

网络动态防御体系下主机安全威胁分析方法

李立勋^{1,2}, 张斌^{1,2}, 董书琴^{1,2}

(1. 信息工程大学, 河南 郑州 450001;
2. 河南省信息安全重点实验室, 河南 郑州 450001)

摘要: 分析网络动态防御体系下的主机安全威胁必须考虑动态变换给主机脆弱性造成的不确定性。为此, 首先, 利用随机抽样模型对网络动态防御变换周期和变换空间给主机脆弱性造成的不确定性进行量化, 并结合通用漏洞评分系统 CVSS (common vulnerability scoring system) 计算入侵者针对单个脆弱性的入侵成功率; 其次, 为避免多脆弱性情况下的入侵路径搜索过程出现自环, 引入节点访问队列并提出改进的递归深度优先入侵路径搜索算法; 然后基于求得的脆弱性入侵成功率计算多脆弱性多入侵路径情况下的主机安全威胁度; 最后, 在典型网络动态防御环境中进行实验, 验证了方法的可用性和有效性。

关键词: 网络安全; 网络动态防御; 主机安全威胁分析; 入侵成功率; 入侵者权限转移图

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2018031

Host security threat analysis approach for network dynamic defense

LI Lixun^{1,2}, ZHANG Bin^{1,2}, DONG Shuqin^{1,2}

1. Information Engineering University, Zhengzhou 450001, China
2. Henan Province Information Security Key Laboratory, Zhengzhou 450001, China

Abstract: Calculating the host security threat in network dynamic defense (NDD) situation has to consider the vulnerabilities' uncertainty because of dynamic mutation. Firstly, the vulnerabilities' uncertainty caused by the mutation space and the mutation period was calculated by random sampling model, and combined with the CVSS, the attack success probability formula of single vulnerability was derived. Secondly, to avoid self-loop during the path searching process in multiple vulnerabilities situation, an improved recursive depth first algorithm which combined with node visited queue was proposed. Then, the host security threat was calculated based on attack success probability in the situation of multiple vulnerabilities and paths. Finally, approach's availability and effectiveness were verified by an experiment conducted in a typical NDD situation.

Key words: cyber security, network dynamic defense, host security threat analysis, attack success probability, attacker privilege transfer graph

收稿日期: 2018-03-02; 修回日期: 2018-03-28

通信作者: 李立勋, lilixun_1994@126.com

基金项目: 河南省基础与前沿技术研究计划基金资助项目 (No. 2014302903); 信息保障技术重点实验室开放基金资助项目 (No. KJ-15-109); 信息工程大学新兴科研方向培育基金资助项目 (No. 2016604703)

Foundation Items: The Foundation and Frontier Technology Research Project of Henan Province (No. 2014302903), Information Protection Technology Key Laboratory Open Fund Project (No. KJ-15-109), New Research Direction Cultivation Fund of Information Engineering University (No. 2016604703)

1 引言

网络动态防御 (NDD, network dynamic defense) 技术通过对安全目标及其对外呈现形式实施空间和时间上的动态变化来降低信息系统确定性、静态性和同构性, 增大入侵者探测、利用主机脆弱性和维持已有渗透成果的成本和难度, 进而降低入侵成功概率^[1,2]。分析 NDD 体系下主机面临的安全威胁有助于准确掌握主机安全状态并合理制订更为有效的 NDD 策略。

目前, 通常从脆弱性利用角度剖析主机面临的安全威胁^[3]。传统静态网络体系下主机脆弱性保持不变, 可结合脆弱性的 CVSS 量化值计算主机安全威胁。然而在 NDD 体系下, 主机脆弱性会由于 NDD 变换周期和变换空间的动态变换而呈现不确定性, 此时基于主机脆弱性实施安全威胁分析需要解决 2 个问题: 1) 量化 NDD 技术的变换周期和变换空间给单个主机脆弱性造成的不确定性; 2) 量化 NDD 体系中多脆弱性和多入侵路径对主机安全威胁造成的影响。

针对问题 1), 文献[4,5]提出基于随机抽样的方法, 利用随机抽样模型对网络入侵过程建模, 可用于量化变换周期和变换空间给主机脆弱性造成的不确定性, 但是其方法只适用于分析主机仅存在单个脆弱性的情况。针对问题 2), 文献[6~8]提出基于图论的方法, 利用有向图对 NDD 体系下入侵者状态转移过程以及攻击步骤间的依赖关系进行建模, 计算入侵成功概率和攻击成本, 此类方法可分析 NDD 体系存在多个脆弱性时主机面临的安全威胁, 但是其主要关注变换周期对安全威胁的影响, 未同时考虑变换空间因素。

