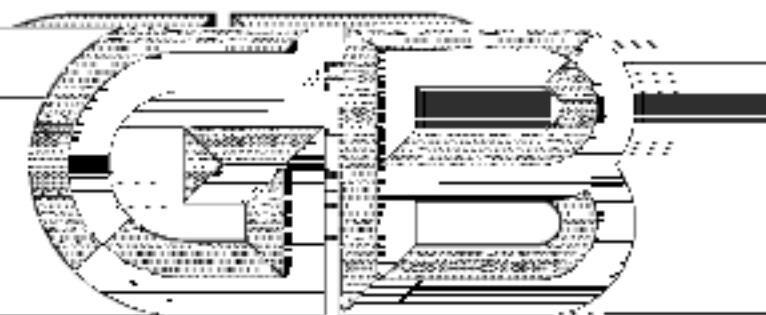




中华人民共和国国家标准

GB/T 36627—2018

信息安全技术 网络安全等级保护测试评估技术指南

Information security technology—
Testing and evaluation technical guide for classified cybersecurity protection

2018-09-17 发布

2019-04-01 实施

国家市场监督管理总局
中国国家标准化管理委员会 发布

目 次

前言	III
引言	IV
1 范围	1
2 规范性引用文件	1
3 术语和定义、缩略语	1
3.1 术语和定义	1
3.2 缩略语	2
4 概述	2
4.1 技术分类	2
4.2 技术选择	2
5 等级测评要求	2
5.1 检查技术	2
5.1.1 文档检查	3
5.1.2 日志检查	3
5.1.3 规则集检查	4
5.1.4 配置检查	4
5.1.5 文件完整性检查	4
5.1.6 密码检查	4
5.2 识别和分析技术	5
5.2.1 网络嗅探	5
5.2.2 网络端口和服务	5
5.2.3 漏洞扫描	5
5.2.4 无线扫描	5
5.3 漏洞验证技术	6
5.3.1 口令破解	6
5.3.2 渗透测试	6
5.3.3 应用漏洞测试	6
附录A 测评用例设计	8
附录B 测评用例设计	8
附录C 测评用例设计	8
附录D 测评用例设计	8
附录E 测评用例设计	8
附录F 测评用例设计	8
附录G 测评用例设计	8
附录H 测评用例设计	8
附录I 测评用例设计	8
附录J 测评用例设计	8
附录K 测评用例设计	8
附录L 测评用例设计	8
附录M 测评用例设计	8
附录N 测评用例设计	8
附录O 测评用例设计	8
附录P 测评用例设计	8
附录Q 测评用例设计	8
附录R 测评用例设计	8
附录S 测评用例设计	8
附录T 测评用例设计	8
附录U 测评用例设计	8
附录V 测评用例设计	8
附录W 测评用例设计	8
附录X 测评用例设计	8
附录Y 测评用例设计	8
附录Z 测评用例设计	8

前言

本标准按照 GB/T 1.1—2009 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

1. 本集团于 2014 年 12 月 31 日及 2015 年 12 月 31 日不存在任何融资租赁业务。

引 言

网络安全等级保护测评过程包括测评准备活动、方案编制活动、现场测评活动、报告编制活动四个

信息安全技术
网络安全等级保护测试评估技术指南

1 范围

2 规范性引用文件

应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文。下列文件对于本文件的应用是必需的。凡是注日期的引用文件,仅注日期的版本适用于本文。下列文件对于本文件的应用是必需的。凡是注日期的引用文件,仅注日期的版本适用于本文。下列文件对于本文件的应用是必需的。

GB 17859-1999—计算机信息系统安全保护等级划分准则

—GB/T 25069—2010—信息安全技术—术语—

3 术语和定义、缩略语

3.1 术语和定义

GB 17859—1999 及 GB/T 25069—2010 界定的以及下列术语和定义适用于本文件。

3.1.1

字典式攻击 **dictionary attack**

在破解口令时,逐一尝试用户自定义词典中的单词或短语的攻击方式。

3.1.2

文件完整性检查 file integrity checking

通过建立文件校验数据库,计算、存储每一个保留文件的校验,将已存储的校验重新计算以比较当前值和存储值,从而识别文件是否被修改。

3.1.3

网络嗅探—network-sniffer

种监测网络通信解密办法,并对关注的信息全部和有效数据进行检查的被动技术,同时配合

[illegible]

