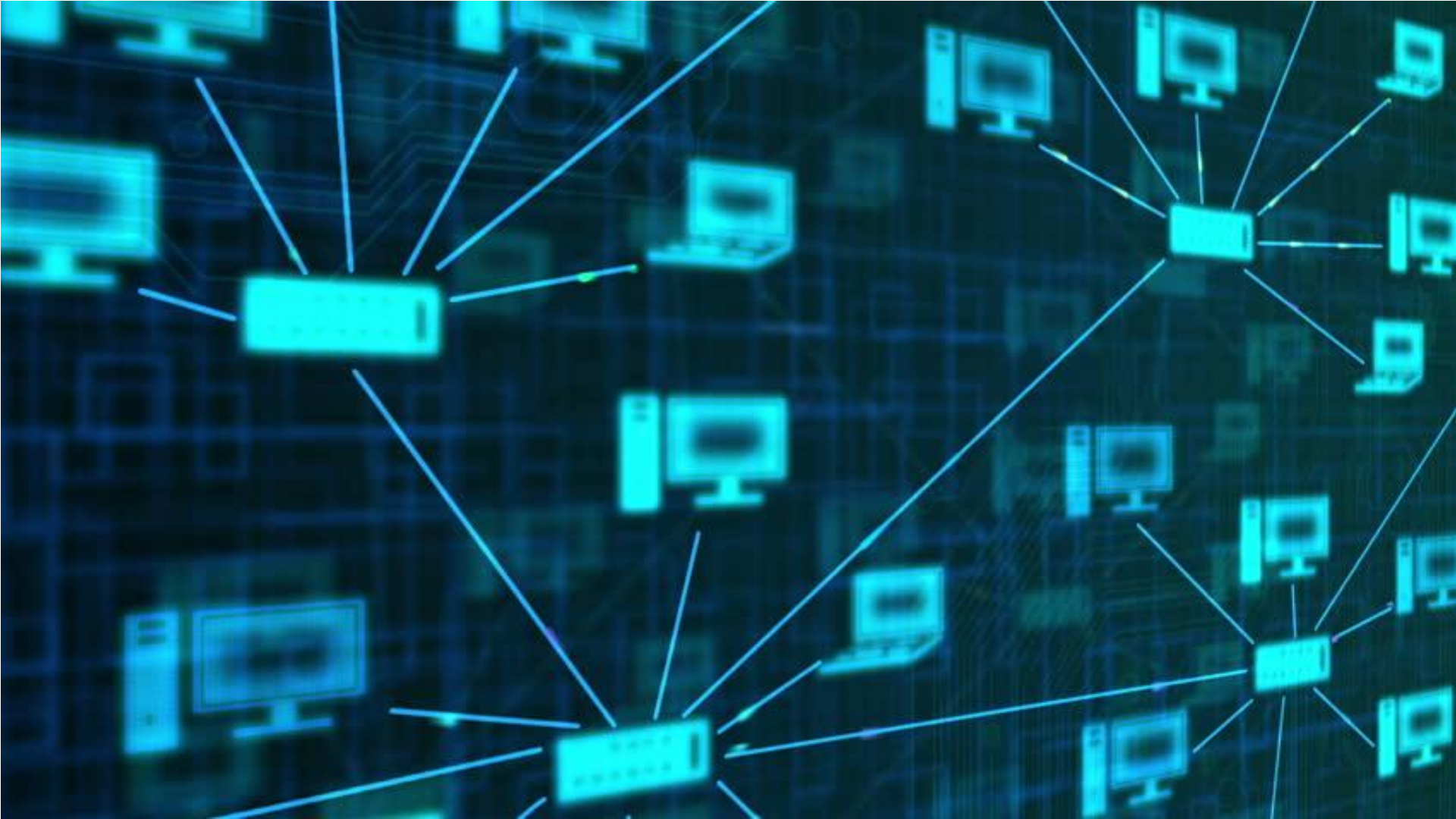
Grafy útokov v kybernetickej bezpečnosti

Autor: Bc. Šimon Javorský

Vedúci: RNDr. JUDr. Pavol Sokol, PhD.