本文首先利用随机抽样模型量化 NDD 技术的变换周期和变换空间给主机脆弱性造成的不确定性, 并结合 CVSS 量化值计算入侵者利用单个脆弱性实施入侵时的入侵成功概率; 然后构建入侵者权限转移图用以搜索入侵者利用多个脆弱性实施入侵时的潜在入侵路径; 最后定义主机安全威胁度, 并提出在多脆弱性多入侵路径情况下利用入侵成功概率计算主机安全威胁度的方法。

2 单脆弱性入侵成功概率

NDD 机制实施动态变换的对象包括硬件平台、软件版本、服务端口等, 而变换时机包括随机变换、定时变换和驱动性变换^[1]。因此, 为刻画 NDD 机制的变换对象、变换时机与主机脆弱性的关系, 给出 NDD 体系下的主机脆弱性定义如下。

定义 1 NDD 体系下的主机脆弱性记为 $hvul$, $hvul = \langle id, \langle A_1, \Delta t_1 \rangle, \langle A_2, \Delta t_2 \rangle, \dots, \langle A_n, \Delta t_n \rangle \rangle$, $n \in N$ (N 为自然数), 其中, id 为主机脆弱性标识; A_i ($1 \leq i \leq n$) 表示入侵该脆弱性所利用的系统属性, 即 NDD 机制的变换对象; Δt_i ($1 \leq i \leq n$) 表示 NDD 技术对 A_i 属性实施变换的变换周期。

定义 2 NDD 体系下的主机脆弱性状态。对任意 $hvul$, 记 $hvul$ 在 t 时刻的状态为 $hvul(t)$, $hvul(t) = \langle id, a_1, a_2, \dots, a_n \rangle$, $n \in N$, 其中, id 为脆弱性标识, a_i ($1 \leq i \leq n$) 表示脆弱性 A_i 属性的当前取值。

定义 3 NDD 体系下的主机脆弱性变换。对任意 $hvul$, 给定 2 个时刻 t_1 和 t_2 , $t_2 > t_1$, 若 $hvul(t_2) \neq hvul(t_1)$, 则称 $hvul$ 发生了变换。

将主机脆弱性的变换周期记为 $interval$, 变换空间记为 Ω 。根据定义 3, $interval = \min\{\Delta t_i\}$; 根据笛卡尔积定义, $\Omega = A_1 \times A_2 \times \dots \times A_n$, 将 Ω 大小记为 $|\Omega|$, 则 $|\Omega| = |A_1| \cdot |A_2| \cdot \dots \cdot |A_n|$, 其中, $|A_i|$ ($1 \leq i \leq n$) 为第 i 个属性的值域空间大小。

针对主机脆弱性的入侵过程主要分为脆弱性探测和脆弱性利用 2 个阶段^[4], 因此入侵成功概率 asp 应为脆弱性探测成功概率 vdP 和脆弱性利用成功概率 sp_{cvss} 的乘积, 即

$$asp = vdp \cdot sp_{cvss} \quad (1)$$

其中, sp_{cvss} 表示根据 CVSS 量化得出的脆弱性利用成功概率, 而脆弱性探测成功概率 vdP 可利用随机抽样^[4]的方法确定。

假设入侵者完成对任意一个主机脆弱性状态探测所需要的时间周期均为 τ , 记入侵者在 $interval$ 变换间隔内可探测的脆弱性状态数量为 k , 则

$$k = \frac{interval}{\tau} \quad (2)$$

在 $interval$ 内,入侵者的探测过程可抽象为不放回抽样事件,将成功探测到单个主机脆弱性当前状态的概率记为 P_{success} , 则

$$P_{\text{success}} = \begin{cases} 1, & k \geq |\Omega| \\ 1 - \frac{C_{|\Omega|-1}^k}{C_{|\Omega|}^k}, & k < |\Omega| \end{cases} \quad (3)$$

其中, $C_{|\Omega|}^k$ 表示入侵者对主机脆弱性的变换空间 Ω 完成 k 次探测后的所有结果数, $C_{|\Omega|-1}^k$ 表示入侵者 k 次探测均失败的所有结果数, $\frac{C_{|\Omega|-1}^k}{C_{|\Omega|}^k}$ 表示入侵者脆弱性探测失败的概率。

