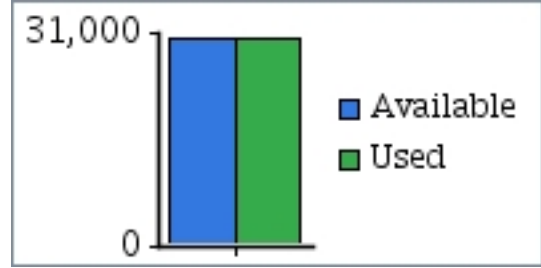


HackerGuardian Audit Report

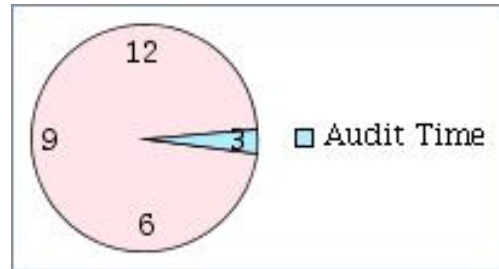
Summary

Plugins available: 30271
Plugins Used: 30271



Options:
 safe_checks = yes
 max_checks = 4
 optimize_test = no
 port_range = default
 use_mac_addr = no
 Netstat scanner = no
 Exclude toplevel domain wildcard host = yes
 Scan for LaBrea tarpitted hosts = no
 Ping the remote host = no
 Nessus TCP scanner = no
 Nmap (NASL wrapper) = no
 SYN Scan = no

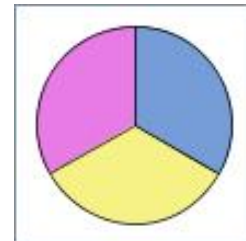
Time started: Sat Sep 19 02:53:44 UTC
Time finished: Sat Sep 19 03:17:54 UTC
Audit time: 00:24:10



<input type="checkbox"/>	Device scanned:	1
<input type="checkbox"/>	Security Holes:	0
<input type="checkbox"/>	Security Warnings:	0
<input type="checkbox"/>	Security Notes:	3



<input type="checkbox"/>	General remote services (Service detection)	1
<input type="checkbox"/>	Firewalls	1
<input type="checkbox"/>	General remote services (General)	1



List of devices scanned:	Security Holes	Security Warnings	Security Notes
208.109.121.165	0	0	3

 Security information found on port/service "general/tcp"

Plugin "Host FQDN"
Category "General "
Priority "Low Priority"
208.109.121.165 resolves as ip-208-109-121-165.ip.secureserver.net.

 Security information found on port/service "general/tcp"

Plugin "Try very hard to identify what runs on common ports"
Category "Service detection "
Priority "Low Priority"
Synopsis :
This plugin performs service detection.
Description :
This plugin is a complement of find_service1.nasl. It attempts to identify common services which might have been missed because of a network problem.

 Risk factor :


None

Plugin output :

While trying to identify services on common ports,
Nessus got 8 timeouts on 8 connection attempts.
The remote machine is probably firewalled.
To get quicker tests, you should restrict the port range
and set "Consider unscanned ports as closed".

 Security information found on port/service "general/tcp"

Plugin "Firewall Enabled"
Category "Firewalls "
Priority "Low Priority"
Synopsis :
The remote host is behind a firewall
Description :
Based on the responses obtained by the TCP scanner, it was possible to determine that the remote host seems to be protected by a firewall.

 Solution :
None Risk factor :

None

Mitigation Plan

You must undertake the following remedial actions or provide us with the relevant information if you think the vulnerabilities are already patched or if compensating controls exist:

We recommend you undertake the following remedial actions:



None.