规则集 rule set

1998, 1999, 2000, 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009, 2010, 2011, 2012, 2013, 2014, 2015, 2016, 2017, 2018, 2019, 2020, 2021, 2022, 2023, 2024, 2025, 2026, 2027, 2028, 2029, 2030, 2031, 2032, 2033, 2034, 2035, 2036, 2037, 2038, 2039, 2040, 2041, 2042, 2043, 2044, 2045, 2046, 2047, 2048, 2049, 2050, 2051, 2052, 2053, 2054, 2055, 2056, 2057, 2058, 2059, 2060, 2061, 2062, 2063, 2064, 2065, 2066, 2067, 2068, 2069, 2070, 2071, 2072, 2073, 2074, 2075, 2076, 2077, 2078, 2079, 2080, 2081, 2082, 2083, 2084, 2085, 2086, 2087, 2088, 2089, 2090, 2091, 2092, 2093, 2094, 2095, 2096, 2097, 2098, 2099, 2100, 2101, 2102, 2103, 2104, 2105, 2106, 2107, 2108, 2109, 2110, 2111, 2112, 2113, 2114, 2115, 2116, 2117, 2118, 2119, 2120, 2121, 2122, 2123, 2124, 2125, 2126, 2127, 2128, 2129, 2130, 2131, 2132, 2133, 2134, 2135, 2136, 2137, 2138, 2139, 2140, 2141, 2142, 2143, 2144, 2145, 2146, 2147, 2148, 2149, 2150, 2151, 2152, 2153, 2154, 2155, 2156, 2157, 2158, 2159, 2160, 2161, 2162, 2163, 2164, 2165, 2166, 2167, 2168, 2169, 2170, 2171, 2172, 2173, 2174, 2175, 2176, 2177, 2178, 2179, 2180, 2181, 2182, 2183, 2184, 2185, 2186, 2187, 2188, 2189, 2190, 2191, 2192, 2193, 2194, 2195, 2196, 2197, 2198, 2199, 2200, 2201, 2202, 2203, 2204, 2205, 2206, 2207, 2208, 2209, 2210, 2211, 2212, 2213, 2214, 2215, 2216, 2217, 2218, 2219, 2220, 2221, 2222, 2223, 2224, 2225, 2226, 2227, 2228, 2229, 2230, 2231, 2232, 2233, 2234, 2235, 2236, 2237, 2238, 2239, 2240, 2241, 2242, 2243, 2244, 2245, 2246, 2247, 2248, 2249, 2250, 2251, 2252, 2253, 2254, 2255, 2256, 2257, 2258, 2259, 2260, 2261, 2262, 2263, 2264, 2265, 2266, 2267, 2268, 2269, 2270, 2271, 2272, 2273, 2274, 2275, 2276, 2277, 2278, 2279, 2280, 2281, 2282, 2283, 2284, 2285, 2286, 2287, 2288, 2289, 2290, 2291, 2292, 2293, 2294, 2295, 2296, 2297, 2298, 2299, 2300, 2301, 2302, 2303, 2304, 2305, 2306, 2307, 2308, 2309, 2310, 2311, 2312, 2313, 2314, 2315, 2316, 2317, 2318, 2319, 2320, 2321, 2322, 2323, 2324, 2325, 2326, 2327, 2328, 2329, 2330, 2331, 2332, 2333, 2334, 2335, 2336, 2337, 2338, 2339, 2340, 2341, 2342, 2343, 2344, 2345, 2346, 2347, 2348, 2349, 2350, 2351, 2352, 2353, 2354, 2355, 2356, 2357, 2358, 2359, 2360, 2361, 2362, 2363, 2364, 2365, 2366, 2367, 2368, 2369, 2370, 2371, 2372, 2373, 2374, 2375, 2376, 2377, 2378, 2379, 2380, 2381, 2382, 2383, 2384, 2385, 2386, 2387, 2388, 2389, 2390, 2391, 2392, 2393, 2394, 2395, 2396, 2397, 2398, 2399, 2400, 2401, 2402, 2403, 2404, 2405, 2406, 2407, 2408, 2409, 2410, 2411, 2412, 2413, 2414, 2415, 2416, 2417, 2418, 2419, 2420, 2421, 2422, 2423, 2424, 2425, 2426, 2427, 2428, 2429, 2430, 2431, 2432, 2433, 2434, 2435, 2436, 2437, 2438, 2439, 2440, 2441, 2442, 2443, 2444, 2445, 2446, 2447, 2448, 2449, 2450, 2451, 2452, 2453, 2454, 2455, 2456, 2457, 2458, 2459, 2460, 2461, 2462, 2463, 2464, 2465, 2466, 2467, 2468, 2469, 2470, 2471, 2472, 2473, 2474, 2475, 2476, 2477, 2478, 2479, 2480, 2481, 2482, 2483, 2484, 2485, 2486, 2487, 2488, 2489, 2490, 2491, 2492, 2493, 2494, 2495, 2496, 2497, 2498, 2499, 2500, 2501, 2502, 2503, 2504, 2505, 2506, 2507, 2508, 2509, 2510, 2511, 2512, 2513, 2514, 2515, 2516, 2517, 2518, 2519, 2520, 2521, 2522, 2523, 2524, 2525, 2526, 2527, 2528, 2529, 2530, 2531, 2532, 2533, 2534, 2535, 2536, 2537, 2538, 2539, 2540, 2541, 2542, 2543, 2544, 2545, 2546, 2547, 2548, 2549, 2550, 2551, 2552, 2553, 2554, 2555, 2556, 2557, 2558, 2559, 2560, 2561, 2562, 2563, 2564, 2565, 2566, 2567, 2568, 2569, 2570, 2571, 2572, 2573, 2574, 2575, 2576, 2577, 2578, 2579, 2580, 2581, 2582, 2583, 2584, 2585, 2586, 2587, 2588, 2589, 2590, 2591, 2592, 2593, 2594, 2595, 2596, 2597, 2598, 2599, 2600, 2601, 2602, 2603, 2604, 2605, 2606, 2607, 2608, 2609, 2610, 2611, 2612, 2613, 2614, 2615, 2616, 2617, 2618, 2619, 2620, 2621, 2622, 2623, 2624, 2625, 2626, 2627, 2628, 2629, 2630, 2631, 2632, 2633, 2634, 2635, 2636, 2637, 2638, 2639, 2640, 2641, 2642, 2643, 2644, 2645, 2646, 2647, 2648, 2649, 2650, 2651, 2652, 2653, 2654, 2655, 2656, 2657, 2658, 2659, 2660, 2661, 2662, 2663, 2664, 2665, 2666, 2667, 2668, 2669, 2670, 2671, 2672, 2673, 2674, 2675, 2676, 2677, 2678, 2679, 26

