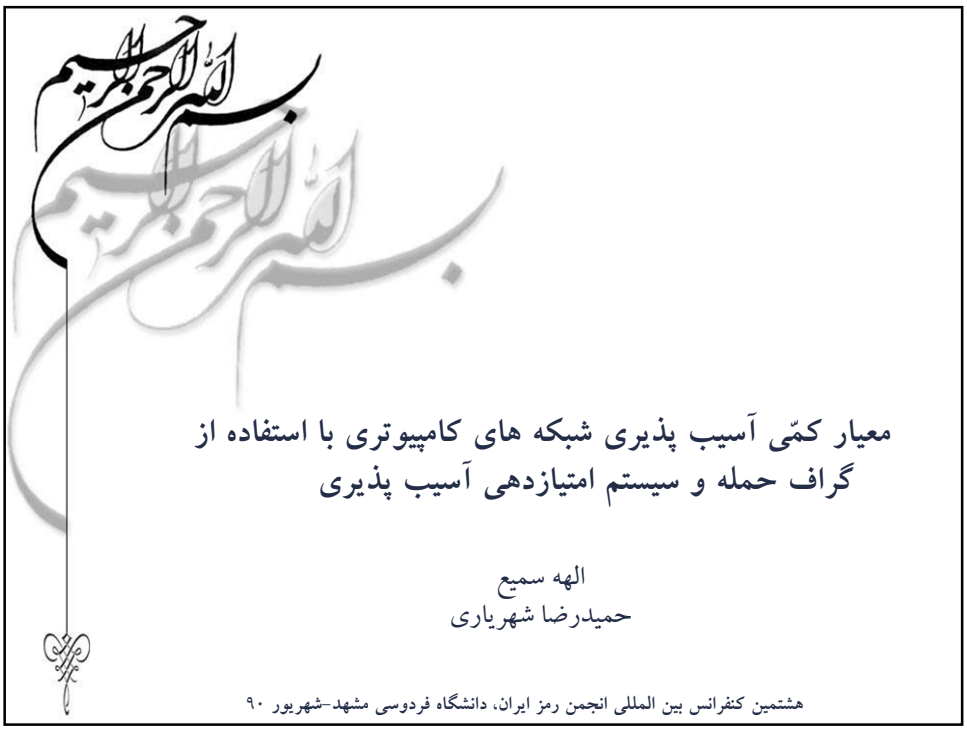


فهرست مطالب

2

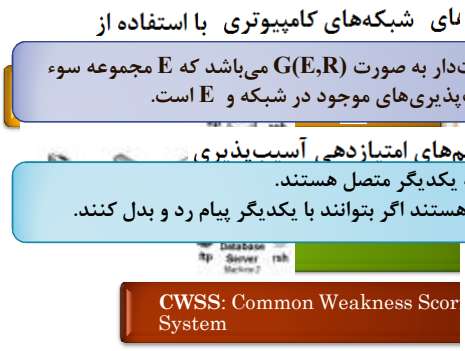
تعاریف اولیه

ای شبکه‌های کامپیوتری با استفاده از

گراف حمله G یک گراف جهت‌دار به صورت G(E,R) می‌باشد که E مجموعه سوء استفاده از آسیب‌پذیری‌های موجود در شبکه و E است.

مجموعه‌ای از کامپیوترها که به یکدیگر متصل هستند.
دو کامپیوتر به یکدیگر متصل هستند اگر بتوانند با یکدیگر پیام رد و بدل کنند.

CWSS: Common Weakness Scor System



خط مشی ا

3

اهمیت تحلیل کمّی آسیب‌پذیری‌ها

- مدیریت سیستم
- ارزیابی میزان امنیت
  - حاصل از پیکربندی‌های مختلف شبکه
  - جهت توسعه مؤثر و بهبود عملکرد سیستم
  - مقایسه و بهبود خط‌مشی‌های امنیتی
- اولویت‌بندی تهدیدها، آسیب‌پذیری‌ها و مخاطرات پیش روی سیستم
- انتخاب راه‌حل‌های امنیتی مناسب
  - قضاوت دقیق‌تر درباره امنیت شبکه و بهبود آن
  - بررسی میزان تأثیر مکانیزم‌های امنیتی و مقایسه آن‌ها

4

مروری بر کارهای پیشین

Pamula, J.; Ammann, P.; Jajodia, S.; Swarup, V.
"A weakest-adversary security metric for network configuration security analysis", 2006

- استفاده از گراف حمله
- معیار نه چندان دقیق مقایسه امنیت پیکربندی‌های مختلف شبکه

