Manažment bezpečnostných informácií a udalosti pre akademický informačný systém

Autor práce: Bc. Eva Marková

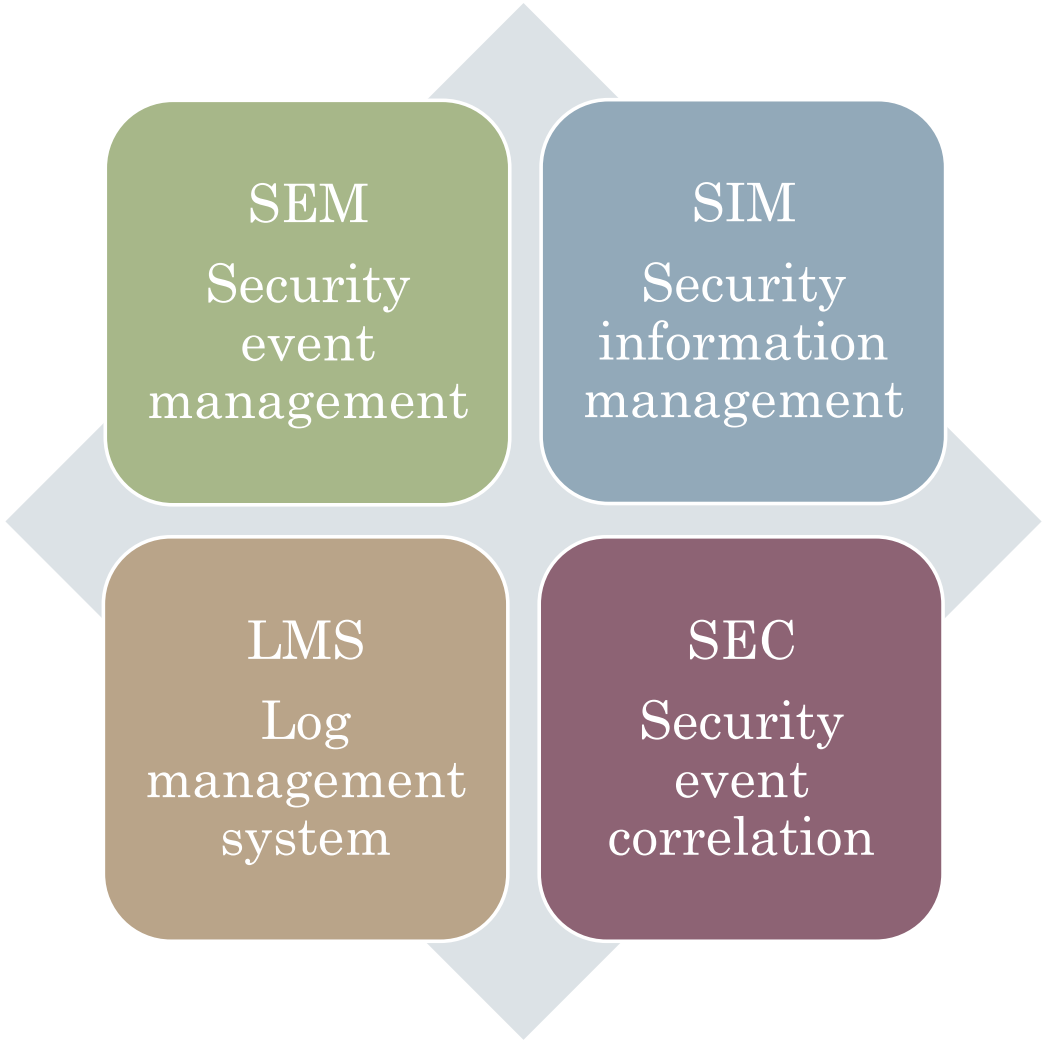
Vedúci práce: RNDr. JUDr. Pavol Sokol, PhD.

