Overview of System Security

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

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

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

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

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

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

ATT&CK - Adversarial Tactics, Techniques, & Common Knowledge

Tactics: the adversary’s tactical objective for performing an action

- the 'why'

Tecniques: the method utilized by an adversary achieves a tactical objective

- the 'how'

ATT&CK - Matrix

Comprehensive matrix, containing *tactics* at the top, and *techniques* listed under each tactic.

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data Staged	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	CMSTP	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Information Repositories	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Local System	Data Encoding	Exfiltration Over Command and Control Channel	Endpoint Denial of Service
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Network Shared Drive	Data Obfuscation	Exfiltration Over Other Network Medium	Firmware Corruption
Spearphishing	Execution	BITS Jobs	Dylib Hijacking	Compile After Delivery	Forced	Network Sniffing	Remote	Data from	Domain	Exfiltration	Inhibit

ATT&CK - Usage

- Detections and Analytics
- Threat Intelligence
- Adversary Emulation and Red Teaming
- Assessment and Engineering

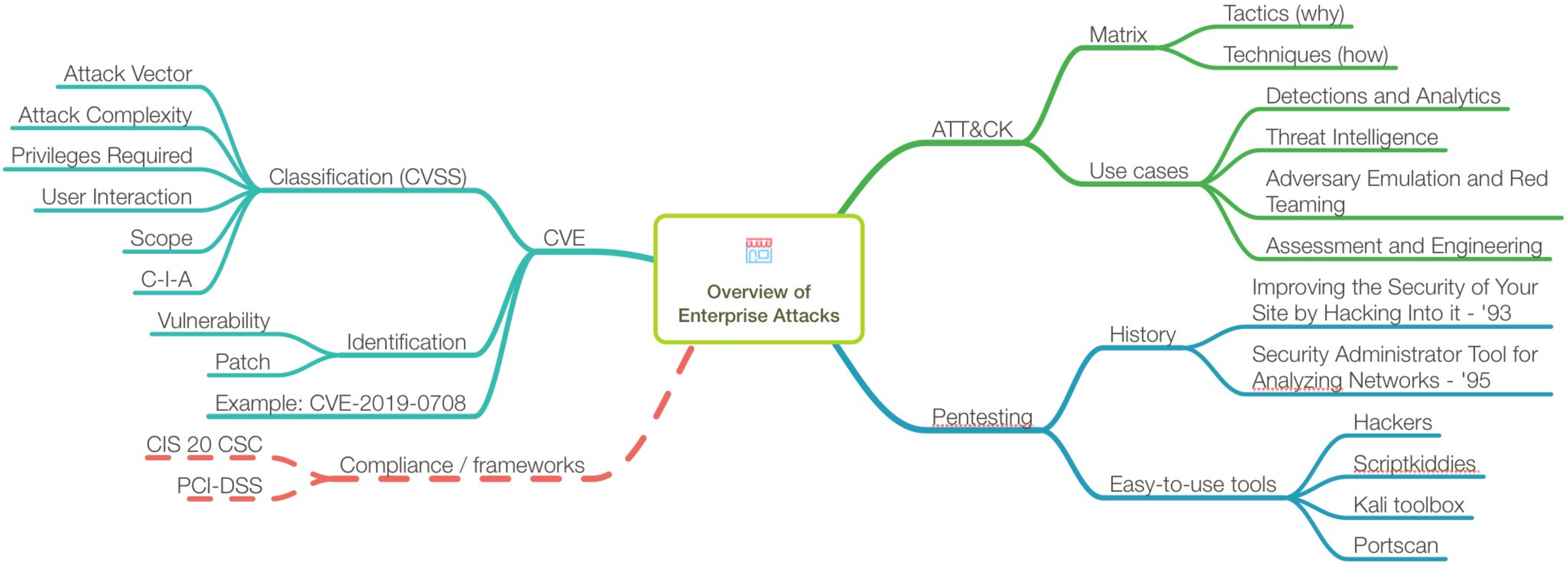
Practical advice - Pentest

History

- 1993 - Improving the Security of Your Site by hacking into it
- 1995 - System Administrator Tool for Analyzing Networks

Easy-to-use tools

- Hackers
- Script kiddies
- Kali - toolbox
- Portscanning - attack surface


Overview of Enterprise Attacks
ATT&CK
Matrix
Tactics (why)
Techniques (how)
Use cases
Detections and Analytics
Threat Intelligence
Adversary Emulation and Red Teaming
Assessment and Engineering
Pentesting
History
Improving the Security of Your Site by Hacking Into it - '93
Security Administrator Tool for Analyzing Networks - '95
Easy-to-use tools
Hackers
Scriptkiddies
Kali toolbox
Portscan
CVE
Classification (CVSS)
Attack Vector
Attack Complexity
Privileges Required
User Interaction
Scope
C-I-A
Identification
Vulnerability
Patch
Example: CVE-2019-0708
Compliance / frameworks
CIS 20 CSC
PCI-DSS