Wang, L.; XIslam, S.K.; Long, T.; Singhal, A.; Jajodia, S.
"An attack graph-based probabilistic security metric", 2008

- استفاده از گراف حمله
- احتمال سوء استفاده از آسیب‌پذیری هدف
- حل مسئله دور در گراف حمله

Frigault, M.; Lingyu Wang.
"Measuring Network Security Using Bayesian Network-Based Attack Graphs, Computer Software and Applications" , 2008

Frigault, M.; Wang, L.; Singhal, A.; Jajodia, S.
"Measuring Network Security Using Dynamic Bayesian Networks", 2008

- استفاده از مقادیر CVSS
- در نظر نگرفتن اثر آسیب‌پذیری‌ها بر هم در تخصیص امتیاز
- احتمال رسیدن به هدف حمله

5

CVSS

پایه

پایه

محیطی

خسارت

- محرمانگی
- اصالت
- دسترس‌پذیری

سوء استفاده

- بردار دسترسی
- پیچیدگی دسترسی
- تصدیق هویت

6

مزایای CVSS

- استاندارد کردن رتبه‌های آسیب‌پذیری
  - مستقل از نوع برنامه
  - امکان استفاده از چارچوب امتیازدهی یکسان برای همه آسیب‌پذیری‌ها
  - امکان استفاده از خط‌مشی امنیتی واحد برای مدیریت آسیب‌پذیری‌ها
- چارچوب مشخص و باز
  - مشخص بودن جزئیات کامل مربوط به مشخصه‌های امتیازها

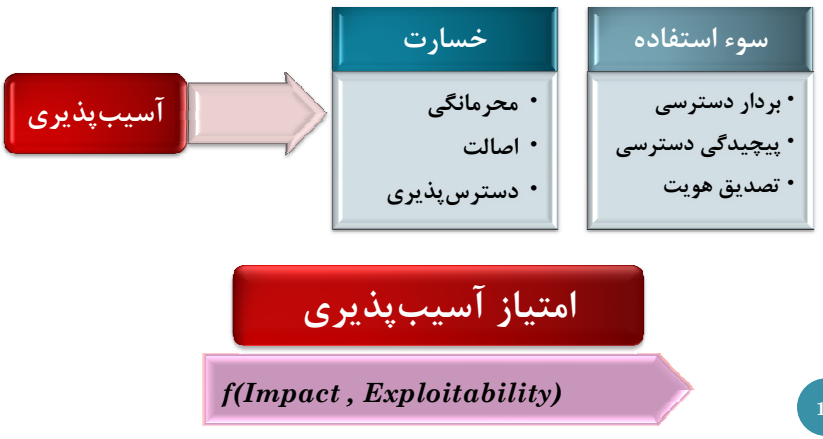
8

محدودیت های CVSS در تحلیل آسیب‌پذیری‌های شبکه

- عدم ارائه راه‌حل جهت بدست آوردن یک امتیاز کلی برای سیستم‌ها
- مستقل بودن امتیاز آسیب‌پذیری‌ها
  - **اثر آسیب‌پذیری‌ها برهم قابل چشم پوشی نیست**
- اثر مشترک سوء استفاده از آسیب‌پذیری‌ها در سیستم
  - **امتیاز آسیب‌پذیری‌ها یا قابلیت سوء استفاده و خسارت آن ها بـر شـبکه، بـا جمـع سـاده امتیازهای CVSS امکان پذیر نیست**
- مبهم بودن نحوه تخصیص امتیاز خسارت آسیب‌پذیری‌ها

9

بررسی آسیب‌پذیری‌ها در شبکه



10

امتیاز آسیب پذیری یک مجموعه آسیب پذیری
تعاریف اولیه

مجموعه آسیب‌پذیری‌ها

$$V = \{v_1, \ldots, v_n\}$$

هر سوء استفاده در گراف حمله شبکه، متناظر با یک آسیب‌پذیری در شبکه است.

$$V_E : E \to V$$
$$V_E(e) = v$$

آسیب پذیری اولیه

$$v_x \in S_0(G)$$

زنجیره آسیب پذیری

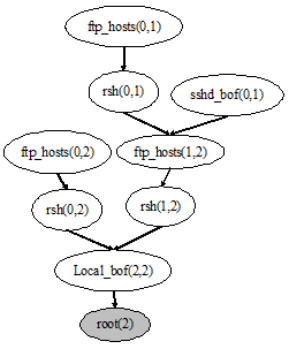
$$C = < v_1, \ldots, v_{n_i} >$$

زنجیره آسیب پذیری پشتیبان

$$C = < v_1, \ldots, v_n > \in SC(v_x) \Leftrightarrow v_1 \epsilon S_0 \wedge (v_n = v_x) \wedge C \in Chain(G)$$

