A PREDICTIVE FRAMEWORK FOR CYBER SECURITY ANALYTICS USING ATTACK GRAPHS

Alexander Patrick / 1706043292

Michael Ariyanto / 1706043235

Nicholas / 1706043254

Dataset used

Service Name	CVE-ID	Exploitability Subscore	Host	AV	AC	AU
Cross site Request	CVE-2014-9385	6.8		Network	Medium	None
Zenoss Core	CVE-2014-9252	2.1		Local	Low	None
Zenoss Core	CVE-2014-9251	5		Network	Low	None
Zenoss Core	CVE-2014-9250	5		Network	Low	None
Zenoss Core	CVE-2014-9249	7.5		Network	Low	None
Zenoss Core	CVE-2014-9248	5		Network	Low	None
Zenoss Core	CVE-2014-9247	4		Network	Low	Single
Zenoss Core	CVE-2014-9245	5		Network	Low	None
Zenoss Core	CVE-2014-6261	9.3		Network	Medium	None
Zenoss Core	CVE-2014-6260	6.8		Network	Medium	None
Zenoss Core	CVE-2014-6259	5		Network	Low	None
Zenoss Core	CVE-2014-6258	5		Network	Low	None
Zenoss Core	CVE-2014-6257	5		Network	Low	None
Zenoss Core	CVE-2014-6256	7.5		Network	Low	None
Zenoss Core	CVE-2014-6255	6.4		Network	Low	None
Multiple XSS	CVE-2014-6254	4.3		Network	Medium	None

Service Name	CVE-ID	Exploitability Subscore	Host	AV	AC	AU
apache	CVE-2014-0098	10	M1			
postgresql	CVE-2014-0063	7.9	M2			
linux	CVE-2014-0038	3.4	M3			
ms-office	CVE-2013-1324	8.6	M3			
bmc	CVE-2013-4782	10	M4			
radius	CVE-2014-1878	10	M4			
HPE Data protector	CVE-2016-2004	9.3		Network	Medium	None
Toshiba 4690	CVE-2014-4876	4.3		Network	Medium	None
read_network_packet	CVE-2014-9751	6.8		Network	Medium	None
ntp_crypto.c	CVE-2014-9750	5.8		Network	Medium	None
CreateBossCredentials	CVE-2014-4875	5		Network	Low	None
Aptexx resident	CVE-2014-4882	7.5		Network	Low	None
Resolveimplicitlevels	CVE-2014-8147	7.5		Network	Low	None
Resolveimplicitlevels	CVE-2014-8146	7.5		Network	Low	None
HP Arcsight Enteprise	CVE-2014-7885	10		Network	Low	None
HP Arcsight Logger	CVE-2014-7884	9		Network	Low	Single

Dataset used

Service Name	CVE-ID	Exploitability Subscore	Host	AV	AC	AU
HP Universal CMDB	CVE-2014-7883	5		Network	Low	None
QPR Portal	CVE-2014-8268	6.4		Network	Low	None
Cross-site-scripting	CVE-2014-8267	4.3		Network	Medium	None
Multiple XSS	CVE-2014-8266	4.3		Network	Medium	None
Panasonic Arbitrator	CVE-2014-9596	4.3		Network	Medium	None
AllefroSoft RomPager	CVE-2014-9222	10		Network	Low	None
ntp_proto.c	CVE-2014-9296	5		Network	Low	None
Multiple Stack-based buffer	CVE-2014-9295	7.5		Network	Low	None
util/ntp-keygen.c	CVE-2014-9294	7.5		Network	Low	None
config_auth	CVE-2014-9293	7.5		Network	Low	None
IPMI 1.5	CVE-2014-8272	5		Network	Low	None
EMC Documentum	CVE-2014-4626	9		Network	Low	Single
SQL Injection	CVE-2014-8248	6.5		Network	Low	Single
Cross-site-scripting	CVE-2014-8247	4.3		Network	Medium	None
Cross site Request	CVE-2014-8246	6.8		Network	Medium	None
Zenoss Core	CVE-2014-9386	6.8		Network	Medium	None

Service Name	CVE-ID	Exploitability Subscore	Host	AV	AC	AU
Mulsiple CSRF	CVE-2014-6253	6.8		Network	Medium	None
Mulriple Stack-based buffer	CVE-2014-8269	7.5		Network	Low	None

Source of Data:
National Vulnerability Database from the National Institute of Standards and Technology from the U.S Department of Commerce
https://nvd.nist.gov/vuln-metrics/cvss

Stochastic Method

Markov Chain

Why? -> widely used in a variety areas such as system performance analysis and dependability analysis

Behavior of the attacker: he/she will choose the vulnerability that maximizes his or her probability of succeeding in compromising the security goal.

