1. 概述 1.1 任务信息 本次任务共发现 0 个资产, 1 个存活ip, 1 个开放端口。经详细分析, 共0个软件产品 0 2 漏洞 端口 资产 存活IP 1.2 任务详情 任务名 测试es3 192.168.31.31 ΙP 20 23 135 445 80 8080 9200 6379 5601 8081 3000 8983 端口 漏洞 社区版poo 1.3 资产分布 1.3.1 软件资产分布 直接访问 邮件营销 ■ 联盟广告 1.3.2 端口资产分布 9200 9200 100% 总共: 1 2. 漏洞 漏洞poc xss/reflected/default dirscan/debug/php dirscan/directory/default dirscan/debug/php baseline/sensitive/server-error xss/reflected/default dirscan/code/git dirscan/debug/readme dirscan/debug/readme dirscan/temp/default dirscan/debug/readme dirscan/code/git dirscan/admin/phpmyadmin dirscan/code/git dirscan/directory/default dirscan/directory/default dirscan/directory/default dirscan/directory/default dirscan/directory/default dirscan/directory/default dirscan/directory/default dirscan/directory/default dirscan/directory/default dirscan/temp/default dirscan/directory/default dirscan/directory/default dirscan/directory/default brute-force/form-brute/default dirscan/directory/default dirscan/directory/default dirscan/directory/default dirscan/directory/default dirscan/directory/default dirscan/directory/default dirscan/directory/default dirscan/directory/default cmd-injection/code/php brute-force/form-brute/default dirscan/directory/default dirscan/directory/default dirscan/directory/default dirscan/directory/default upload/upload/default cmd-injection/injection/cmd upload/upload/default dirscan/directory/default dirscan/directory/default dirscan/directory/default dirscan/directory/default brute-force/form-brute/default xss/reflected/default dirscan/directory/default xss/reflected/default dirscan/directory/default xss/reflected/default xss/reflected/default xxe/xxe/echo dirscan/directory/default dirscan/directory/default xss/reflected/default dirscan/directory/default baseline/sensitive/server-error sqldet/error-based/default baseline/sensitive/server-error sqldet/error-based/default baseline/sensitive/server-error sqldet/error-based/default sqldet/blind-based/default sqldet/blind-based/default dirscan/directory/default saldet/blind-based/default sqldet/blind-based/default dirscan/directory/default path-traversal/path-traversal/default path-traversal/path-traversal/default baseline/sensitive/server-error brute-force/form-brute/default redirect/redirect/default > baseline/sensitive/server-error sqldet/error-based/default sqldet/blind-based/default xss/reflected/default sqldet/error-based/default dirscan/directory/default dirscan/directory/default dirscan/directory/default dirscan/directory/default xss/reflected/default dirscan/directory/default dirscan/directory/default dirscan/directory/default dirscan/directory/default dirscan/directory/default dirscan/directory/default dirscan/directory/default xss/reflected/default xss/reflected/default brute-force/form-brute/default dirscan/directory/default sqldet/blind-based/default sqldet/blind-based/default sqldet/blind-based/default xss/reflected/default 192.168.137 80 dirscan/debug/php 192.168.137 80 dirscan/directory/default 192.168.137 80 dirscan/debug/php 192.168.137 80 baseline/sensitive/server-error 192.168.137 8080 xss/reflected/default 192.168.137 8089 dirscan/debug/php 192.168.137 80 dirscan/debug/php 192.168.137.2 80 dirscan/debug/php 192.168.137.3 80 dirscan/debug/php 192.168.137.4 80 dirscan/debug/php 192.168.137.6 80 dirscan/debug/php 192.168.137.7 80 dirscan/debug/php 192.168.137.8 80 dirscan/debug/php 192.168.137.16 80 dirscan/debug/php 192.168.137.17 80 dirscan/debug/php 192.168.137.18 80 dirscan/debug/php 192.168.137.19 80 dirscan/debug/php 192.168.137.20 80 dirscan/debug/php 192.168.137.21 80 dirscan/debug/php 192.168.137.22 80 dirscan/debug/php 192.168.137.23 80 dirscan/debug/php 192.168.137.24 80 dirscan/debug/php 192.168.137.25 80 dirscan/debug/php 192.168.137.26 80 dirscan/debug/php 