode of propagation B. Vulnerabilities exploited C. Similarity to past attacks

D. Type of antivirus used E. Number of hosts available

Q3. The Code Red worm targeted which system?

A. Linux Apache Server B. Cisco Routers C. Microsoft IIS D. UNIX Solaris E. Android Systems

Q4. What additional feature did Code Red II include?

A. Keylogger B. Ransomware module C. Backdoor installation D. Rootkit injector

E. Email spamming

Q5. A worm that spreads through mass emails is classified as:

A. Polymorphic worm B. Mass-mailing worm C. Bluetooth worm D. Multi-exploit worm

E. Stealth worm

Q6. Which type of worm can change its code during each infection?

A. Static worm B. Metamorphic worm C. Ultrafast worm D. Multi-exploit worm

E. Zero-day worm

Q7. Which characteristic allows worms to attack several operating systems?

A. Multi-exploit B. Zero-day C. Multiplatform D. Polymorphic E. Bluetooth-based

Q8. Which worm technology feature accelerates worm spread using prior scans?

A. Polymorphism B. Metamorphism C. Ultrafast spreading D. Zero-day exploit

E. Sandboxing

Q9. CommWarrior spreads using which methods?

A. Wi-Fi and NFC B. Bluetooth and MMS C. Email and FTP D. USB and Wi-Fi E. Cloud sync

Q10. Mobile phone worms typically target:

A. Operating system kernels B. Banking servers C. Web browsers only D. Mobile phones

E. Data centers

Q11. Which countermeasure requirement ensures minimal disruption to normal operations?

A. Generality

B. Transparency

C. Global coverage

D. Minimal denial-of-service costs

E. Resiliency

Q12. Which countermeasure focuses on detecting worm scan signatures?

A. Filter-based containment

B. Zero-day patching

C. Signature-based filtering

D. Metamorphic scanning

E. Encrypted detection

Q13. Which device can act as an ingress monitor?

A. USB drive

B. Internal printer

C. Border router

D. Bluetooth beacon

E. Webcam

Q14. A honeypot is used for:

A. Storing passwords

B. Blocking IP ranges

C. Deceiving attackers

D. Encrypting data

E. Managing firewalls

Q15. Which component correlates and analyzes alerts from sensors?

A. Firewall

B. IDS probe

C. Correlation server

D. Traffic shaper

E. Router

Q16. The protected environment in the countermeasure system is mainly used for:

A. User authentication B. Worm sandboxing C. Email filtering D. Log archiving E. Routing

Q17. What does the protected system generate after analyzing a worm?

A. Antivirus license B. Software patch C. New firewall rules D. User alerts E. Database backups

Q18. Which worms exploit unknown vulnerabilities?

A. Multi-exploit worms B. Multiplatform worms C. Zero-day worms D. Polymorphic worms

E. Bluetooth worms

Q19. Which approach focuses on detecting worm content instead of signatures?

A. Signature-based filtering B. Filter-based containment C. Static detection

D. File hashing E. Password sniffing

Q20. Which monitor observes outgoing traffic?

A. Ingress monitor B. Egress monitor C. Internal scanner D. Bluetooth scanner E. Keylogger

Correct Answers

Q1: B

Q2: D

Q3: C

Q4: C

Q5: B

Q6: B

Q7: C

Q8: C

Q9: B

Q10: D

Q11: D

Q12: C

Q13: C

Q14: C

Q15: C

Q16: B

Q17: B

Q18: C

Q19: B

Q20: B