当主机脆弱性变换后,入侵者并不能维持先前取得的探测结果,因此在穷举性地探测脆弱性变换空间 Ω 的过程中,入侵者会经历 $\frac{|\Omega|}{k}$ 次变换,那么脆弱性探测失败事件可抽象为放回抽样事件,此时脆弱性探测失败概率 P_{failall} 为

$$P_{\text{failall}} = (1 - P_{\text{success}})^{\frac{|\Omega|}{k}} \quad (4)$$

入侵者成功探测到当前脆弱性状态的概率,即脆弱性探测成功概率 vdp 为

$$\begin{aligned} vdp &= 1 - P_{\text{failall}} \\ &= 1 - \left(\frac{C_{|\Omega|-1}^k}{C_{|\Omega|}^k} \right)^{\frac{|\Omega|}{k}} \end{aligned} \quad (5)$$

3 多脆弱性入侵路径

当网络中的主机存在多个脆弱性时,入侵者可选取多条入侵路径对目标主机实施入侵。为搜索多脆弱性情况下潜在入侵路径,首先根据网络连接关系、脆弱性分布等情况构造入侵者权限转移图 APTG 以刻画入侵过程,再利用改进的递归深度优先搜索算法搜索 APTG 以发现潜在入侵路径。

3.1 入侵者权限转移图

入侵者权限转移图是一个有向图,记为 $APTG = (N, E)$,用于表示入侵者在网络入侵过程中获取到的主机权限。其中

1) N 是入侵者权限节点集合, $\forall n \in N$, $n = \langle \text{hostid}, \text{privilege} \rangle$, 表示入侵者在主机 hostid

具有权限 privilege 。

2) E 是连接入侵者权限节点的有向边集合,表示节点间的入侵关系。 $\forall e \in E$, $e = \langle \text{shost}, \text{thost}, \text{prep}, \text{postp}, \text{vulset} \rangle$, 表示入侵者在源主机 shost 具有初始权限 prep , 并可通过目标主机 thost 的脆弱性集合 vulset 中的脆弱性对目标主机实施入侵,成功入侵后可在目标主机获得 postp 权限。

在一个网络中,将入侵者初始权限集合记为 H , $\forall h \in H$, $h = \langle \text{hostid}, \text{privilege} \rangle$, 表示入侵者在主机 hostid 具有权限 privilege 。连接关系矩阵记为 C , 矩阵元素 $c_{i,j}$ 为主机 i 可访问主机 j 的服务集合。 $\forall \text{service} \in c_{i,j}$, $\text{service} = \langle \text{serviceid}, \text{port}, \text{protocol} \rangle$, serviceid 为服务标识, port 为服务端口, protocol 表示承载服务的网络协议。脆弱性权限集合记为 VP , $\forall vp \in VP$, $vp = \langle \text{hvul}, \text{serviceid}, \text{prep}, \text{postp}, \text{asp} \rangle$, 表示主机脆弱性 hvul 与服务 serviceid 关联,在利用该脆弱性前,入侵者需要拥有目标主机的初始权限 prep , 利用成功后会取得目标主机的 postp 权限,且该脆弱性的入侵成功概率为 asp 。

下面根据入侵者初始权限、连接关系和脆弱性权限构造入侵者权限转移图。

算法1 APTG 构造算法

输入 入侵者初始权限集合 H , 连接关系矩阵 C , 脆弱性权限集合 VP

输出 入侵者权限节点集合 N , 有向边集合 E , 入侵者权限转移图 APTG

$N = \emptyset$, $E = \emptyset$, $APTG = \emptyset$

for each $c_{i,j} \in C$ //遍历连接关系矩阵

for each $vp \in VP$ //遍历主机 j 上的脆弱性权限

if $vp.\text{serviceid} \cap c_{i,j}.\text{serviceid} \neq \emptyset \ \& \ H_j \neq \emptyset$

//该连接关系中的服务存在脆弱性并且入侵者在目标主机具备初始权限

for each $h \in H_j$

if $h.\text{privilege} \geq vp.\text{prep}$ //当前权限大于脆弱性利用所需权限

$n_{\text{start}} = \langle i, vp.\text{prep} \rangle$

$n_{\text{end}} = \langle j, vp.\text{postp} \rangle$ //生成新的入侵者权限节点

if $\exists e = \langle i, j, vp.\text{prep}, vp.\text{postp}, \text{vulset} \rangle \in E$