Motivácia

- Množstvo hrozieb pre každý informačný systém
  - Krádež, modifikácia, zničenie dát
  - Neoprávnený prístup
- Akademický informačný systém
  - Najkritickejšia infraštruktúra v rámci univerzity
  - Kumulácia množstva osobných údajov

SIEM

Security
Information
and
Event
Management



SIEM

- prístup, ktorý ponúka pozorovanie informačnej bezpečnosti organizácie

Rôzne implementácie:

- Elastic
- Alien Vault
- IBM QRadar
- Splunk

Ciele

1. Analýza aktuálnych prístupov k manažmentu bezpečnostných informácií a udalosti (SIEM)
2. Návrh dátového modelu a pravidiel detekcie bezpečnostných hrozieb pre akademický informačný systém zohľadňujúc bezpečnostné riziká podľa ISO/IEC 27000 a MITRE ATT&CK rámec
3. Návrh, implementácia a optimalizácia SIEM systému pre akademický informačný systém

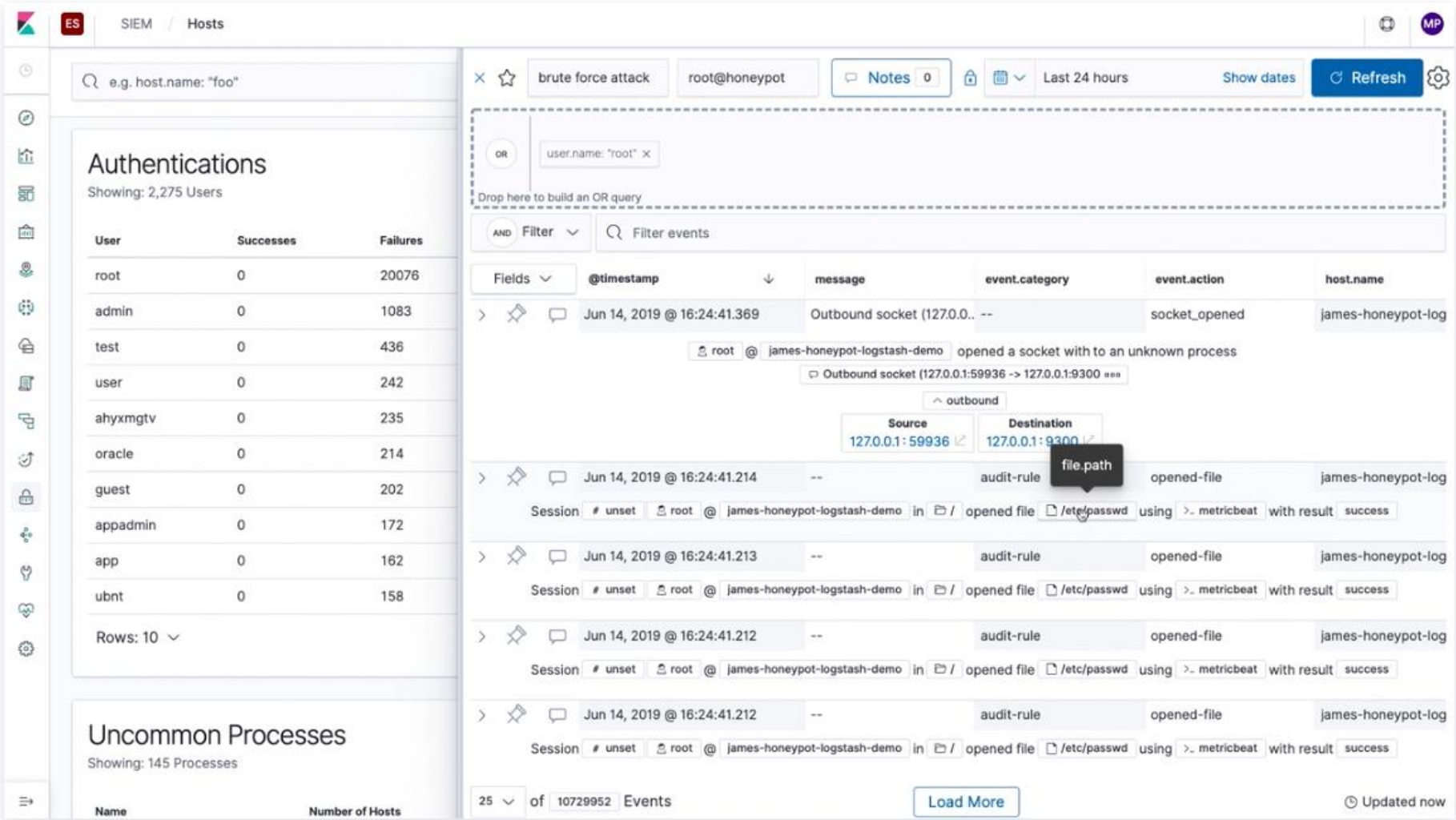
Analýza rizík

ID hrozby	ID zraniteľnosti	Zdroj zraniteľnosti (aktívum)	Popis zraniteľnosti
T01	V01		
T02	V02		
T03	V03		
T04	V04		
T05	V05		
T06	V06		
T07	V07		
T08	V08		
T09	V09		
T10	V10		
T11	V11		
T12	V12		
T13	V13		
T14	V14		
T15	V15		
T16	V16		
T17	V17		
T18	V18		
T19	V19		
T20	V20		
T21	V21		
T22	V22		
T23	V23		
T24	V24		
T25	V25		

MITRE ATT&CK

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	Command-Line Interface	.bash_profile and .bashrc	Exploitation for Privilege Escalation	Binary Padding	Bash History	Account Discovery	Application Deployment Software	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	Exploitation for Client Execution	Bootkit	Process Injection	Clear Command History	Brute Force	Browser Bookmark Discovery	Exploitation of Remote Services	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
Hardware Additions	Graphical User Interface	Browser Extensions	Setuid and Setgid	Compile After Delivery	Credential Dumping	File and Directory Discovery	Internal Spearphishing	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Spearphishing Attachment	Local Job Scheduling	Create Account	Sudo	Connection Proxy	Credentials from Web Browsers	Network Service Scanning	Remote File Copy	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Spearphishing Link	Scripting	Hidden Files and