11

نمایش زنجیره آسیب‌پذیری در گراف حمله



$$SC(local\_bof(2)) = \{($$

$$C_1 = < sshd\_bof(0), fi \qquad \_bof(2) >$$

$$C_2 = < ftp\_rhosts(0), rsh(0), ftp\_rhosts(1), rsh(1,2), local\_bof(2) >$$

$$C_3 = < ftp\_rhosts(0), rsh(0), local\_bof(2) >$$

12

لزوم بررسی خسارت جمعی آسیب‌پذیری‌ها

- حذف همه آسیب‌پذیری‌های سیستم غیر ممکن است
- بررسی خسارت‌ها نیازمند در نظر گرفتن ترکیب بیش از یک آسیب‌پذیری است.
- امتیاز خسارت هر آسیب‌پذیری در CVSS، مجزا و مستقل و محدود به یک میزبان می‌باشد
- اثر مشترک آسیب پذیری ها در سیستم
  - **خسارت ناشی از سوءاستفاده از مجموعه‌ای از آسیب‌پذیری‌ها با جمع ساده خسارت تک‌تک آسیب‌پذیری‌ها قابل محاسبه نمی‌باشد.**

" مدلی برای تحلیل عددی خسارت جمعی ناشی از آسیب‌پذیری‌های امنیتی "
شانزدهمین کنفرانس ملی سالانه انجمن کامپیوتر ایران، تهران، ۱۳۸۹.

13

امتیاز سوء استفاده زنجیره آسیب‌پذیری

- **امتیاز سوء استفاده**

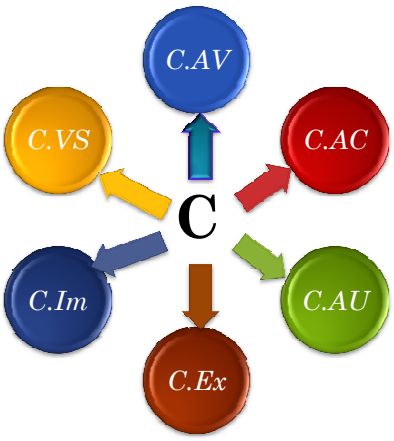
$$C.Ex = 20 * C.AV * C.AC * C.AU$$

14

مشخصه‌های سوء استفاده

15

مشخصه‌های زنجیره آسیب‌پذیری

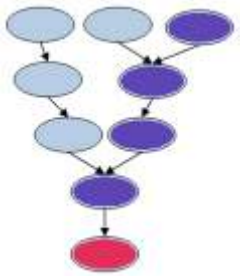


16

امتیاز متأثر آسیب‌پذیری

{1,3,4,8}

- ✓میانگین ریاضی
- ✓یانگین هندسی
- ✓=میانگین نمایی



$$EVS_N(v_x) = \ln \sum_{C_{2_j} \in C(v_x)} e$$

17

امتیاز آسیب‌پذیری شبکه

$$NVS = \ln \sum_{j=1}^{n} e^{EVS_N(v_j)}; v_j \in NCV$$

$$EVS_N(v_x) = \ln \sum_{C_{2_j} \in SC(v_x)} e^{C_{2_j}.vs}$$

for (every $v_j \in NCV$) {
  for (every $C_1 \in SC(v_j)$) {
    for (every $v_i \in NCV$ and $i \neq j$) {
    $C = \max_{C_2 \in SC(v_i)} (C_1 \cap C_2)$}
  if ($C \neq \varnothing$ and $C_2.vs \leq C_1.vs$) {
    $(C_2 - C) \in SC(v_i)$;
    $SC(v_i) = SC(v_i) - C_2$; }
}}

18

امتیاز آسیب‌پذیری

$$Vulnerability.score(v) = f(Impact(v), Exploitability(v))$$

$$BaseScore(v) = round\_to\_1\_decimal\left(\left((0.6 * Impact(v)) + (0.4 * Exploitability(v)) - 1.5\right) * f(Impact(v))\right)$$

$$f(impact(v)) = 0 \text{ if } Impact(v) = 0,\ 1.176 \text{ otherwise}$$

- امتیاز متأثر آسیب‌پذیری

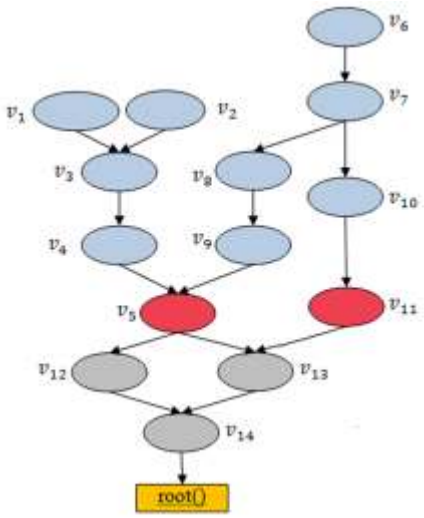
$$EVS_N(v) = \ln \sum_{C_i \in SC(v)} e^{C_i.vs}$$

