HELIXSTORM

SECURITY ASSESSMENT

RISK REPORT

Prepared by: Helixstorm
Prepared for: Prospect Or Customer 12/3/2014

DISCOVERY TASKS

The following discovery tasks were performed:

	TASK	DESCRIPTION
✔	Detect System Protocol Leakage	Detect protocols that should not be allowed outbound.
✔	Detect Unrestricted Protocols	Detect system controls for protocols that should be allowed but restricted.
✔	Detect User Controls	Determine if controls are in place for user web browsing.
	Detect Wireless Access	Detect and determine if wireless networks are available and secured.
✔	External Security Vulnerabilities	Perform detailed External Vulnerability Scan. List and categorize external security threats.
✔	Network Share Permissions	Document access to file system shares.
✔	Domain Security Policy	Document domain computer and domain controller security policies.
✔	Local Security Policy	Document and assess consistency of local security policies.

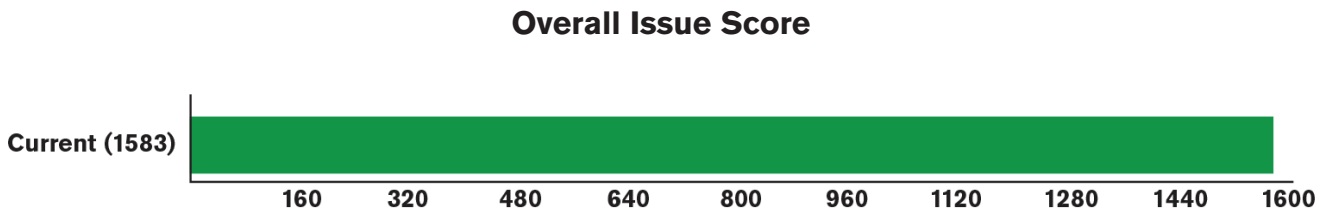
RISK SCORE

The Risk Score is a value from 1 to 100, where 100 represents significant risk and potential issues.

Several critical issues were identified. Identified issues should be investigated and addressed according to the Management Plan.

ISSUES SUMMARY

This section contains summary of issues detected during the Security Assessment. It is based on general best practices and may indicate existing issues or points of interest.



Critical External Vulnerabilities Detected (95 pts)

Issue: External vulnerabilities may potentially allow malicious attacks from outside your network and should be addressed as soon as possible. External vulnerabilities are considered potential security holes that can allow hackers access to your network and information.
Recommendation: We recommend assessing the risk of each vulnerability and remediating all external vulnerabilities as prescribed.

Account lockout disabled (77 pts)

Issue: Account lockout (disabling an account after a number of failed attempts) significantly reduces the risk of an attacker acquiring a password through a brute force attack.
Recommendation: Enable account lockout for all users.

Medium Severity External Vulnerabilities Detected (75 pts)

Issue: External vulnerabilities may potentially allow malicious attacks from outside your network and should be addressed as soon as possible. External vulnerabilities are considered potential security holes that can allow hackers access to your network and information.
Recommendation: We recommend assessing the risk of each vulnerability and remediating all external vulnerabilities as prescribed.

Automatic screen lock not turned on. (72 pts)

Issue: Automatic screen lock prevents unauthorized access when users leave their computers. Having no screen lock enable allows authorized access to network resources.
Recommendation: Enable automatic screen lock on the specified computers.

Password history not remembered for at least 6 passwords (72 pts)

Issue: Short password histories allow users to rotate through a known set of passwords, thus reducing the effectiveness of a good password management policy.
Recommendation: Increase password history to remember at least 6 passwords.

Inconsistent password policy / Exceptions to password policy (68 pts)

Issue: Password policies are not consistently applied from one computer to the next. A consistent password policy ensure adherence to password best practices.
Recommendation: Eliminate inconsistencies and exceptions to the password policy.