$e.\text{vulset} \leftarrow vp.\text{vul}$

$E \leftarrow e$ //更新主机 i 到主机 j 的有向边集合

```

else
 $e_{\text{new}} = \langle i, j, vp.prep, vp.postp, vulset \rangle$ 
 $e_{\text{new}}.vulset \leftarrow vp.vul$ 
 $E \leftarrow e_{\text{new}}$  //生成新的主机  $i$  到主机  $j$  的有向边
并存储
 $N \leftarrow n_{\text{start}}, n_{\text{end}}$  //存储新生成的入侵者权限节点
 $H \leftarrow n_{\text{start}}, n_{\text{end}}$  //更新初始入侵者权限集合
return  $N, E, APTG$ 

```

假设目标网络共有 n 个主机并相互连通，每个主机具有 l 个脆弱性和 m 个权限状态，则该算法复杂度为 $O(lm \cdot (n^2 - n))$ ，因为 l 和 m 为常数，所以 APTG 构造算法的最终复杂度为 $O(n^2)$ 。

3.2 入侵路径搜索

根据入侵单调性原理^[9]，单条入侵路径不存在环路，不同入侵路径可存在交叉。在利用传统的深度优先搜索算法搜索 APTG 中的潜在入侵路径时，可能会因为 APTG 中存在的环路而陷入死循环。因此，本文提出改进的递归深度优先入侵路径搜索算法（IDFPS），IDFPS 在传统递归深度优先搜索算法中加入节点访问队列 *visitedqueue*，用于记录单条路径上已被访问过的节点，避免入侵路径搜索时因 APTG 存在环路而导致算法无法终止的情况。

算法 2 IDFPS 算法

输入 APTG 边集合 E ，入侵者权限节点集合 N ，入侵者源权限节点 n_{aid} ，入侵者目标权限节点 n_{tid}

输出 入侵路径集合 P

$M_{|N|} \leftarrow [0]_{|N|}$ // $|N|$ 阶矩阵 $M_{|N|}$ 用于存储

APTG 节点间的连接关系

$visitedqueue = \emptyset$ //记录节点访问情况

$path = \emptyset$ //记录单条入侵路径路径

$num = 1$ //记录路径上的节点数，初始值为 1

$P = \emptyset$ //入侵路径集合初始为空

for each $e_{i,j} \in E$

$m_{i,j} = 1$ //根据 APTG 边集合 E 确定 APTG 节点间的连接关系，其中 $m_{i,j} \in M_{|N|}$

$Dfs(n_{\text{aid}})$ //递归深度优先搜索源节点

FUNCTION $Dfs(v)$ //递归深度优先搜索函数

$visitedqueue[v] = 1$ //标记当前节点为已访问状态

```

 $i = 0$ 
while  $i < |N|$  do
if  $m_{v,i} \neq 0$  and  $visitedqueue[i] = 0$  //节点  $v$  和
 $i$  存在连接关系且节点  $i$  未被访问
if  $i = n_{\text{tid}}$   $P \leftarrow path$  //到达目标节点，存储
路径
else
 $m_{v,i} = 0$  //递归前清空当前连接关系，避免重复搜索
 $path[num] = i$  //记录访问到的节点
 $num++$  //路径长度加 1
 $Dfs(i)$  //递归搜索节点  $i$ 
 $m_{v,i} = 1$  //递归完成后恢复当前连接关系
 $visitedqueue[i] = 0$  //恢复当前节点为未访问状态
 $num--$  //路径长度减 1
 $i++$ 
end while
return  $P$ 

```

假设有 n 个入侵者权限节点，则 IDFPS 算法复杂度为 $O(n^2)$ 。

4 主机安全威胁度

文献[3]将脆弱性利用威胁度定义为从攻击图到区间[0,1]的映射，入侵者达成脆弱性利用目标成功率越大，脆弱性利用威胁度越大，反之越小。本文对该定义进行扩展，定义主机安全威胁度，并给出计算方法。

定义 4 主机安全威胁度 *threat* 为从指定入侵者权限转移图 APTG 到区间[0,1]的映射，用来综合评估入侵者达成目标的成功概率，攻击者达成目标的成功概率越大，主机安全威胁度越大，反之越小。因此，本文通过计算入侵者对目标主机的入侵成功概率来刻画目标主机的安全威胁度。