- امتیاز آسیب‌پذیری شبکه

$$NVS = \ln \sum_{v \in NCV} e^{SEVS_N(v)}$$

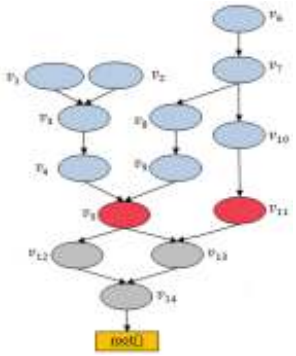
19

ارزیابی-۱
گراف حمله



20

ارزیابی-۱
محاسبه امتیاز آسیب پذیری شبکه



- مجموعه دسترسی‌های بحرانی شبکه

$$CV = \begin{Bmatrix} \{C(f_2), E(f_2, f_5), W(f_3)\}, \\ \{D(S_1), K(f_7)\} \\ R(f_3), W(f_2), E(f_2, f_5) \end{Bmatrix}$$

- مجموعه آسیب‌پذیری‌های بحرانی شبکه

$$NCV = \{v_5, v_{11}\}$$

- حذف امتیاز سوء استفاده‌های مشترک

$$C.Ex = 3.8 \quad C.Impact = 8.5$$

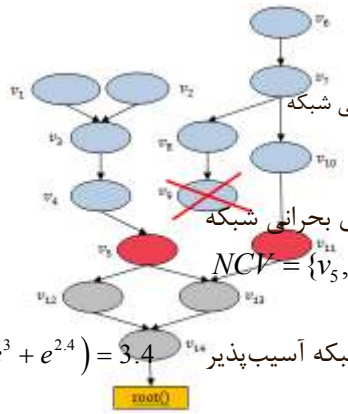
- امتیاز سوء استفاده از شبکه آسیب‌پذیر

$$NC_{Ex} = \ln\left(e^{3} + e^{3.7}\right) = 4.6$$

- امتیاز آسیب‌پذیری شبکه

$$NVS = \ln\left(e^{5.9} + e^{6}\right) = 6.6$$

ارزیابی-۲
حذف یک آسیب پذیری از شبکه



- مجموعه دسترسی‌های بحرانی شبکه
- مجموعه آسیب‌پذیری‌های بحرانی شبکه

$$NCV = \{v_5, v_{11}\}$$

- مجموعه سوء استفاده از شبکه آسیب‌پذیر

$$NC_{Ex} = \ln\left(e^{3} + e^{2.4}\right) = 3.4$$

- امتیاز آسیب‌پذیری شبکه

$$NVS = \ln\left(e^{5.6} + e^{5.2}\right) = 6.1$$

نتایج ارزیابی ۲

	ارزیابی ۱	ارزیابی ۲
امتیاز سوء استفاده متأثر آسیب پذیری v_5	۳	۲.۴
امتیاز سوء استفاده شبکه آسیب پذیر	۳.۷	۳.۴
امتیاز آسیب پذیری شبکه	۶.۶	۶.۱

23

بحث و بررسی

- استفاده از جمع مقادیر امتیاز آسیب‌پذیری‌ها در امتیازدهی زنجیره آسیب‌پذیری

{۱.۳، ۱.۳، ۱.۳، ۱.۳، ۱۰} و {۵، ۵، ۵}

- استفاده از حداکثر امتیاز آسیب‌پذیری‌ها در امتیازدهی زنجیره آسیب‌پذیری

{۸.۶، ۸.۶، ۸.۶، ۸.۶} و {۱.۳، ۱.۳، ۱.۳، ۸.۶}

- استفاده از میانگین امتیاز آسیب‌پذیری‌ها در امتیازدهی زنجیره آسیب‌پذیری

$$C_1 = \{v_1, v_2, v_3, v_4\}$$
$$C_2 = \{v_1, v_2, v_3, v_4\}$$

$$C_1 vs = C_2 vs = \sum_{v_i \in C_1} v_i vs$$

24

بحث و بررسی

- استفاده از حداکثر مقدار مشخصه آسیب‌پذیری‌ها در امتیازدهی زنجیره آسیب‌پذیری

v_5	v_4	v_3	v_2	v_1	
L:0.395	N:1	N:1	N:1	L:0.395	**AV**
L:0.71	H:0.35	L:0.71	L:0.71	H:0.35	**AC**
N:0.704	N:0.704	M:0.45	N:0.704	M:0.45	**AU**
4	5	6.4	10	1.3	**v_i.Ex**