Konzultant: Mgr. Terézia Mezešová

29.11.2017, Košice, PDSI



OpenVAS

Open Vulnerability Assessment System

- Framework pozostávajúci z viacerých nástrojov a služieb
- Ponúka komplexné riešenia na skenovanie a správu zraniteľností

NIST NVD

National Vulnerability Database

- Repozitár štandardizovaných zraniteľností
- Security Content Automation Protocol (SCAP)
- Dáta umožňujú automatizáciu spravovania bezpečnostných hrozieb

Latest Scored Vulns

Showing some of the latest 20 scored vulnerabilities from the NVD, updated once per hour.

Vuln ID & Summary	CVSS Severity
CVE-2017-1000174 — In SWFTools, an address access exception was found in swfdump swf_GetBits(). **Published:** November 16, 2017; 08:29:00 PM -05:00	*V3:* 5.5 MEDIUM *V2:* 4.3 MEDIUM
CVE-2017-0847 — An elevation of privilege vulnerability in the Android media framework (mediaanalytics). Product: Android. Versions: 8.0. Android ID: A-65540999. **Published:** November 16, 2017; 06:29:00 PM -05:00	*V3:* 9.8 CRITICAL *V2:* 7.5 HIGH
CVE-2017-0845 — A denial of service vulnerability in the Android framework (syncstorageengine). Product: Android. Versions: 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A-35028827. **Published:** November 16, 2017; 06:29:00 PM -05:00	*V3:* 7.5 HIGH *V2:* 5.0 MEDIUM
CVE-2017-0835 — A remote code execution vulnerability in the Android media framework (libmpeg2). Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2, 8.0. Android ID: A-63316832. **Published:** November 16, 2017; 06:29:00 PM -05:00	*V3:* 7.8 HIGH *V2:* 9.3 HIGH

CVE-2017-13852 Detail

Current Description

An issue was discovered in certain Apple products. iOS before 11.1 is affected. macOS before 10.13.1 is affected. tvOS before 11.1 is affected. watchOS before 4.1 is affected. The issue involves the "Kernel" component. It allows attackers to monitor arbitrary apps via a crafted app that accesses process information at a high rate.

Source: MITRE **Last Modified:** 11/12/2017 +View Analysis Description

QUICK INFO

CVE Dictionary Entry: CVE-2017-13852
Original release date: 11/12/2017
Last revised: 11/28/2017
Source: US-CERT/NIST

Impact

CVSS Severity (version 3.0):

CVSS v3 Base Score: 3.3 Low
Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N (legend)
Impact Score: 1.4
Exploitability Score: 1.8

CVSS Version 3 Metrics:

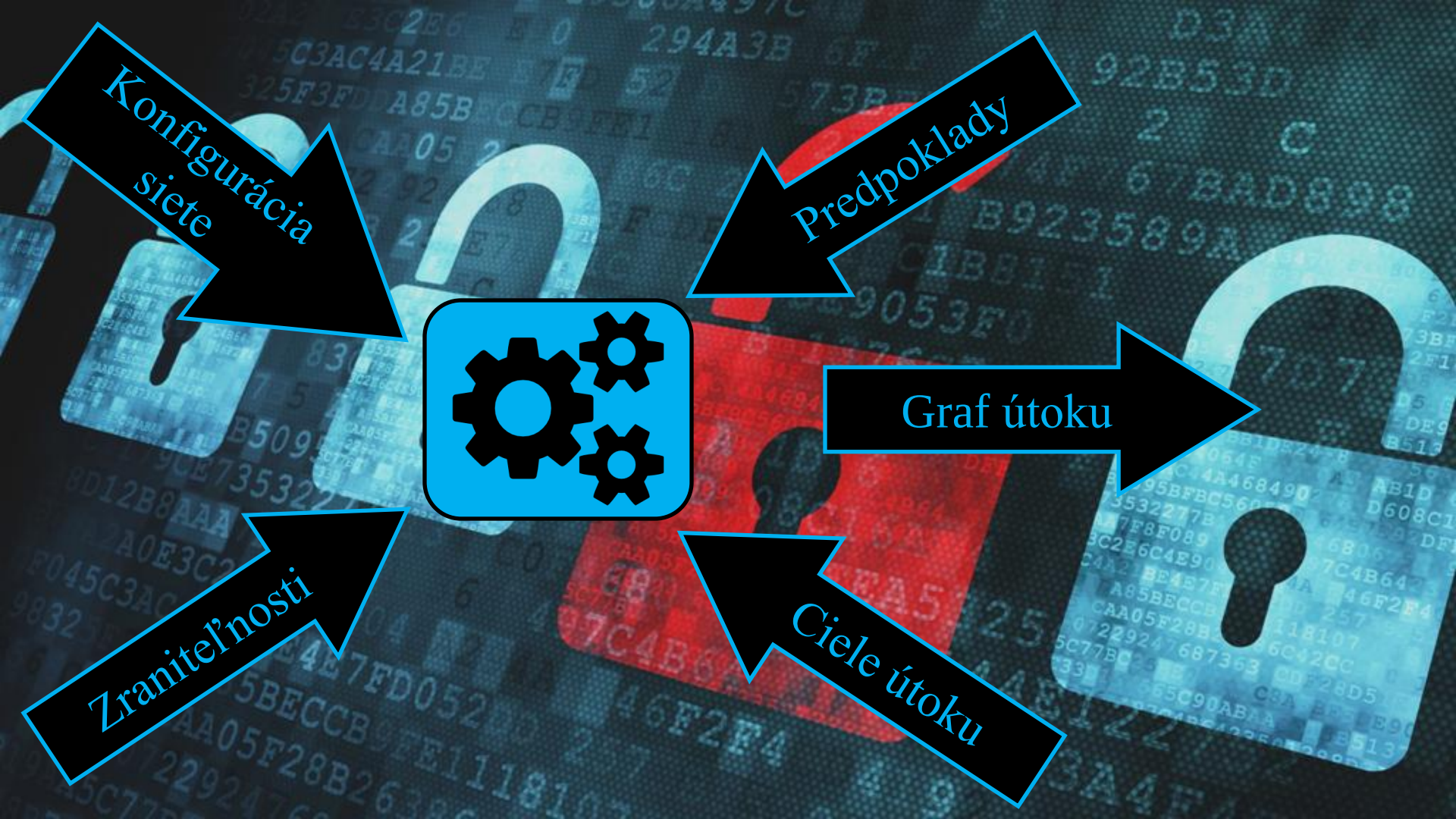
Attack Vector (AV): Local
Attack Complexity (AC): Low
Privileges Required (PR): None
User Interaction (UI): Required
Scope (S): Unchanged
Confidentiality (C): Low
Integrity (I): None
Availability (A): None

CVSS Severity (version 2.0):