若针对主机共有 w 条入侵路径，入侵者通过任意一条路径均可实施入侵。对于单条入侵路径 $path_i$ ($1 \leq i \leq w$)，其上共有 n_i 条有向边，任意有向边 e_j ($1 \leq j \leq n_i$) 包含 m_j 个脆弱性，入侵者在有向边 e_j 上可任意选择其中一个脆弱性入

侵，则该路径上共有 $q \left(q = \prod_{i=1}^{n_i} m_j \right)$ 种入侵方法。

将入侵方法记为 $method_x$ ($1 \leq x \leq q$)，根据

$method_x$ 中每个脆弱性的入侵成功概率 asp_j ($1 \leq j \leq n_i$) 可计算该方法的入侵成功概率

$$methodasp_x = \prod_{j=1}^{n_i} asp_j \quad (6)$$

在单条路径上, 通过任意一种方法入侵成功均可视作通过该路径入侵成功, 所以该路径的入侵成功概率为

$$pathasp_i = 1 - \prod_{x=1}^q (1 - methodasp_x) \quad (7)$$

同理, 当针对目标主机存在 w 条入侵路径时, 入侵者的入侵成功概率为

$$hostasp = 1 - \prod_{i=1}^w (1 - pathasp_i) \quad (8)$$

5 实验测试与分析

5.1 环境设置

搭建如图 1 所示的网络环境, 其中, 企业网

根据防火墙安全规则分为内网办公区和 DMZ 区。内网办公区设置 1 台数据库服务器和 1 台办公主机, 模拟正常办公环境。DMZ 区设置 1 台 Web 服务器和 1 台邮件服务器。攻击者主机位于外部网络, 可通过 Internet 对企业网进行入侵。各主机脆弱性见表 1。

表 1 中 Telnet 弱口令没有对应的 CVE 编号, 但是根据 CVSS 标准, 该脆弱性可以导致远程获取目标主机最高权限, 且攻击复杂度低, 故将其利用成功概率定为 0.8。

分别在 Server1 上应用 Web 服务多态化^[10]技术、Server3 上应用数据库接口随机化^[11]技术、Switch2 上应用 MTD-switch^[12]技术用以构建 NDD 环境。其中

1) Web 服务多态化技术为若干虚拟 Web 服务器配置唯一的软件栈, 通过轮换机制提供在线 Web 服务, 进而为入侵者呈现不断变换的 Web 渗透面。根据文献[11], 可配置的虚拟服务器数为 1554, 因此该技术的变换空间 $|\Omega| = 1554$ 。同

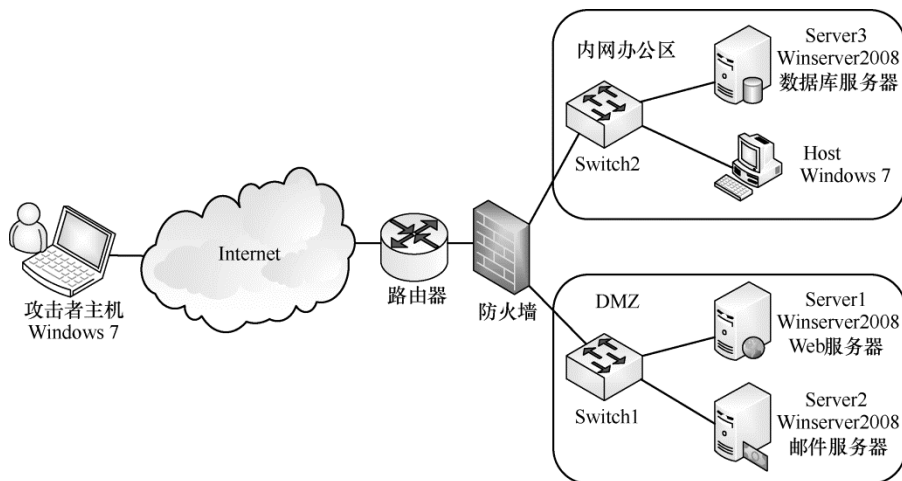


图 1 实验网络拓扑

表 1

主机脆弱性

主机脆弱性编号	主机	脆弱性	CVE 编号	初始权限	目标权限	利用成功概率
V1	Server1(S1)	Web 远程代码注入	CVE-2015-1635	none	root	0.8
V2		FTP 路径遍历	CVE-2011-4800	user	user	0.8
V3	Server2(S2)	U-Mail 输入验证错误	CVE-2008-4932	user	root	0.8
V4	Server3(S3)	SMB 远程代码执行	CVE-2017-0143	none	root	0.6
V5		SQL 远程代码注入	CVE-2015-1762	user	root	0.2
V6		Tenlet 弱口令	无	user	root	0.8
V7	Host(H)	SMB 远程代码执行	CVE-2017-0143	none	root	0.6
V8		IE8 缓冲区溢出	CVE-2010-1117	none	root	0.2