Cost of testing and evaluation

测评对象 target

Abstract



3.2 缩略语

下列缩略语适用于本文件。

CNVD:国家信息安全漏洞共享平台(China National Vulnerability Database)

DNS:域名系统(Domain Name System)

DDoS:分布式拒绝服务(Distributed Denial of Service)

ICMP:Internet 控制报文协议(Internet Control Message Protocol)

IDS:入侵检测系统(Intrusion Detection Systems)

IPS:入侵防御系统(Intrusion Prevention System)

MAC:介质访问控制(Media Access Control)

SSH:安全外壳协议(Secure Shell)

SSID:服务集标识(Service Set Identifier)

SQL:结构化查询语言(Structured Query Language)

VPN:虚拟专用网络(Virtual Private Network)

4 概述

4.1 技术分类

可用于等级测评的测评技术分成以下三类。

漏洞验证技术,验证漏洞存在性的测评技术。基于检查、目标识别和手动执行或使用自动化工具,主要包括网络扫描、渗透测试、远程访问安全漏洞进行验证确认,获得证据。

4.2 技术选择

当选择和使用二等级测评活动的技术方法时,应满足国家信息安全等级保护测评专家测评技术通用指南测评技术对测评对象可能引入的安全风险防控措施符合的技术方法。

当使用漏洞验证技术时,应满足国家信息安全等级保护测评专家测评技术通用指南漏洞验证技术对测评对象可能引入的安全风险防控措施符合的技术方法。

当使用漏洞验证技术时,应满足国家信息安全等级保护测评专家测评技术通用指南漏洞验证技术对测评对象可能引入的安全风险防控措施符合的技术方法。

5 等级测评要求

5.1 检查技术

5.1.1 文档检查

文档检查的主要功能是其于等级保护对象运营单位提供的文档,评价其策略和规程

和完整性。进行文档检查时,可考虑以下评估要素:

- a) 检查对象包括安全策略、体系结构和要求、标准作业程序、系统安全计划和授权许可、系统互连

三、技术规范, 事先的行动计划等, 确保技术的准确性和可靠性

②) 检查安全策略、体系结构和要求、保护令、程序、系统安全计划、授权策略、系统互连协议、规程、事件响应计划等文档的完整性。通过检查执行记录和相关表单,确认被测方安全措施落实,并与制度文档保持一致。

c) 一發即可能導致沸溫或天檢當所定施安全控制措施於該情形時應

中國經濟的未來取決於中國經濟安全體系能否真正建立起來。在我們
筆下。

③ 文档检查的结果可用于调整其他的测试技术。例如,当配置管理策略规定了覆盖率要求的时候,该信息可用于配置工具破解工具,以提高工具破解效率。

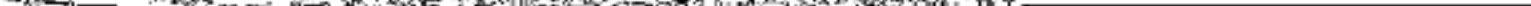
5.1.2 日志检查

日志检查的主要功能是验证安全控制措施是否记录了测评对象的信息系统、设备和修改的历史记录等适当信息,等级保护对象的运营使用单位是否坚持了日志管理策

- **数据库系统日志**：记录数据库或表级操作的结果。
- **操作系统日志**：包括系统和数据库启动、关闭、未授权软件的安装、文件访问、安全变更(例如账户创建和删除、账户权限分配)以及权限使用等信息。
- **IDS日志**：包括报警信息和安全事件。

——《共产党宣言》——

Figure 1. The study area, showing the location of the study area in the north-east of Iran, and the location of the study area in the north-east of Iran.



5.1.3 规则集检查

规则集检查的主要功能是发现基于规则集的安全控制措施的漏洞,检查对象包括网络设备、服务器、数据库、操作系统及应用系统的访问控制列表、策略集。二级及以上等级保护对象还应包括扫描漏洞。进行规则集检查时,应参考以下二级以上等级保护对象的保护原则:

- 2) 勝山訪問控制列表

各規則和規定在教學計劃中用藍色表示而特定的規則在不重要的時候被省略

Figure 6

[illegible]

相同的访问规则；

- 3) 以文件形式存储和操作的用户数据,在操作系统的支持下,应实现文件级精度的强制访问

控制；

- 3.2 以数据库形式存储和操作的用户数据,在数据库管理系统的支持下,应实现表、记录

级粒度的强制访问控制；

- 4) 检查强制访问控制的范围,应限定在已定义的主体与客体中。

5.1.4 配置检查

配置检查的主要功能是通过检查测评对象的安全策略设置和安全配置文件,评价测评对象安全策略配置的强度,以及验证测评对象安全策略配置与测评对象安全加固策略的符合程度。进行配置检查时,可考虑以下评估要素:

- a) 依据安全策略进行加固或配置;

- 1) 应实施以两因素认证和加密,以及可验证安全策略控制;

- c) 用户账号的唯一性标识和口令复杂度设置;

- 1) 应实施以两因素认证和加密,以及可验证安全策略控制;

- e) 合理设置文件访问权限;

- f) 三级及以上等级保护措施;

- 1) 应由系统安全员创建;

- 2) 实施相同强制访问;

- 3) 检查标记的范围,应

5.1.5 文件完整性检查

可考虑以下评估要素:

- a) 采用哈希或数字签

- 1) 应采用哈希或数字签

- 2) 应采用哈希或数字签

5.1.6 密码检查

密码检查的主要功能是
可考虑以下评估原则:

- a) 所提供的密码算法

- 1) 应使用经国家密码

5.2 识别和分析技术

5.2.1 网络嗅探

网络嗅探的主要功能
未授权和不恰当的行为

能是通过捕捉和重放网络流量,收集、识别网络中活动的设备、操作系统和协议、
息信息。进行网络嗅探时,可考虑以下评估要素和评估原则

- a) 网络嗅探设备应安装在网络中活动的设备、操作系统和协议、

- 1) 应安装在网络中活动的设备、操作系统和协议、

- 2) 应安装在网络中活动的设备、操作系统和协议、

- 响或干扰操作系统和网络服务的数据库已知的正在运行的操作系统、端

口及端口的状态。

- d) 在网络边界处部署网络嗅探器,用以评估进出网络的流量;

e) 在网络边界处部署网络嗅探器,用以评估进出网络的流量;

5.2.2 网络端口和服务识别

网络端口和服务识别的主要功能是识别活动设备上开放的端口、相关服务与应用程序。端口和服务识别时,可考虑以下评估要素和评估原则:

- 对主机及存在潜在漏洞的端口进行识别,并用于确定渗透性测试的目标;
- 在从网络边界外执行扫描时,应使用含分离、复制、重叠、乱序和定时技术的工具,并改变数据包,让数据包融入正常流量中,使数据包避开 IDS/IPS 检测的同时穿越防火墙;
- 应尽量减少扫描工具对网络运行的干扰,如选择端口扫描的时间。

