GoodSecurity Penetration Test Report

[Philippe.Henry@GoodSecurity.com](mailto:Philippe.Henry@GoodSecurity.com)

April 15, 2022

# High-Level Summary

-GoodSecurity was tasked with performing an internal penetration test on GoodCorp’s CEO, Hans Gruber. An internal penetration test is a dedicated attack against internally connected systems. The focus of this test is to perform attacks, similar to those of a hacker and attempt to infiltrate Hans’ computer and determine if it is at risk. GoodSecurity’s overall objective was to exploit any vulnerable software and find the secret recipe file on Hans’ computer, while reporting the findings back to GoodCorp.

-When performing the internal penetration test, there were several alarming vulnerabilities that were

identified on Hans’ desktop. When performing the attacks, GoodSecurity was able to gain access to his machine and find the secret recipe file by exploit two programs that had major vulnerabilities. The details of the attack can be found in the ‘Findings’ category.

# Findings

**Machine IP:** 192.168.0.20

**Hostname:** MSEDGEWIN10

**Vulnerability Exploited:** buffer overflow and can be exploited via this module:

windows/http/icecast\_header

**Vulnerability Explanation:**

Explain the vulnerability as best you can by explaining the attack type (i.e. is it a heap overflow attack, buffer overflow, file inclusion, etc.?) and briefly summarize what that attack is (Might need Google’s help!)

**From my own words:**

This web streaming media server as some codes vulnerabilities which allow an attacker to gain access to the system via an admin remote shell exploit, directory traversal which allow to do any kind of changes on the target.

\* buffer overflow in url authentication with a base score of 8.1, HIGH: <https://nvd.nist.gov/vuln/detail/CVE-2018-18820>

\* DoS Exec Code Overflow with a score of 7.5 rated by <https://www.cvedetails.com/vulnerability-list/vendor_id-693/Icecast.html>

\*A step by step pdf guide is available at: <https://www.giac.org/paper/gcih/687/remote-exploitation-icecast-201-server/106910>

**From the Metasploit documentation:**

This module exploits a buffer overflow in the header parsing of icecast versions 2.0.1 and earlier, discovered by Luigi Auriemma.

Sending 32 HTTP headers will cause a write one past the end of a pointer array. On win32 this happens to overwrite the saved instruction pointer, and on linux (depending on compiler, etc) this seems to generally overwrite nothing crucial (read not exploitable).

This exploit uses ExitThread(), this will leave icecast thinking the thread is still in use, and the thread counter won't be decremented.

This means for each time your payload exits, the counter will be left incremented, and eventually the threadpool limit will be maxed so you can multihit, but only till you fill the threadpool.