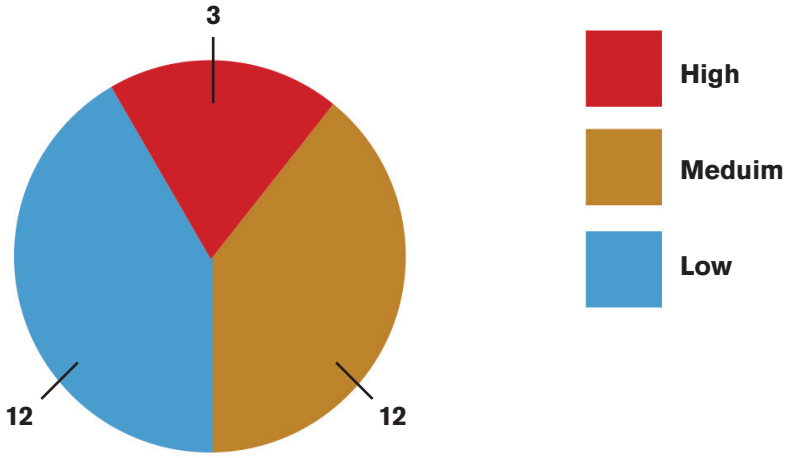
Lack of Web Filtering (62 pts)

Issue: Access appears to all websites appears to be unrestricted. This issue does not imply that any particular user is currently accessing restricted sites, but rather that they can. Controlling access to the Internet and websites may help reduce risks related to security, legal, and productivity concerns. Lack of adequate content management filtering to block restricted sites may lead to increased network risk and business liability.
Recommendation: We propose putting in place access controls to block websites that violate the company's Internet use policy.

System Protocol Leakage (45 pts)

Issue: System protocols were allowed to be sent outbound. To prevent potential loss of data and reduce the risk of malicious behavior by malware, these protocols should be restricted or blocked by external access controls. There are very few instances where system protocols are needed outside of the internal network. Allowing these protocols to \"leak\" does not mean that they are currently posing a threat, but is an indication of a lack of a managed firewall or proper policies to block these protocols.
Recommendation: We suggest ensuring adequate access controls in place to block these protocols or note them as acceptable risks.