5.2.3 漏洞扫描

漏洞扫描的主要功能是针对主机和开放端口识别已知漏洞、提供建议降低漏洞风险;同时识别过时的软件版本、缺失的补丁和错误配置,并验证其与机构安全策略的一致性。进行漏洞扫描时,可考虑以下评估要素和评估原则:

- 识别漏洞扫描工具是否支持目标系统,并用于确定扫描工具;
- 在从网络边界外执行扫描时,应使用含分离、复制、重叠、乱序和定时技术的工具,并改变数据包,让数据包融入正常流量中,使数据包避开 IDS/IPS 检测的同时穿越防火墙;
- 应尽量减少扫描工具对网络运行的干扰,如选择扫描的时间。
- 识别漏洞扫描工具是否支持目标系统,并用于确定扫描工具;
- 在从网络边界外执行扫描时,应使用含分离、复制、重叠、乱序和定时技术的工具,并改变数据包,让数据包融入正常流量中,使数据包避开 IDS/IPS 检测的同时穿越防火墙;
- 应尽量减少扫描工具对网络运行的干扰,如选择扫描的时间。

5.2.4 无线扫描

无线扫描的主要功能是针对无线设备识别已知漏洞、提供建议降低漏洞风险;同时识别过时的软件版本、缺失的补丁和错误配置,并验证其与机构安全策略的一致性。进行无线扫描时,可考虑以下评估要素和评估原则:

- 识别无线扫描工具是否支持目标系统,并用于确定扫描工具;
- 在从网络边界外执行扫描时,应使用含分离、复制、重叠、乱序和定时技术的工具,并改变数据包,让数据包融入正常流量中,使数据包避开 IDS/IPS 检测的同时穿越防火墙;
- 应尽量减少扫描工具对网络运行的干扰,如选择扫描的时间。
- 识别无线扫描工具是否支持目标系统,并用于确定扫描工具;
- 在从网络边界外执行扫描时,应使用含分离、复制、重叠、乱序和定时技术的工具,并改变数据包,让数据包融入正常流量中,使数据包避开 IDS/IPS 检测的同时穿越防火墙;
- 应尽量减少扫描工具对网络运行的干扰,如选择扫描的时间。

5.3 漏洞验证技术

5.3.1 口令破解

口令破解的主要功能是在评估过程中通过采用暴力猜测(密码穷举)、字典攻击等技术手段验证数据库、操作系统、应用系统、设备的管理员口令复杂度。进行口令破解时,可考虑以下评估方法和评估原则:

- a) 使用字典式攻击方法或采用预先计算好的彩虹表(散列值查找表)进行口令破解尝试;
- b) 使用混合攻击或暴力破解的方式进行口令破解;混合攻击以字典攻击方法为基础,在字典中增

加了新密码和原口令的

组合,攻击效率更高;

尝试;

c) 如被测对象采用带有益值的加密散列函数时,不宜使用彩虹表方式进行口令破解

采用穷举或字典攻击方式破解的效率

比使用暴力破解时,会

5.3.2 渗透测试

客户的攻击方法,攻击等级保护对象的应用程序、系统或者网络缺陷或漏洞的一种评估方法。进行渗透测试时,可考虑以

存在:

系统、数据库、中间件等为应用系统提供服务或支撑的环境;

缓冲区溢出漏洞(堆/栈溢出)、内存泄露等,可能造成程序

等后果;更为严重的,可以导致程序执行非授权指令,甚至

非法操作;

员编写代码不规范或缺少必要的校验措施,导致应用系统

、跨站脚本、任意上传文件等漏洞;攻击者可利用这些漏洞,

窃取敏感信息或敏感信息,更严重的,可以导致系统瘫痪

数据访问功能模块访问控制规则不严或存在缺失,导致攻击者

能模拟二、权限旁路类漏洞通常可分为越权访问及并行权限,

授权访问高权限用户的功能模块或数据信息,并行权限是指

模块,非授权访问或操作他人的数据信息。

配置文件进行安全加固,仅使用默认配置或配置不合理,所导

置支持http方法,可能给攻击者利用,http方法上传木马文

渗透测试的主要功能是通过模拟恶意网络的安全功能,从而验证测评对象弱点、技术下评估要素和评估原则:

- a) 通过渗透测试评估确认以下漏洞的

1) 系统(服务)类漏洞。由于操作系

存在缺陷,所导致的安全漏洞,

运行失败、系统宕机、重新启动

取得系统特权,进而进行各种非

2) 应用代码类漏洞。由于开发人

存在安全漏洞,包括 SQL 注入

等漏洞,系统被攻击或破坏范

漏洞;