**References**:

<https://cvedetails.com/cve/CVE-2004-1561/>

<http://www.securityfocus.com/bid/11271>

<http://archives.neohapsis.com/archives/bugtraq/2004-09/0366.html>

**Severity:**

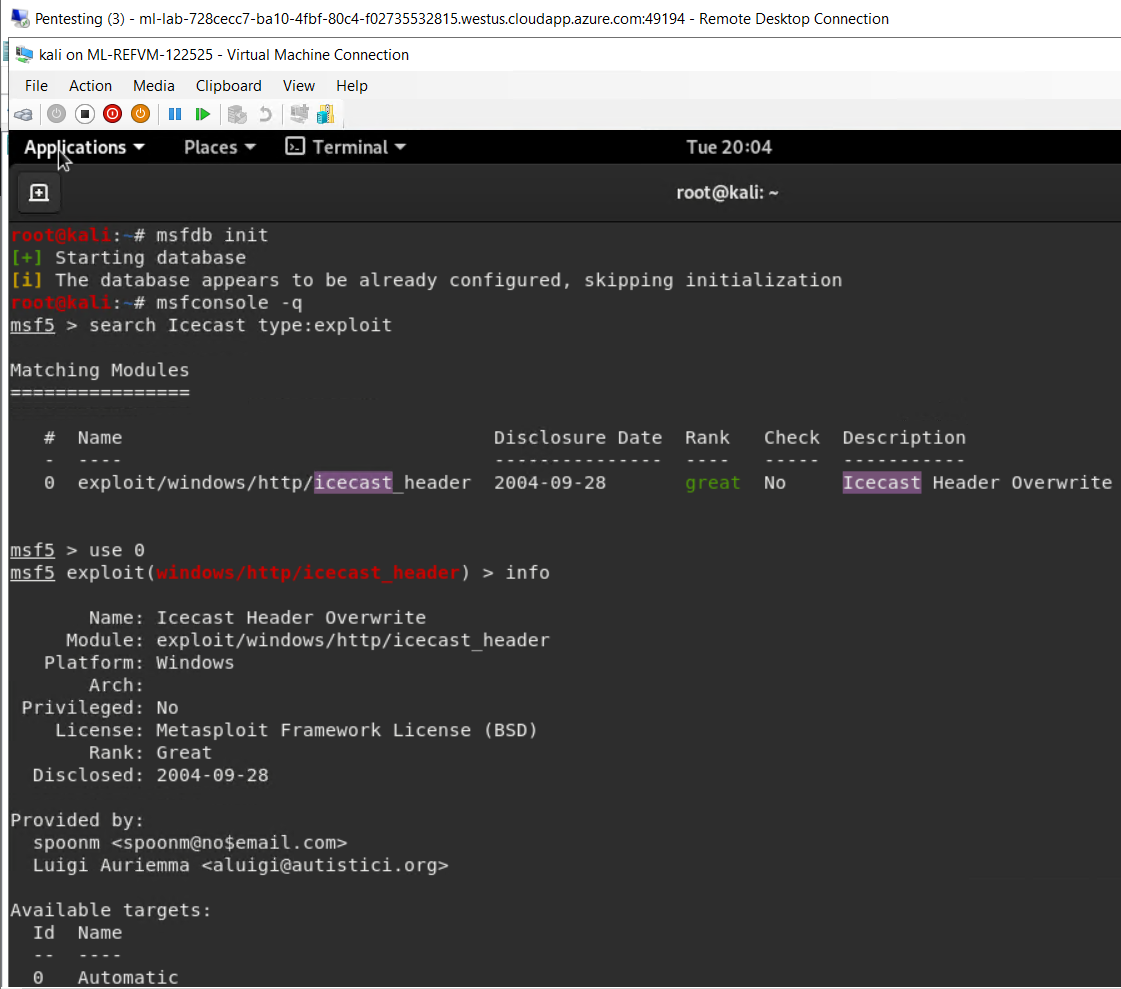
In your expert opinion, how severe is this vulnerability?

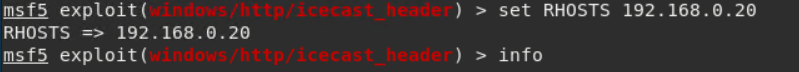
-This Remote Code Execution vulnerability is Critical, must be patch as soon as possible as the exploit is publicly available and can be exploited via Metasploit. The CVSS score is rated 7.5.

