Malware, intrusion & vulnerabilities

Kresten Jacobsen

Intro to System Security

Goals

Prevention

Detection

Recovery

C-I-A

Confidentiality

Integrity

Availability

Threats

Snooping

Modification

Spoofing

Repudiation of Origin

Denial of Receipt

Delay

Security Policies

Requirements

- Common understanding (implicit / explicit)
- Trust (in people and computers)
- Assumption (that policies are enforced)

Policy types

- Confidentiality
- Integrity Policy
- Availability Policy

Malware types

Computer virus

Polymorphic virus

Trojan horse

Worm

Bot

Logic bomb

Spyware / Adware

Ransomware

CVE - Common Vulnerabilities and Exposure

- Running list of all vulnerabilities
- Maintained by Mitre (not-for-profit org)
- Referenced in patches by vendors to create a closed loop

CVE-ID	
CVE-2019-0708	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

A remote code execution vulnerability exists in Remote Desktop Services formerly known as Terminal Services when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests, aka 'Remote Desktop Services Remote Code Execution Vulnerability'.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- CONFIRM:http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20190529-01-windows-en
- CONFIRM:http://www.huawei.com/en/psirt/security-notices/huawei-sn-20190515-01-windows-en
- CONFIRM:https://cert-portal.siemens.com/productcert/pdf/ssa-166360.pdf
- CONFIRM:https://cert-portal.siemens.com/productcert/pdf/ssa-406175.pdf
- CONFIRM:https://cert-portal.siemens.com/productcert/pdf/ssa-433987.pdf
- CONFIRM:https://cert-portal.siemens.com/productcert/pdf/ssa-616199.pdf
- CONFIRM:https://cert-portal.siemens.com/productcert/pdf/ssa-832947.pdf
- CONFIRM:https://cert-portal.siemens.com/productcert/pdf/ssa-932041.pdf
- MISC:http://packetstormsecurity.com/files/153133/Microsoft-Windows-Remote-Desktop-BlueKeep-Denial-Of-Service.html
- MISC:https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708

Assigning CNA

Microsoft Corporation

Date Entry Created

20181126	Disclaimer: The entry creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

CVSS - Common Vulnerability Scoring System

- Open industry standard
- Scores are calculated based on a formula that depends on several metrics that approximate ease of exploit and the impact of exploit

$$Exploitability = 20 \times AccessVector \times AttackComplexity \times Authentication$$