$$C_1 = \{v_2, v_3, v_4, v_5\}$$
$$C_2 = \{v_1, v_1, v_1, v_1\}$$
$$C_1.Ex = 20 * \max_{i=2,3,4,5} v_i.AV * \max_{i=2,3,4,5} v_i.AC * \max_{i=2,3,4,5} v_i.AU = 1.3$$
$$C_2.Ex = 20 * \max_{i=1} v_i.AV * \max_{i=1} v_i.AC * \max_{i=1} v_i.AU = 1.3$$

- عدم تأثیر ترتیب سوء استفاده از آسیب‌پذیری‌ها در امتیاز آسیب‌پذیری

25

محدودیت‌ها و نواقص روابط پیشنهادی

- نحوه امتیازدهی سوء استفاده از آسیب پذیری ها در شبکه، با در نظر گرفتن اثر سوء استفاده از دیگر آسیب پذیری های موجود، مشخص نیست.
- امتیاز آسیب‌پذیری شبکه برمبنای رابطه استفاده شده در CVSS است.
  - رابطه CVSS برای محاسبه امتیاز آسیب‌پذیری‌ها بر اساس مشخصه‌های آسیب‌پذیری تعریف شده و با توزیع نرمال امتیازهای آسیب‌پذیری بدست آمده است.
- نیاز به یک مدل تکمیلی جهت خودکار سازی تعریف دسترسی‌های بحرانی شبکه بر اساس خط‌مشی‌های امنیتی شبکه

26

پیشنهاد کارهای آینده

- حل مسأله دسترسی لازم جهت سوء استفاده از آسیب‌پذیری‌های متوالی در شبکه
- ارائه رابطه امتیاز آسیب‌پذیری شبکه

27

مراجع

1. سمیع، الهه، شهریاری، حمیدرضا، **" مدلی برای تحلیل عددی خسارت جمعی ناشی از آسیب‌پذیری‌های امنیتی"**، شانزدهمین کنفرانس ملی سالانه انجمن کامپیوتر ایران، تهران، ۱۳۸۹.
2. Common Vulnerability Scoring System (CVSS), http://www.first.org/cvss/
3. Frigault, M., Wang, L., *"Measuring Network Security Using Bayesian Network-Based Attack Graphs, Computer Software and Applications"*, COMPSAC '08: 32nd Annual IEEE International Computer Software and Applications Conference, Presented at the Proceedings, pp.698-703, 2008.
4. Frigault, M., Wang, L., Singhal, A., Jajodia, S., *"Measuring Network Security Using Dynamic Bayesian Networks"*, QoP'08: 4th ACM Workshop on Quality of Protection, 2008.
5. Ghosh, N.,Ghosh, S.K., *"An Approach for Security Assessment of Network Configurations Using Attack Graph"*, NetCoM-2009: The First International Conference on Networks & Communications, Presented at the Proceedings, pp.283-288, 2009.
6. Wang, L., Singhal, A., Jajodia, S., *"Measuring the overall security of network configurations using attack graphs"*, DBSec'07: 21st Annual IFIP WG 11.3 Working Conference on Data and Applications Security, Presented at the Proceedings, pp.98-112, 2007.
7. Scarfone, K., Mell, P., *"Vulnerability scoring for security configuration settings"*, CCS'08: 15th ACM Conference on Computer and Communications Security, Presented at the Proceedings, pp.3-8, 2008.
8. Wang, L., Singhal, A., Jajodia, S., *"Measuring network security using attack graphs"*, QoP'07: 3rd ACM workshop on Quality of protection, Presented at the Proceedings, pp.98-112, 2007.
9. Pamula, J., Ammann, P., Jajodia, S., Swarup, V., *"A weakest-adversary security metric for network configuration security analysis"*, QoP'06: 2nd ACM Workshop on Quality of Protection, Presented at the Proceedings, pp.31-37, 2006.
10. Xiang, Z., Chen, Y., Jian, W., Yan, F., *"A Jackson Network-Based Model for Quantitative Analysis of Network Security"*, Lecture Notes in Computer Science, Berlin: Springer-Verlag, pp.517-522, 2005.
11. Mell, P., Scarfone, K., *"Improving the Common Vulnerability Scoring System"*, J.IET Inf.Secur., Vol.1, pp. 119 – 127, 2007.

28