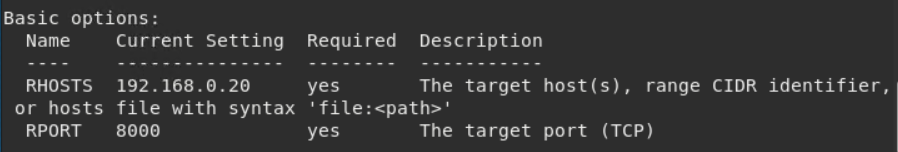
**Proof of Concept:**

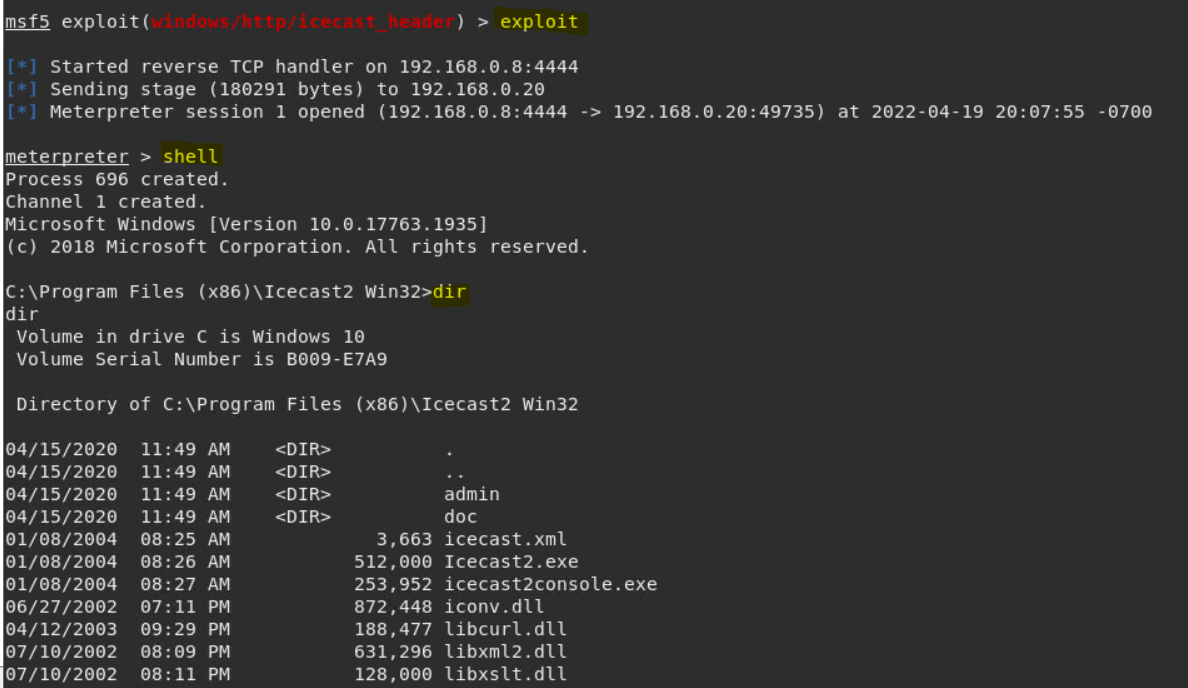
This is where you show the steps you took. Show the client how you exploited the software services. Please include screenshots!

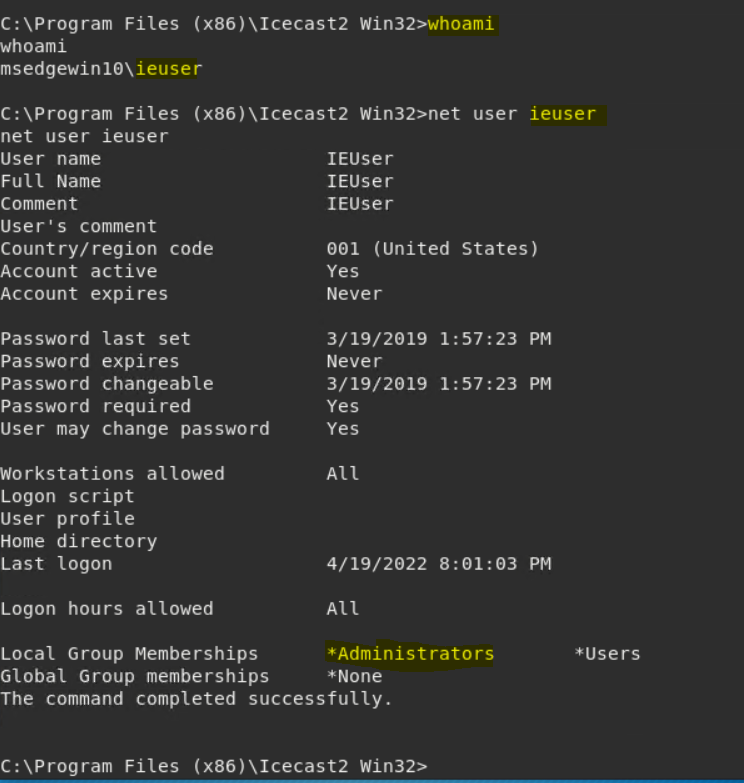
See below how easy with Metasploit to run a remote shell on the impacted server:



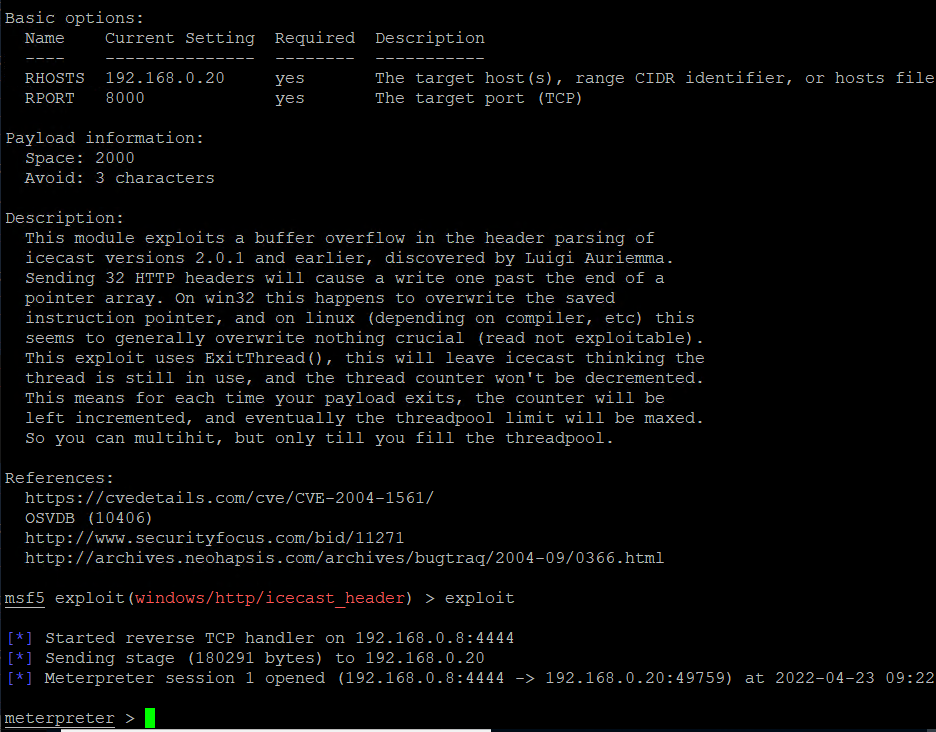


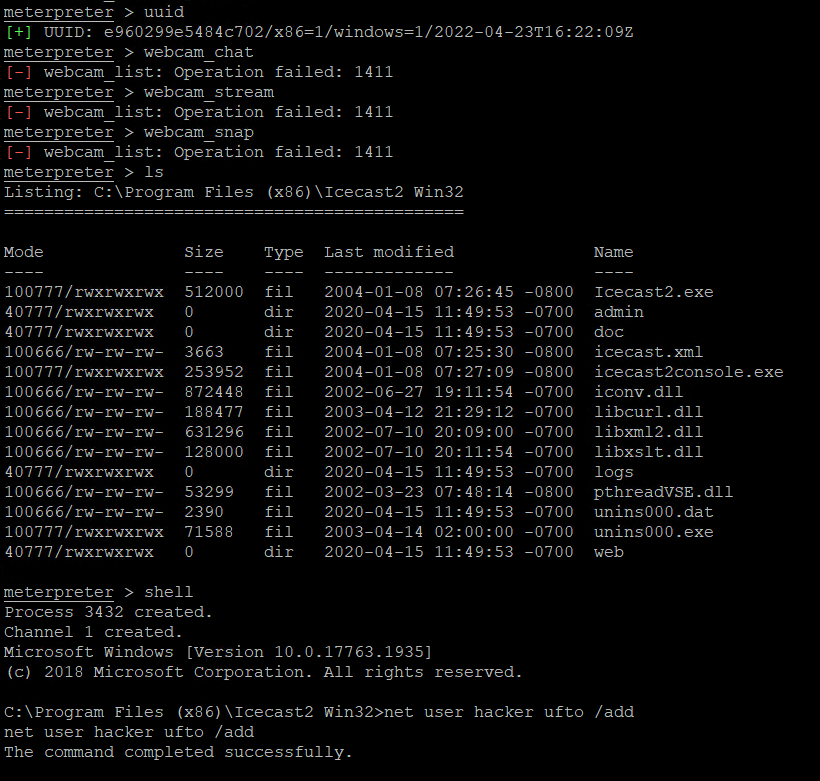