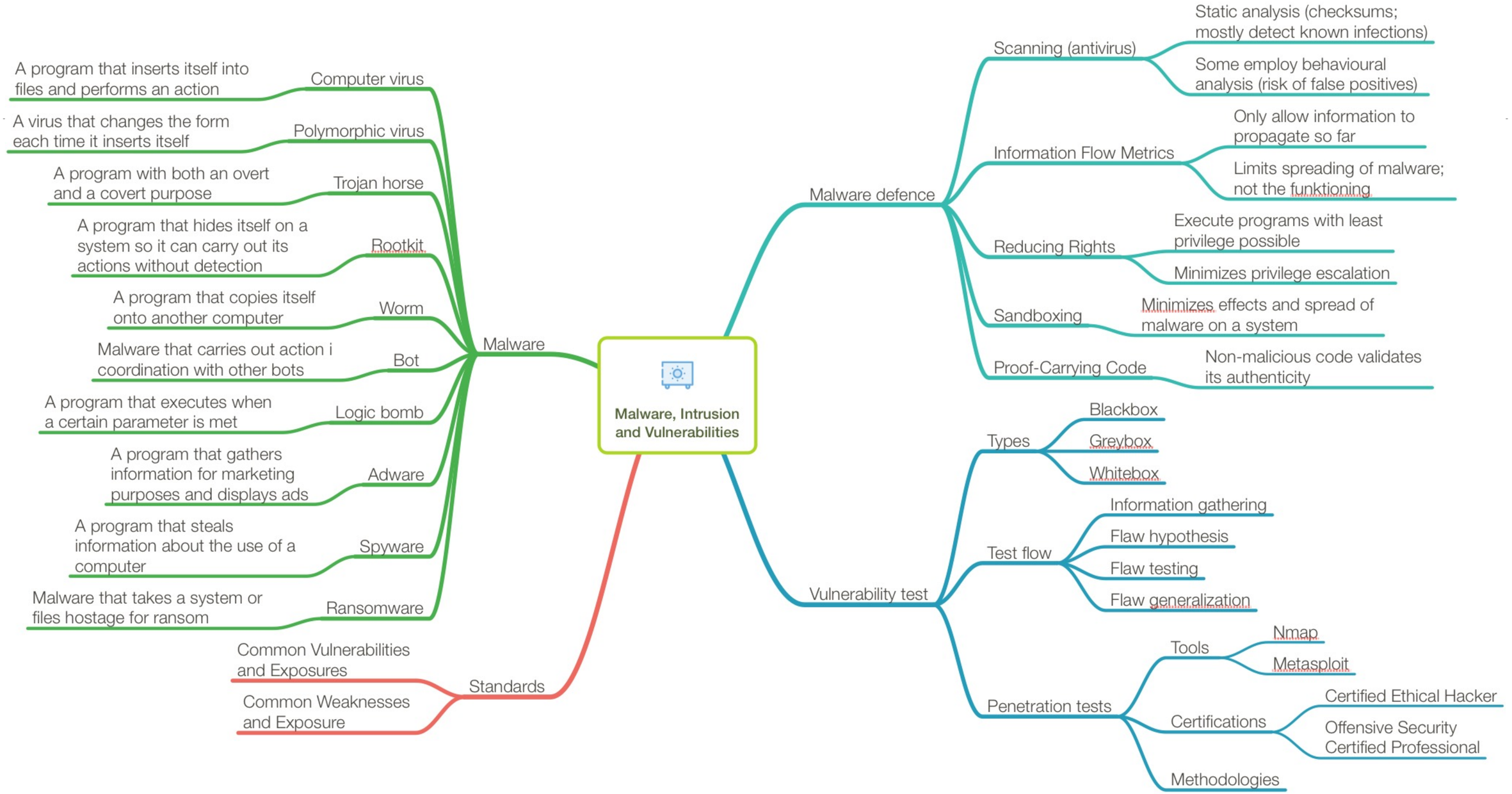
$$Impact = 10.41 \times (1 - (1 - ConfImpact) \times (1 - IntegImpact) \times (1 - AvailImpact))$$

$$f(Impact) = \begin{cases} 0, & \text{if } Impact = 0 \\ 1.176, & \text{otherwise} \end{cases}$$

$$BaseScore = roundTo1Decimal(((0.6 \times Impact) + (0.4 \times Exploitability) - 1.5) \times f(Impact))$$

Malware defence

- Scanning (antivirus)
- Information Flow Metrics
- Reducing Rights
- Sandboxing
- Proof-Carrying Code
- Vulnerability testing


Malware, Intrusion and Vulnerabilities
Malware
Computer virus
A program that inserts itself into files and performs an action
Polymorphic virus
A virus that changes the form each time it inserts itself
Trojan horse
A program with both an overt and a covert purpose
Rootkit
A program that hides itself on a system so it can carry out its actions without detection
Worm
A program that copies itself onto another computer
Bot
Malware that carries out action i coordination with other bots
Logic bomb
A program that executes when a certain parameter is met
Adware
A program that gathers information for marketing purposes and displays ads
Spyware
A program that steals information about the use of a computer
Ransomware
Malware that takes a system or files hostage for ransom
Standards
Common Vulnerabilities and Exposures
Common Weaknesses and Exposure
Malware defence
Scanning (antivirus)
Static analysis (checksums; mostly detect known infections)
Some employ behavioural analysis (risk of false positives)
Information Flow Metrics
Only allow information to propagate so far
Limits spreading of malware; not the funktioning
Reducing Rights
Execute programs with least privilege possible
Minimizes privilege escalation
Sandboxing
Minimizes effects and spread of malware on a system
Proof-Carrying Code
Non-malicious code validates its authenticity
Vulnerability test
Types
Blackbox
Greybox
Whitebox
Test flow
Information gathering
Flaw hypothesis
Flaw testing
Flaw generalization
Penetration tests
Tools
Nmap
Metasploit
Certifications
Certified Ethical Hacker
Offensive Security Certified Professional
Methodologies