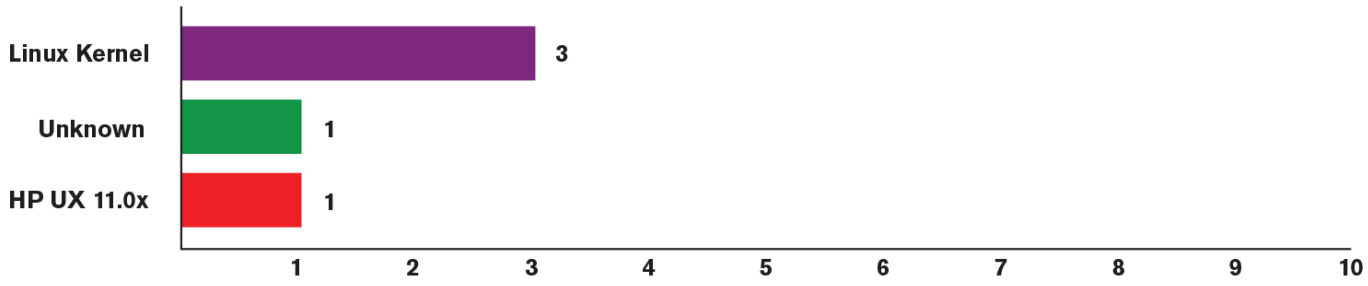
EXTERNAL VULNERABILITIES

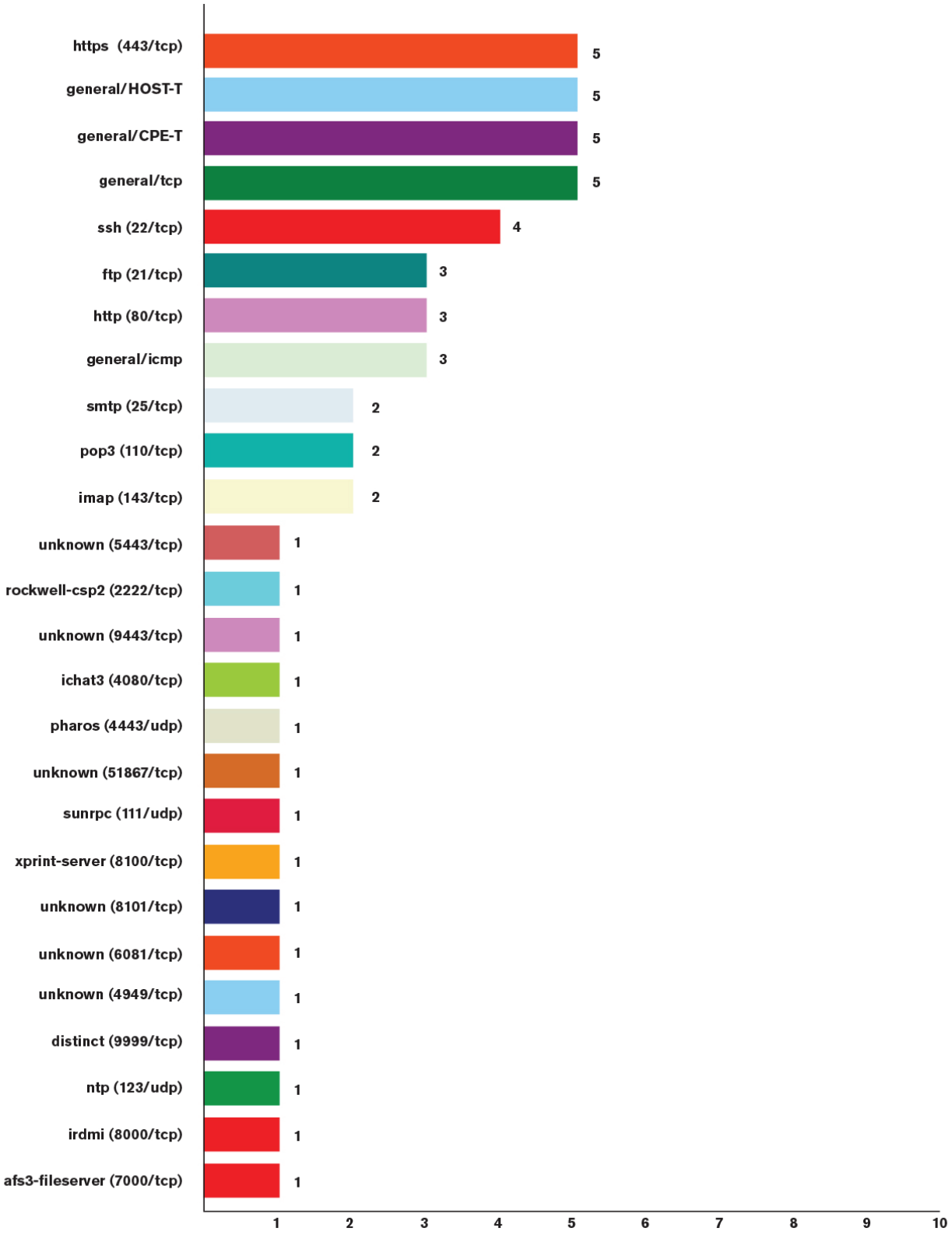


Host Issue Summary

Host	Analysis	Open Ports	High	Med	Low	False	CVSS
42.62.65.25	Medium risk	14	0	1	3	0	2.6
176.28.51.58 (rs208305.rs.hosteurope.de)	High risk	7	1	2	2	0	14.4
46.38.236.232 (fbnhffmnn.de)	Medium risk	13	0	2	4	0	8.8
63.230.176.46 (etsio-prod.cnf.com)	Medium risk	11	0	3	3	0	13.1
193.23.123.40 (rev-040.snrm.fr)	High risk	9	2	4	0	0	27.0
Total: 5	High risk	54	3	12	12	0	65.9

Detected Operating System




https (443/tcp) 5
general/HOST-T 5
general/CPE-T 5
general/tcp 5
ssh (22/tcp) 4
ftp (21/tcp) 3
http (80/tcp) 3
general/icmp 3
smtp (25/tcp) 2
pop3 (110/tcp) 2
imap (143/tcp) 2
unknown (5443/tcp) 1
rockwell-csp2 (2222/tcp) 1
unknown (9443/tcp) 1
ichat3 (4080/tcp) 1
pharos (4443/udp) 1
unknown (51867/tcp) 1
sunrpc (111/udp) 1
xprint-server (8100/tcp) 1
unknown (8101/tcp) 1
unknown (6081/tcp) 1
unknown (4949/tcp) 1
distinct (9999/tcp) 1
ntp (123/udp) 1
irdmi (8000/tcp) 1
afs3-fileserver (7000/tcp) 1
1 2 3 4 5 6 7 8 9 10

INTERNAL VULNERABILITIES

LOCAL SECURITY POLICY CONSISTENCY