Directories	Sudo Caching	Disabling Security Tools	Credentials in Files	Network Sniffing	Remote Services	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Spearphishing via Service	Source	Kernel Modules and Extensions	Valid Accounts	Execution Guardrails	Exploitation for Credential Access	Password Policy Discovery	SSH Hijacking	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe
Supply Chain Compromise	Space after Filename	Local Job Scheduling	Web Shell	Exploitation for Defense Evasion	Input Capture	Permission Groups Discovery	Third-party Software	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Endpoint Denial of Service

Elastic


ES
SIEM / Hosts
e.g. host.name: "foo"
brute force attack
root@honeypot
Notes 0
Last 24 hours
Show dates
Refresh
OR
user.name: "root"
Drop here to build an OR query
AND Filter
Filter events
Authentications
Showing: 2,275 Users
User Successes Failures
root 0 20076
admin 0 1083
test 0 436
user 0 242
ahyxmgtv 0 235
oracle 0 214
guest 0 202
appadmin 0 172
app 0 162
ubnt 0 158
Rows: 10
Uncommon Processes
Showing: 145 Processes
Name
Number of Hosts
Fields
@timestamp
message
event.category
event.action
host.name
Jun 14, 2019 @ 16:24:41.369
Outbound socket (127.0.0..
socket_opened
james-honeypot-log
root @ james-honeypot-logstash-demo opened a socket with to an unknown process
Outbound socket (127.0.0.1:59936 -> 127.0.0.1:9300
outbound
Source
127.0.0.1:59936
Destination
127.0.0.1:9300
file.path
Jun 14, 2019 @ 16:24:41.214
audit-rule
opened-file
Session unset root @ james-honeypot-logstash-demo in / opened file /etc/passwd using metricbeat with result success
Jun 14, 2019 @ 16:24:41.213
Jun 14, 2019 @ 16:24:41.212
Jun 14, 2019 @ 16:24:41.212
25 of 10729952 Events
Load More
Updated now

Odporúčaná literatúra

1. MURDOCH, D. W. SOC, SIEM, and Threat Hunting (V1.02): A Condensed Guide for the Security Operations Team and Threat Hunter. Independent Publishing, 2019.
2. COLLINS, Michael. Network Security Through Data Analysis: From Data to Action. O'Reilly Media, Inc., 2017.
3. STROM, Blake E., et al. Finding cyber threats with ATT&CK-based analytics. Technical Report MTR170202, MITRE, 2017.

Ďakujem za pozornosť