时, 将虚拟服务器使用期限设置为 300 s, 即 $interval = 300\text{ s}$ 。

2) 数据库接口随机化技术通过 MD5 杂凑和字符移位将每次 SQL 查询中的数据库表名和列名分别随机化为包含 16 个字符的字符串(包含大小写字母和数字共 62 个字符), 从而减小 SQL 注入成功概率。因此该技术的变换周期和变换空间分别为 $interval = 10\text{ s}$, $|\Omega| = 62^{16}$ 。

3) MTD-switch 通过周期性地改变内网 Server3 和 Host 对外呈现的虚拟 IP 地址, 隐藏主机真实 IP 地址, 增大入侵者探测主机脆弱性的难度, 进而减小入侵成功概率。设置内网办公区主机虚拟 IP 在一个 B 类子网地址段内每 60 s 变换一次, 即 $|\Omega| = 2^{16} - 1$, $interval = 60\text{ s}$ 。

5.2 主机安全威胁分析

根据实验环境可确定入侵者初始权限集合 H , 连接关系矩阵 C , 脆弱性权限集合 V , 运行 APTG 构造算法可得如图 2 所示入侵者权限转移图 APTG。其中, 圆形节点表示入侵者权限状态, up 表示 user 权限, rp 表示 root 权限, 如 (S1,rp) 表示入侵者在主机 S1 具有 root 权限; 有向边表示节点间入侵关系, 起点为入侵前的初始权限节点, 终点为入侵成功后的权限节点, 值为可利用的脆弱性集合, 如图 2 中的 (V4,V5,I6) 边表示可利用脆弱性 V4、V5 或 V6 从节点 N6 入侵至节点 N5。

设入侵者攻击目标为获取 Host 的 root 权限, 运行 IDFPS 算法可搜索潜在入侵路径, 再结合 3 种 NDD 技术应用情况, 分别计算各入侵方法和防御措施下的入侵成功概率及主机安全威胁, 结果见表 2。计算过程中均假设入侵者实施一次通道探测的时间成本 $\tau = 10\text{ s}$ 。

由表 2 可知如下结论。

1) 在未采取任何防御措施时, 入侵者可通过 9 条入侵路径, 共 16 种入侵方法对 Host 实施入侵。虽然单个入侵方法的入侵成功概率均在 0.3 以下, 但是主机安全威胁度却高达 0.946 37。此时该网络中脆弱性总数仅为 8, 然而在实际网络环境中, 由于 0day 漏洞等的存在, 实际脆弱性数目将更多。因此, 在未采取防御措施时, Host 面临极大的安全威胁。

2) 数据库接口随机化降低了入侵者对脆弱性 V5 的探测成功概率, 但是因为只作用于 Server3 的数据库服务, 所以该技术对其他脆弱性的探测成功概率并没有影响, 进而未明显降低 Host 的安全威胁。与无防御措施时相比, Host 的安全威胁降低幅度仅为 1.5%。

3) Web 服务多态化减小了脆弱性 V1 和 V2 的暴露时间, 增加了主机脆弱性的不确定性。与数据库接口随机化相比, 因为同时降低了 2 个脆弱性的探测成功概率, 所以取得了更好的防御效果。与无防御措施相比, Host 的安全威胁降低幅度为 9.3%。