3) 权限旁路类漏洞。由于对数

可非授权访问这些数据及非

越权访问是指低权限用户非

攻击者利用自身权限的功能

4) 配置不当类漏洞。由于未对

致的安全风险,如中间件配

存在漏洞,攻击者利用漏洞使

一、信息泄露类漏洞。攻击者

5.3.3 远程访问测试

远程访问测试的主要功能是评估远程访问方法中的漏洞,发现未授权的接入方式。进行远程访问测试时,可考虑以下评估要素和评估原则:

- a) 发现除 VPN、SSH、远程桌面应用之外是否存在其他的非授权的接入方式。
- b) 发现未授权的远程访问服务。通过端口扫描定位经常用于进行远程访问的公开的端口,通过查看运行的进程和安装的应用来手工检测远程访问服务。
- c) 检测规则集来查找非法的远程访问路径。评估者应检测远程访问规则集,如 VPN 网关的规则集,查看其是否存在漏洞或错误的配置,从而导致非授权的访问。
- d) 测试远程访问认证机制。可尝试默认的账户和密码或暴力攻击(使用社会工程学的方法重设密码来进行访问),或尝试通过密码找回功能机制来重设密码从而获得访问权限。

~~c) 嗅探远程访问通信。可以通过网络嗅探器监视远程访问通信。如果通信未被加密,则可得到这些通信数据作为远程访问的认证信息,或者将这些数据作为远程访问用户发送或接收的数据。~~

附录 A
(资料性附录)
测评后活动

A.1 测评结果分析

测评结果分析的主要目标是确定和排除误报,对漏洞进行分类,并确定产生漏洞的原因,此外,找出在整个测评中需要立即处理的严重漏洞。以下列举了常见的造成漏洞的根本原因,包括:

- a) 威胁模型不足,未及时更新威胁模型,导致的安全策略不能及时反映最新威胁及不兼容安全策略的防火墙策略等;
- b) 缺乏安全基准,同类的系统使用了不一致的安全配置策略;
- c) 在系统开发中缺乏对安全性的整合,如系统开发不满足安全要求,甚至未考虑应用程序代码中是否存在漏洞;
- d) 安全体系结构存在缺陷,如安全技术未能有效地集成至系统中(例如,安全防护设备不能有效集成至安全策略中);
- e) 安全策略的响应策略不完善,如未及时更新策略策略;
- f) 安全策略的更新不及时,如未及时更新策略策略;
- g) 安全策略的更新不及时,如未及时更新策略策略;
- h) 安全策略的更新不及时,如未及时更新策略策略;
- i) 安全策略的更新不及时,如未及时更新策略策略;
- j) 安全策略的更新不及时,如未及时更新策略策略;
- k) 安全策略的更新不及时,如未及时更新策略策略;
- l) 安全策略的更新不及时,如未及时更新策略策略;
- m) 安全策略的更新不及时,如未及时更新策略策略;
- n) 安全策略的更新不及时,如未及时更新策略策略;
- o) 安全策略的更新不及时,如未及时更新策略策略;
- p) 安全策略的更新不及时,如未及时更新策略策略;
- q) 安全策略的更新不及时,如未及时更新策略策略;
- r) 安全策略的更新不及时,如未及时更新策略策略;
- s) 安全策略的更新不及时,如未及时更新策略策略;
- t) 安全策略的更新不及时,如未及时更新策略策略;
- u) 安全策略的更新不及时,如未及时更新策略策略;
- v) 安全策略的更新不及时,如未及时更新策略策略;
- w) 安全策略的更新不及时,如未及时更新策略策略;
- x) 安全策略的更新不及时,如未及时更新策略策略;
- y) 安全策略的更新不及时,如未及时更新策略策略;
- z) 安全策略的更新不及时,如未及时更新策略策略;

A.2 提出改进建议

针对每个漏洞,应提出具体的改进建议,如:对于高危漏洞,应立即采取整改措施;对于中危漏洞,应在规定时间内采取整改措施;对于低危漏洞,应在规定时间内采取整改措施。改进建议应具体、可操作,并应明确责任人和完成时间。

A.3 报告

在测评结果分析完成后,应生成包括系统安全问题、漏洞及其改进建议的报告。报告应包括以下方面:

- a) 作为实施改进措施的依据;
- b) 制定改进措施的时间表;
- c) 作为制定安全策略的依据,如系统级安全策略、安全要求而未在改进措施中;
- d) 作为制定安全策略的依据,如系统级安全策略、安全要求而未在改进措施中;
- e) 为改进系统提供依据的安全而进行的安全检查;
- f) 用于跟踪其他生命周期活动,如风险评估;
- g) 用于跟踪网络安全策略的更新和改进措施。