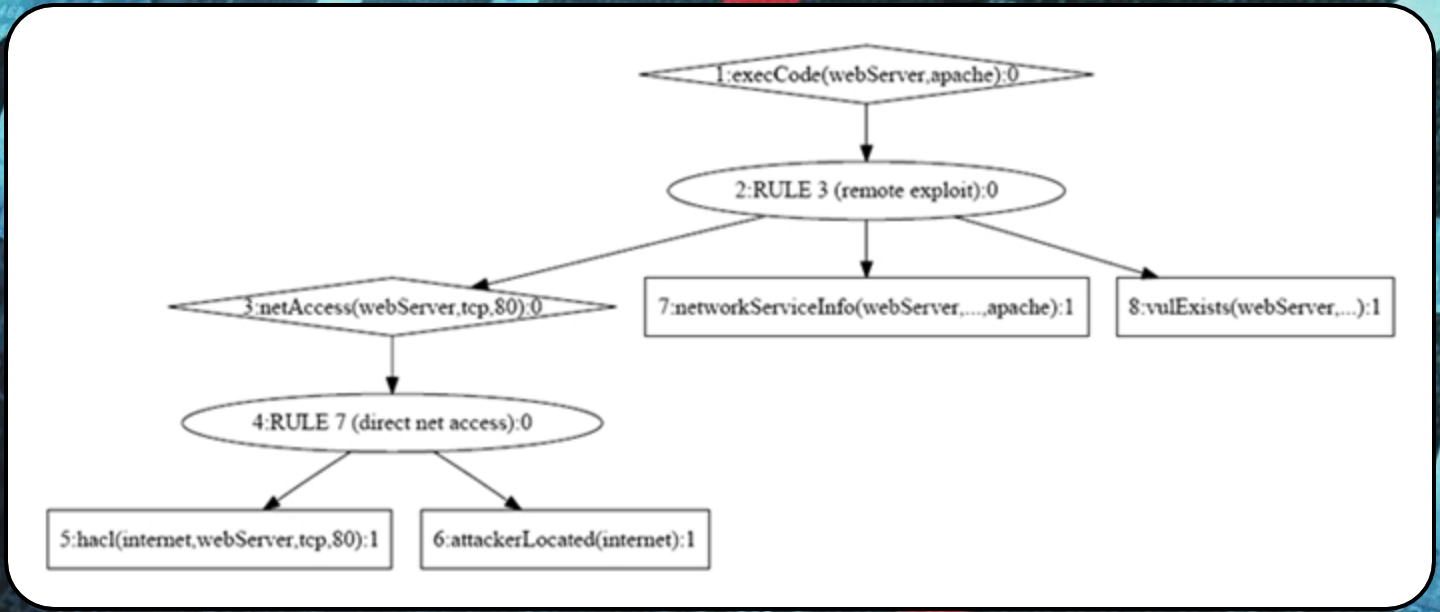
CVSS v2 Base Score: 4.3 MEDIUM
Vector: (AV:N/AC:M/Au:N/C:P/I:N/A:N) (legend)
Impact Subscore: 2.9
Exploitability Subscore: 8.6

CVSS Version 2 Metrics:

Access Vector: Network exploitable - Victim must voluntarily interact with attack mechanism
Access Complexity: Medium
Authentication: Not required to exploit
Impact Type: Allows unauthorized disclosure of information


Konfigurácia siete
Predpoklady
Graf útoku
Zraniteľnosti
Ciele útoku

Graf útoku


1:execCode(webServer,apache):0
2:RULE 3 (remote exploit):0
3:netAccess(webServer,tcp,80):0
7:networkServiceInfo(webServer,...,apache):1
8:vulExists(webServer,...):1
4:RULE 7 (direct net access):0
5:hacl(internet,webServer,tcp,80):1
6:attackerLocated(internet):1

MulVAL

Multi-host, Multi-stage Vulnerability Analysis Language

- Cyber Security Lab, University of South Florida
- Výskumný nástroj pre bezpečnostných technikov a správcov systémov
- Pomáha riadiť konfiguráciu veľkých sietí a kontrolovať bezpečnostné hrozby
- CVSS v2

Ciele

1) Preskúmať možnosti použitia grafov útokov s prihliadnutím na aktuálne bezpečnostné hrozby.

2) Analyzovať a porovnať prístupy ku generovaniu a vizualizácii grafov útokov v kybernetickej bezpečnosti.

3) Navrhnúť a implementovať systém na generovanie a vizualizáciu grafov útokov v kybernetickej bezpečnosti.

Zdroje

- www.openvas.org
- nvd.nist.gov
- www.arguslab.org/software/mulval

- WANG, Lingyu; JAJODIA, Sushil; SINGHAL, Anoop. Network Security Metrics. Springer, 2017.
- KAYNAR, Kerem. A taxonomy for attack graph generation and usage in network security. Journal of Information Security and Applications, 2016, 29: 27-56.
- OU, Xinming; GOVINDAVAJHALA, Sudhakar; APPEL, Andrew W. MulVAL: A Logic-based Network Security Analyzer. In: USENIX Security Symposium. 2005. p. 8-8.

Ďakujem za pozornosť

Otázky?