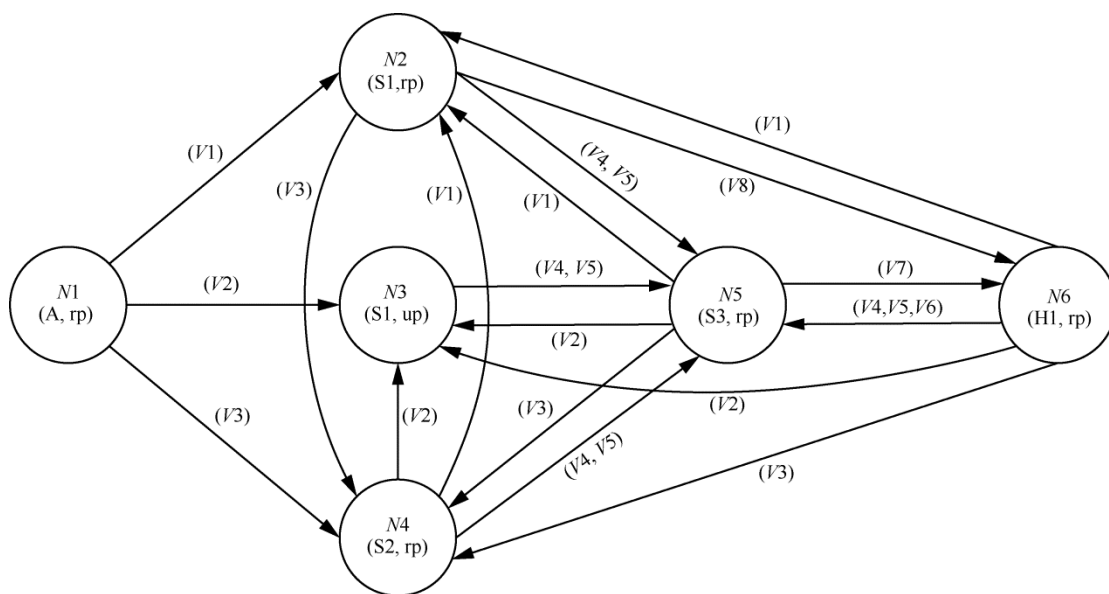


图2 入侵者权限转移图 APTG

表 2

入侵成功概率和主机安全威胁

序号	路径	入侵方法	各防御措施下的入侵成功概率				
			无防御措施	数据库接口随机化	Web 服务多态化	MTD-switch	协同防御
1	(N1, N2, N4, N3, N5, N6)	(I1, I3, I2, I4, I7)	0.184 32	0.184 32	0.117 17	0.073 65	0.046 82
2		(I1, I3, I2, I5, I7)	0.061 44	0.038 80	0.039 06	0.024 55	0.009 85
3	(N1, N2, N4, N5, N6)	(I1, I3, I4, I7)	0.230 40	0.230 40	0.146 47	0.092 06	0.058 52
4		(I1, I3, I5, I7)	0.076 80	0.048 50	0.048 82	0.030 69	0.012 32
5	(N1, N2, N5, N6)	(I1, I4, I7)	0.288 00	0.288 00	0.183 08	0.115 07	0.073 15
6		(I1, I5, I7)	0.096 00	0.060 70	0.061 03	0.038 36	0.015 42
7	(N1, N2, N6)	(I1, I8)	0.160 00	0.160 00	0.101 71	0.101 14	0.064 29
8	(N1, N3, N5, N6)	(I2, I4, I7)	0.288 00	0.288 00	0.183 08	0.115 07	0.073 15
9		(I2, I5, I7)	0.096 00	0.060 70	0.061 03	0.038 36	0.015 42
10	(N1, N4, N5, N6)	(I3, I1, I4, I7)	0.230 40	0.230 40	0.146 47	0.092 06	0.058 52
11		(I3, I1, I5, I7)	0.076 80	0.048 50	0.048 82	0.030 69	0.012 32
12	(N1, N4, N2, N6)	(I3, I1, I8)	0.128 00	0.128 00	0.081 37	0.080 90	0.051 43
13	(N1, N4, N3, N5, N6)	(I3, I2, I4, I7)	0.230 40	0.230 40	0.146 47	0.092 06	0.058 52
14		(I3, I2, I5, I7)	0.076 80	0.048 50	0.048 82	0.030 69	0.012 32
15	(N1, N4, N5, N6)	(I3, I4, I7)	0.288 00	0.288 0	0.288 00	0.115 07	0.115 07
16		(I3, I5, I7)	0.096 00	0.060 70	0.096 00	0.038 36	0.024 25
主机安全威胁	—	—	0.946 37	0.932 55	0.858 13	0.686 40	0.515 68

4) 与数据库接口随机化和 Web 服务多态化相比, Host 在 MTD-switch 保护下的安全威胁降低为 0.6864。这是因为该技术部署于内网办公区, 通过同时动态变换 Server3 和 Host 的 IP 地址, 增加了脆弱性 I4、I5、I6、I7、I8 的不确定性, 所以取得了更为显著的防御效果。与无防御措施相比, 主机安全威胁降低幅度为 27.5%。