附录 B
(资料性附录)
渗透测试的有关概念说明

B.1 综述

渗透测试是一种安全性测试,在该类测试中,测试人员将模拟攻击者,利用攻击者常用的工具和技术对应用程序、信息系统或者网络的安全功能发动真实的攻击。相对于单一的漏洞,大多数渗透测试试图寻找一组安全漏洞,从而获得更多能够进入系统的机会。渗透测试也可用于确定:

- b) 攻击者需要成功破坏系统所面对的大体复杂程度;
- c) 可减少系统威胁的其他对策;
- d) 防御者能够检测攻击并且做出正确反应的能力。

渗透测试是一种非常重要的安全测试,测试人员需要丰富的专业知识和技能。尽管有经验的测试人员可以降低这种风险,但不等完全避免风险。某些渗透测试通常包括非技术攻击方法。例如,一个渗透测试人员在互联网上搜索敏感数据,直接收集信息可能通过物理安全渗透测试而能直接获取。明确如何验证测试文档。另一种非技术攻击手段是通过社会工程学,如伪装成用户打电话给客服坐席人员要求重置密码。更多关键技术手段的渗透攻击测试,不在本标准的讨论范围。

B.2 渗透测试阶段

B.2.1 概述

渗透测试通常包括规划、发现、攻击、报告四个阶段,

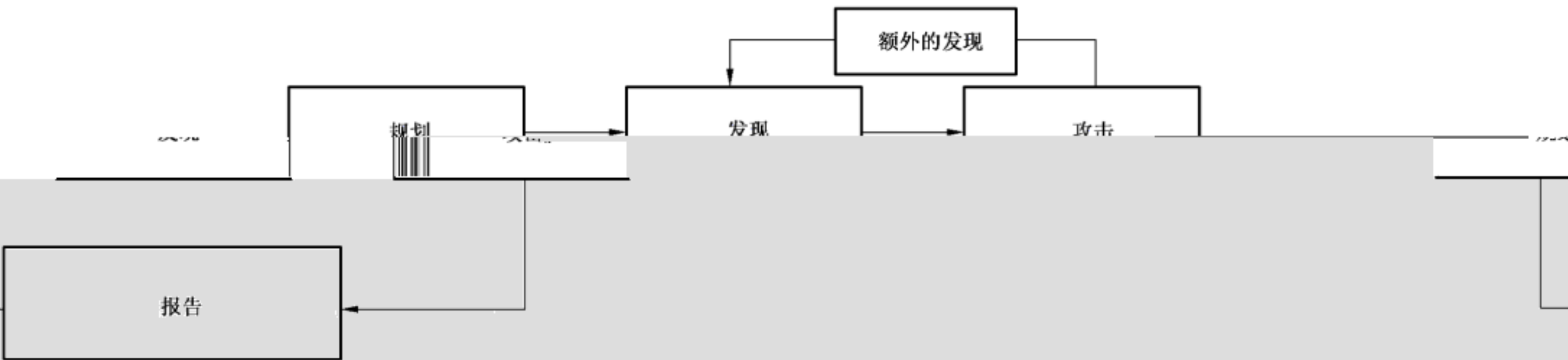


图 B.1 渗透测试的四个阶段

B.2.2 规划阶段

在规划阶段,确定规则测试奠定基础,在该阶段不

B.2.3 发现阶段

渗透测试的发现阶段包括两个部分：

[illegible]

B.2.4 攻击阶段

[illegible]

R 25 报告阶段

其他三个阶段同时进行(见图 B.1)。在规划阶段,将编写测试计划;在发现记录并定期向系统管理员和/或管理部门报告。在测试结束后,报告通常

B.3 渗透测试方案

在应用程序、系统或网络中的设计和实现中,定位和挖掘出可利用的漏洞缺
和最具破坏性的攻击模式,包括最坏的情况,诸如管理员的恶意行为。由于
攻击者通常攻击系统薄弱环节,或被忽视的部分,因此外部渗透测试通常比内部
渗透测试都要执行,则通常优先执行外部测试。