192.168.137.27 80 dirscan/debug/php 192.168.137.28 80 dirscan/debug/php 192.168.137.29 80 192.168.137.30 dirscan/debug/php 80 192.168.137.32 dirscan/debug/php 80 192.168.137.33 dirscan/debug/php 80 192.168.137.34 dirscan/debug/php 80 dirscan/debug/php 192.168.137.5 80 192.168.137.36 dirscan/debug/php 80 192.168.137.38 dirscan/debug/php 80 dirscan/debug/php 192.168.137.39 80 192.168.31.30 dirscan/debug/default 8080 baseline/sensitive/server-error 192.168.31.30 8080 192.168.31.30 dirscan/debug/default 8080 192.168.31.30 poc-go-tomcat-put 8080 poc-yaml-tomcat-cve-2017-12615-rce 192.168.31.30 8080 192.168.31.30 poc-yaml-tomcat-cve-2017-12615-rce 8080 poc-yaml-tomcat-cve-2017-12615-rce 192.168.31.30 8080 192.168.31.30 baseline/sensitive/server-error 8080 192.168.31.30 baseline/sensitive/server-error 8080 dirscan/config/dependence 192.168.31.37 8080 192.168.31.37 dirscan/config/dependence 8080 poc-yaml-phpunit-cve-2017-9841-rce 192.168.31.37 8080 192.168.31.37 dirscan/debug/default 8080 poc-vaml-kibana-unauth 192.168.31.34 5601 poc-yaml-kibana-cve-2018-17246 192.168.31.34 5601 192.168.31.39 baseline/sensitive/server-error 8983 dirscan/admin/solr 192.168.31.39 8983 poc-vaml-kibana-cve-2018-17246 192.168.31.204 5601 poc-yaml-kibana-unauth 192.168.31.204 5601 192.168.31.215 baseline/sensitive/server-error 8983 dirscan/admin/solr 192.168.31.215 8983 192.168.31.217 dirscan/config/dependence 8080 192.168.31.217 dirscan/config/dependence 8080 poc-vaml-phpunit-cve-2017-9841-rce 192.168.31.217 8080 192.168.31.217 dirscan/debug/default 8080 192.168.31.203 dirscan/debug/readme 8080 dirscan/debug/readme 192.168.31.203 8080 192.168.31.203 dirscan/debug/readme 8080 192.168.31.33 dirscan/debug/readme 8080 192.168.31.33 dirscan/debug/readme 8080 192.168.31.33 dirscan/debug/readme 8080 dirscan/debug/default 192.168.31.200 8080 192.168.31.200 poc-go-tomcat-put 8080 192.168.31.200 dirscan/debug/default 8080 baseline/sensitive/server-error 192.168.31.200 8080 192.168.31.200 poc-yaml-tomcat-cve-2017-12615-rce 8080 poc-yaml-tomcat-cve-2017-12615-rce 192.168.31.200 8080 192.168.31.200 poc-yaml-tomcat-cve-2017-12615-rce 8080 192.168.31.200 baseline/sensitive/server-error 8080 192.168.31.200 baseline/sensitive/server-error 8080 baseline/sensitive/server-error 192.168.31.32 8080 192.168.31.32 8080 baseline/sensitive/server-error 192.168.31.32 baseline/sensitive/server-error 8080 192.168.31.32 baseline/sensitive/server-error 8080 192.168.31.32 8080 baseline/sensitive/server-error 192.168.31.32 baseline/sensitive/server-error 8080 baseline/sensitive/server-error 192.168.31.214 8080 192.168.31.214 baseline/sensitive/server-error 8080 192.168.31.214 baseline/sensitive/server-error 8080 192.168.31.214 baseline/sensitive/server-error 8080 192.168.31.214 baseline/sensitive/server-error 8080 baseline/sensitive/server-error 192.168.31.214 8080 192.168.31.214 baseline/sensitive/server-error 8080 192.168.31.214 baseline/sensitive/server-error 8080 192.168.31.214 baseline/sensitive/server-error 8080 192.168.31.214 baseline/sensitive/server-error 8080 baseline/sensitive/server-error 192.168.31.214 8080 192.168.31.214 baseline/sensitive/server-error 8080 192.168.31.214 baseline/sensitive/server-error 8080 192.168.31.214 baseline/sensitive/server-error 8080 192.168.31.214 baseline/sensitive/server-error 8080 baseline/sensitive/server-error 192.168.31.214 8080 192.168.31.214 baseline/sensitive/server-error 8080 192.168.31.214 baseline/sensitive/server-error 8080 192.168.31.214 baseline/sensitive/server-error 8080 192.168.31.214 8080 baseline/sensitive/server-error baseline/sensitive/server-error 192.168.31.214 8080 poc-yaml-elasticsearch-unauth 192.168.31.31 9200 poc-yaml-elasticsearch-cve-2014-3120 192.168.31.31 9200 2. 资产 IP 端口 服务 协议 主机系统 192.168.31.31 tcp