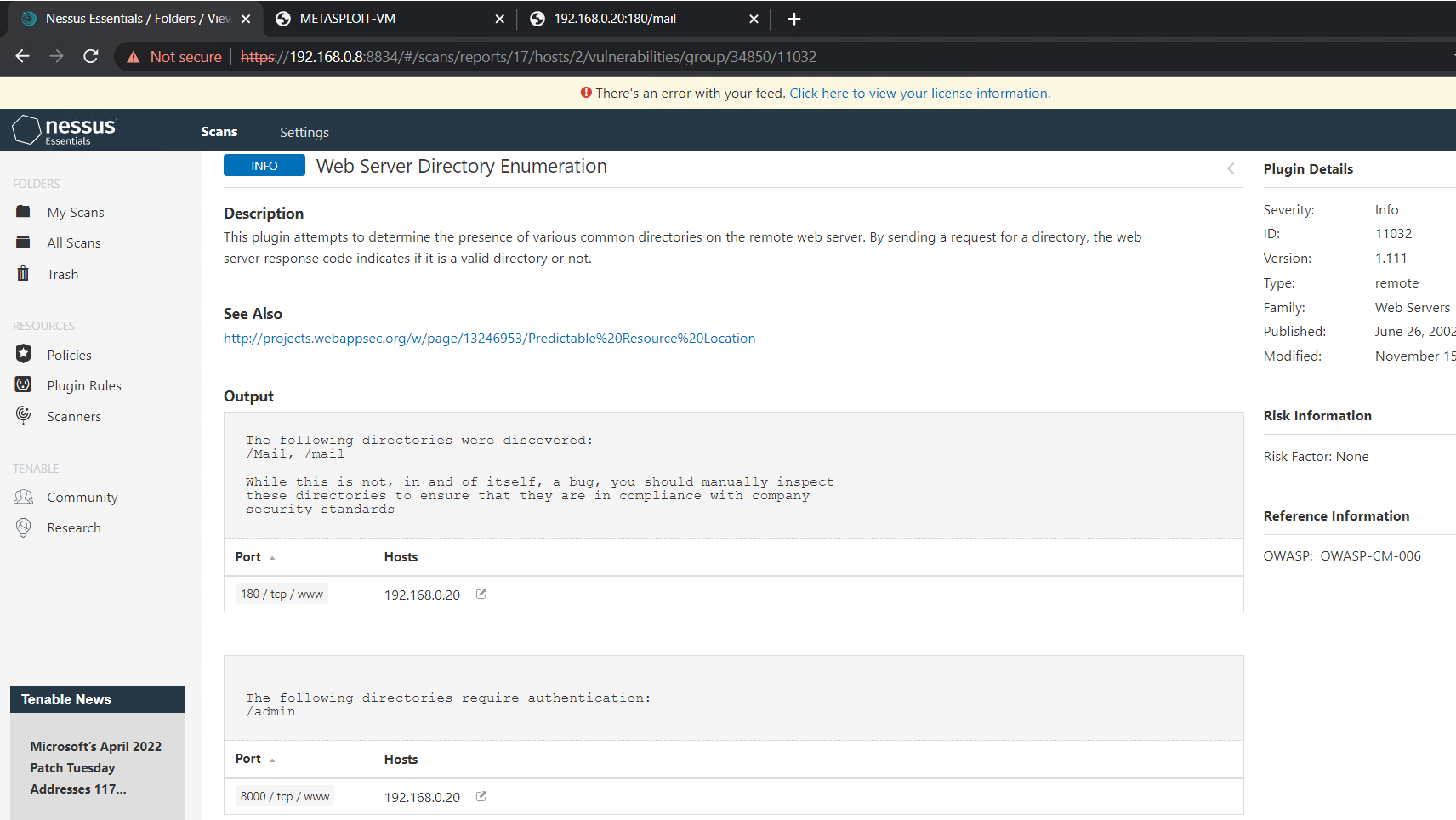
**\*Remote shell access therefore any kind of damages is possible:**