从外部发起的攻击行为,可能来自那些对组织内部信息一无所知的攻击者。模
拟一个外部攻击,测试人员不知道任何关于目标环境以外的信息,特别是 IP 地址或地址范围情况的真
实信息。攻击者通常利用公共信息源,如搜索引擎、网络目录、公开数据库、新闻组、
搜索引擎和目录索引,从而收集关于目标系统所需信息,如 IP 地址范围、域名、
网络名称、测试系统名称等。从外部进行网络系统或网络上的主机测试,通常比内部测试
将更容易发现漏洞,它模拟攻击者的攻击方法,攻击者通常通过网络或物理媒介,在攻击目标上
实施渗透测试是一个迭代的过程,利用攻击者的知识限制攻击以及发现漏洞。

内部攻击是模拟组织内部违规操作者行为。除了测试人员位于内部网络(即防火墙后面)之外,还授予对网络或特定系统一定程度的访问权限(通常是作为一个用户,但有时是更高权限)。内部渗透测试与外部测试类似。测试人员可以访问权限提升获得更大范围的网络及系统测试权限。

[illegible]

B.4 渗透测试风险

在渗透测试过程中,测试人员通常会利用攻击者常用的工具和技术来对被测系统和数据发动攻击。因此,白盒测试会模拟攻击者从外部对系统进行攻击,并模拟攻击者可能使用的各种攻击手段,如SQL注入、跨站脚本攻击(XSS)、跨站请求伪造(CSRF)等。而黑盒测试则模拟攻击者从外部对系统进行攻击,但不了解系统的内部结构,只通过系统的输入输出来进行测试。

- 在利用 Web 盈利方面，互联网营销公司所起的作用会令 Web 服务器开发商感到吃惊。据估计，目前，一些网络服务提供商已经可以占到前 10 家 Web 服务器提供商利润的 50%。而像 Amazon 这样的大型零售商则能够占到 20%。亚马逊公司每年在 Web 服务器上的投入高达 10 亿美元。而 Web 盈利方面所占比例会随着时间的增长而增长。《福布斯》杂志最近指出，在未来 5 年内，网络服务提供商的利润将占到 Web 服务器提供商总利润的 60%。

Figure 1. The location of the study area.

- 在对 Web 应用程序、操作系统、数据库等进行命令暴力破解时，可能触发导致 Web 应用程序、操作系统、数据库的账号被锁定，暂时无法使用；
- 在进行主机远程漏洞扫描及进行主机、数据库溢出类攻击测试，极端情况会引发操作系统、数据库崩溃死机或重启现象。

B.5 渗透测试风险规避

2007年12月26日 星期三 12:00

THE FUTURE OF THE FUTURE

不刊之論

——《中国农村经济》1992年第1期

[!\[\]\(1e785a35c87067562e5eed96a1b6021d_img.jpg\)
 首页](#)
[!\[\]\(879e46fb952806e82ed7b0cab5f1aa5c_img.jpg\)
 产品](#)
[!\[\]\(16ef78d01996d00cdee57a3e8de2f72f_img.jpg\)
 服务](#)
[!\[\]\(1f0b3d71821c34df1f6fa670bb0b6211_img.jpg\)
 案例](#)
[!\[\]\(3982afd0e39e028e4f7c0bbdfca933ba_img.jpg\)
 关于](#)
[!\[\]\(4448a15d7ac23de0434bcbee4d774a1f_img.jpg\)
 联系](#)

何慶基經理人：胡大為

[illegible]

Figure 1. The proposed model for the development of the self-regulated learning strategy.

[illegible]

中止渗透测试,并配合用户进行修复处理;在确认问题并恢复系统后,经用户同意方可继续进行其余的测试;

- e) 沟通机制:在测试前,宜确定测试人员和用户配合人员的联系方式,用户方宜在测试期间安排专人职守,与测试人员保持沟通,如发生异常情况,可及时响应;测试人员宜在测试结束后要求用户检查系统是否正常,以确保系统的正常运行。

参 考 文 献

[1] GB/T 20269—2006 信息安全技术 信息系统安全管理要求

[2] GB/T 20270—2006 信息安全技术 网络基础安全技术要求

[3] GB/T 20288—2006 信息安全技术 信息系统安全 工程的要求

[4] GB/T 22239—信息安全技术 信息系统安全等级保护基本要求

[5] GB/T 28446—信息安全技术 信息系统安全等级保护测评要求

[6] GB/T 28449—信息安全技术 信息系统安全等级保护测评过程指南

中 华 人 民 共 和 国
国 家 标 准
信息安全技术
网络安全等级保护测试评估技术指南
GB/T 36627—2018

*

中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)

网址: www.spc.org.cn

服务热线: 400-168-0010

2018年9月第一版

*

书号: 155066 · 1-61231

版权专有 侵权必究



GB/T 36627-2018