5) 若同时部署 3 类 NDD 方案, 会进一步将 Host 面临的安全威胁降低至 0.51568, 与无防御措施相比, 降低幅度为 45.5%。

6 结束语

本文提出一种 NDD 体系的主机安全威胁分析方法, 可用于分析 NDD 体系中多脆弱性多入侵路径情况下主机面临的安全威胁。首先利用随机抽样模型对动态变换给主机脆弱性造成的不确定性进行量化, 并给出入侵者针对单个脆弱性的入侵成功概率计算方法; 然后提出改进的递归深度优先入侵路径搜索算法以避免路径搜索过程中出现自环; 最后基于脆弱性入侵成功概率计算多脆弱性多入侵路径情况下的主机安全威胁。实验

结果表明, 所提方法可适用于多种类型 NDD 技术防护下的主机安全威胁分析。未来将继续研究如何根据主机安全威胁分析结果制订最优 NDD 策略。

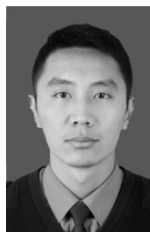
参考文献:

- [1] 蔡桂林, 王宝生, 王天佐, 等. 移动目标防御技术研究进展[J]. 计算机研究与发展, 2016, 53(5):968-987.
CAI G L, WANG B S, WANG T Z, et al. Research and development of moving target defense technology[J]. Journal of Computer Research and Development, 2016, 53(5):968-987.
- [2] 杨林, 于全. 动态赋能网络空间防御[M]. 北京: 人民邮电出版社, 2016.
YANG L, YU Q. Dynamically-enabled cyber defense[M]. Beijing: Post & Telecom Press, 2016.
- [3] 吴迪, 连一峰, 陈恺, 等. 一种基于攻击图的安全威胁识别和分析方法[J]. 计算机学报, 2012, 35(9):1938-1950.
WU D, LIAN Y F, CHEN K, et al. A security threats identification and analysis method based on attack graph[J]. Chinese Journal of Computers, 2012, 35(9):1938-1950.
- [4] CARROLL T E, CROUSE M, FULP E W, et al. Analysis of network address shuffling as a moving target defense[C]// IEEE International Conference on Communications. 2014:701-706.
- [5] LUO Y B, WANG B S, CAI G L. Effectiveness of port hopping as a moving target defense[C]// International Conference on Security

Technology. 2014:7-10.

- [6] HAMLET J R, LAMB C C. Dependency graph analysis and moving target defense selection[C]// ACM Workshop on Moving Target Defense. 2016:105-116.
- [7] 雷程, 马多贺, 张红旗, 等. 基于变点检测的网络移动目标防御效能评估方法[J]. 通信学报, 2017, 38(1):126-140.
- LEI C, MA D H, ZHANG H Q, et al. Performance assessment approach based on change-point detection for network moving target defense[J]. Journal on Communications, 2017, 38(1):126-140.
- [8] ZHUANG R, DELOACH S A, OU X. A model for analyzing the effect of moving target defenses on enterprise networks[C]// Cyber and Information Security Research Conference. 2014:73-76.
- [9] 陈锋, 张怡, 苏金树, 等. 攻击图的两种形式化分析[J]. 软件学报, 2010, 21(4):838-848.
- CHEN F, ZHANG Y, SU J S, et al. Two formal analyses of attack graphs[J]. Journal of Software, 2010, 21(4):838-848.
- [10] YIH H, ANUP K G. Introducing diversity and uncertainty to create moving attack surfaces for Web services[M]// Moving Target Defense. Springer, 2011:131-151.
- [11] CHRISTODORESCU M, FREDRIKSON M, JHA S, et al. End-to-end software diversification of internet services[M]// Moving Target Defense. Springer, 2011:117-130.
- [12] 崔臣浩, 祝跃飞, 李伟, 等. 基于移动目标防御的内网防渗透技术研究[J]. 计算机应用研究, 2016, 33(4):1141-1144.
- CUI C H, ZHU Y F, LI W, et al. Research on inner network permeating prevention based on moving target defense[J]. Application Research of Computers, 2016, 33(4):1141-1144.

[作者简介]



李立勋(1994-), 男, 四川都江堰人, 信息工程大学硕士生, 主要研究方向为动态目标防御。



张斌(1969-), 男, 河南郑州人, 信息工程大学教授、博士生导师, 主要研究方向为网络空间安全。



董书琴(1990-), 男, 河北邢台人, 信息工程大学博士生, 主要研究方向为网络空间态势感知。