The stochastic model is the third layer of the cyber security analytics architecture

The daily transition-probability matrices are calculated using the well-established Frei's Vulnerability lifecycle model

Model Representation

The exploitability score e for vulnerability v is e(v) and calculated as

$$e\ v\ = 20\ \times\ AV \times AC \times Au \qquad e\ v_t\ = temporal\ weight\ \times e\ v$$

The transition matrix $P = \begin{matrix} Q & R \\ 0 & I \end{matrix}$

R = absorbing states, Q = transient states

The transition probability of matrix P $\quad p\ i,j\ = \dfrac{e(v_j)}{\sum_{k=1}^{n} e(v_k)}$

$$Q^n \to 0\ as\ n\ \to \propto$$

$$N = (I - Q)^{-1} = I + Q + Q^2 + Q^3 + \cdots$$

Non-homogenous model

Frei's model is used to calculate the temporal weight score of vulnerabilities as a part of the attack graph model

$$F\ t\ = 1 - \frac{k}{t}^{\ a} \qquad \text{a} = 0.26, \text{k} = 0.00161$$

The Markov model, the covariate is considered as time dependent

$$p\ i,j\ = \frac{e\ v_{t\ j}}{\sum_{l=1}^{n} e\ v_{t\ l}}$$

$$where\ e\ v_t\ = \ 1 - \frac{k}{t}^{\ a} \times e\ v$$

Impact Analysis

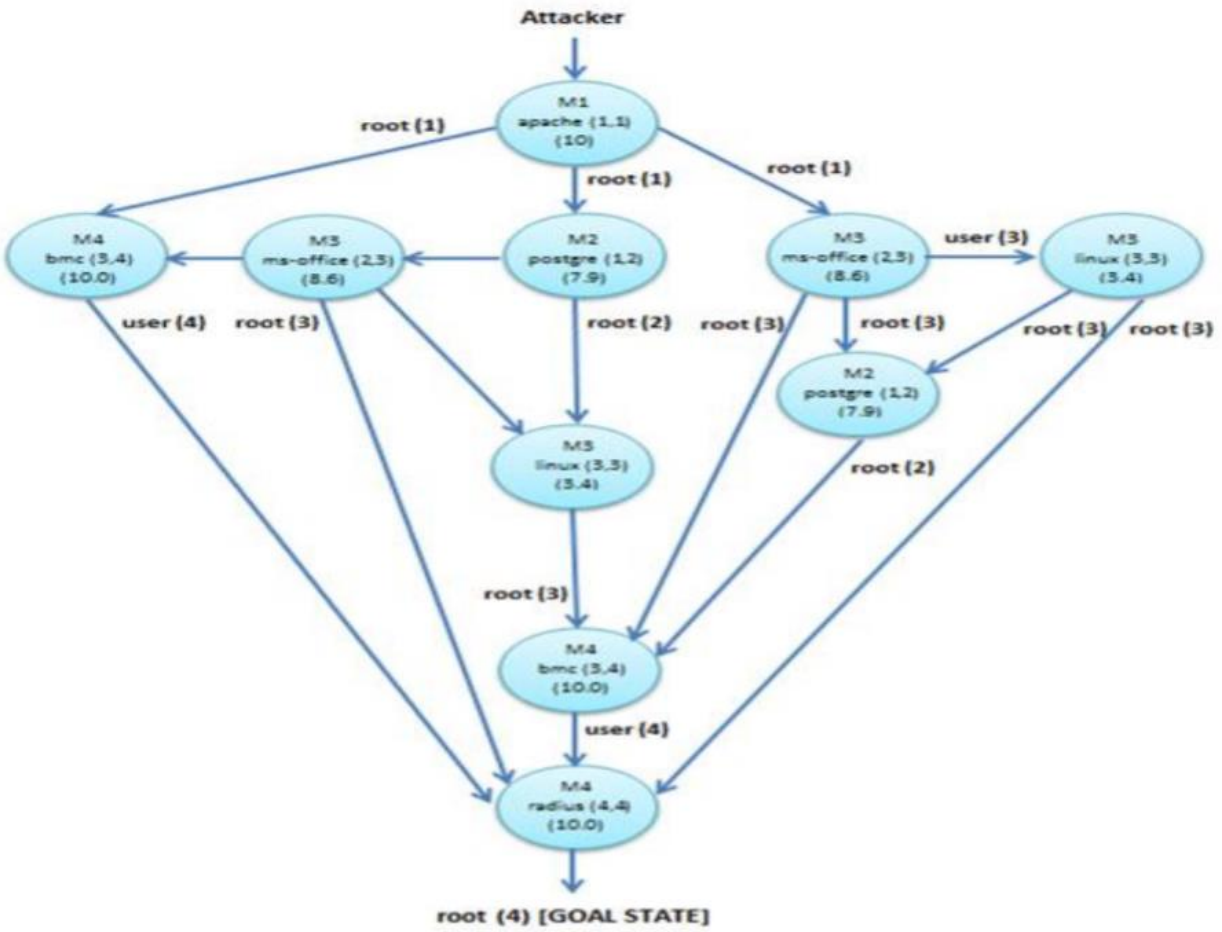
The CVSS standard provides a framework for computing the impact associated with an individual vulnerability (v) using confidentiality impact (c), integrity impact (I) and availability impact (A) measures as follows $Impact\ v\ = 10.41 * (1 - \ 1 - C\ *\ 1 - I\ * (1 - A)$

Given our existing DTMC model, we can represent the Markov Reward process as (ρ, S, P) where S,P is a DMTC and ρ is a reward function for each state.

$$\sum_{i=1}^{n} \rho\ s_i\ .P\{X\ t\ = s_i\} = r.x\ t\ = r.P^t.x(0)$$

Result

Berdasarkan data yang didapatkan dibuatlah sebuah topologi yang mengikuti Absorbing Markov Chain untuk mencari state mana yang paling vulnerable dan harus dilakukan patch



Result

Berdasarkan hasil simulasi yang dilakukan 2000 kali, didapatkan bahwa service bmc pada M4 yang merupakan titik paling sering diexploit dan service linux pada M3 merupakan titik yang paling sedikit diexploit