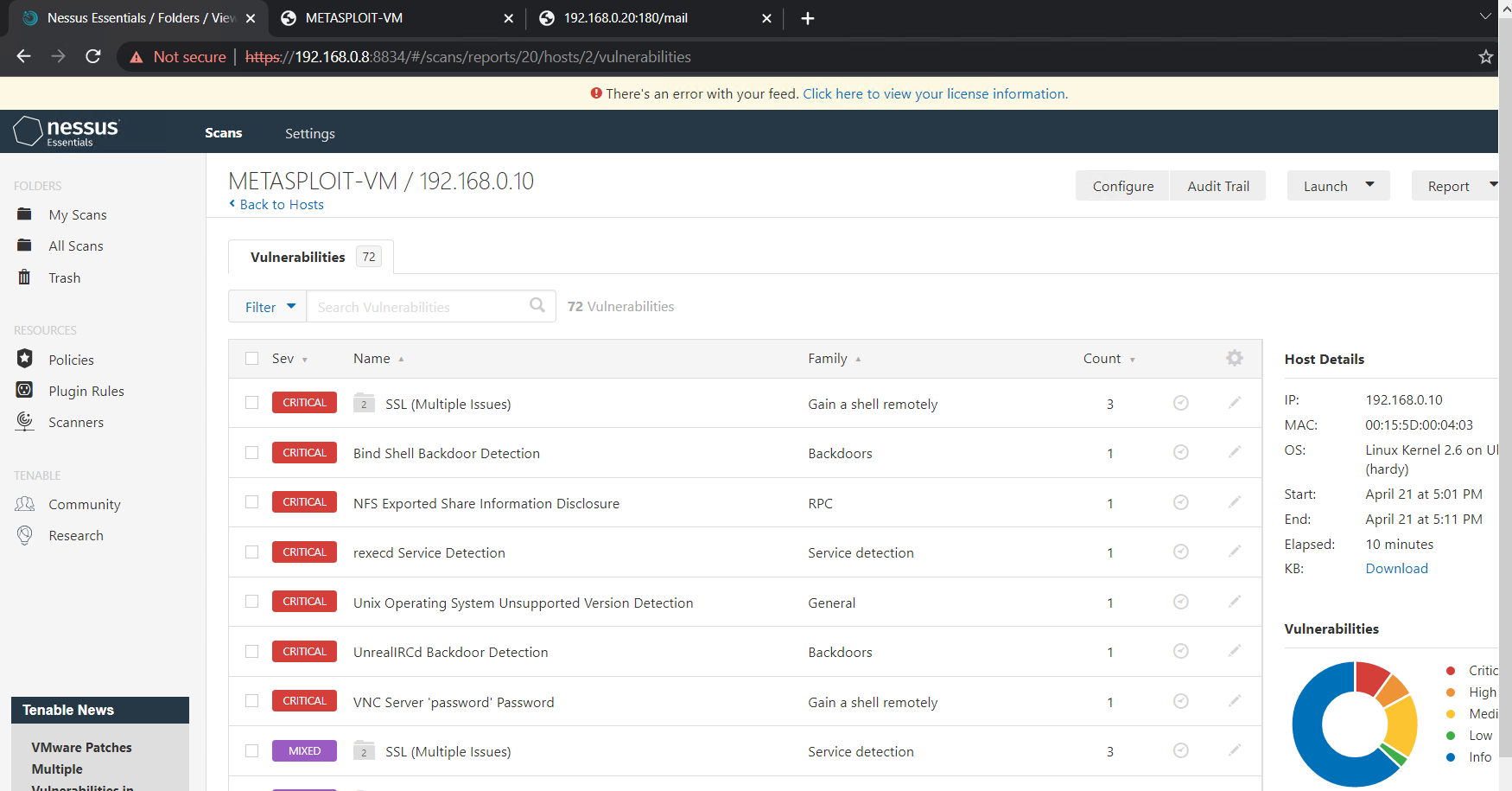


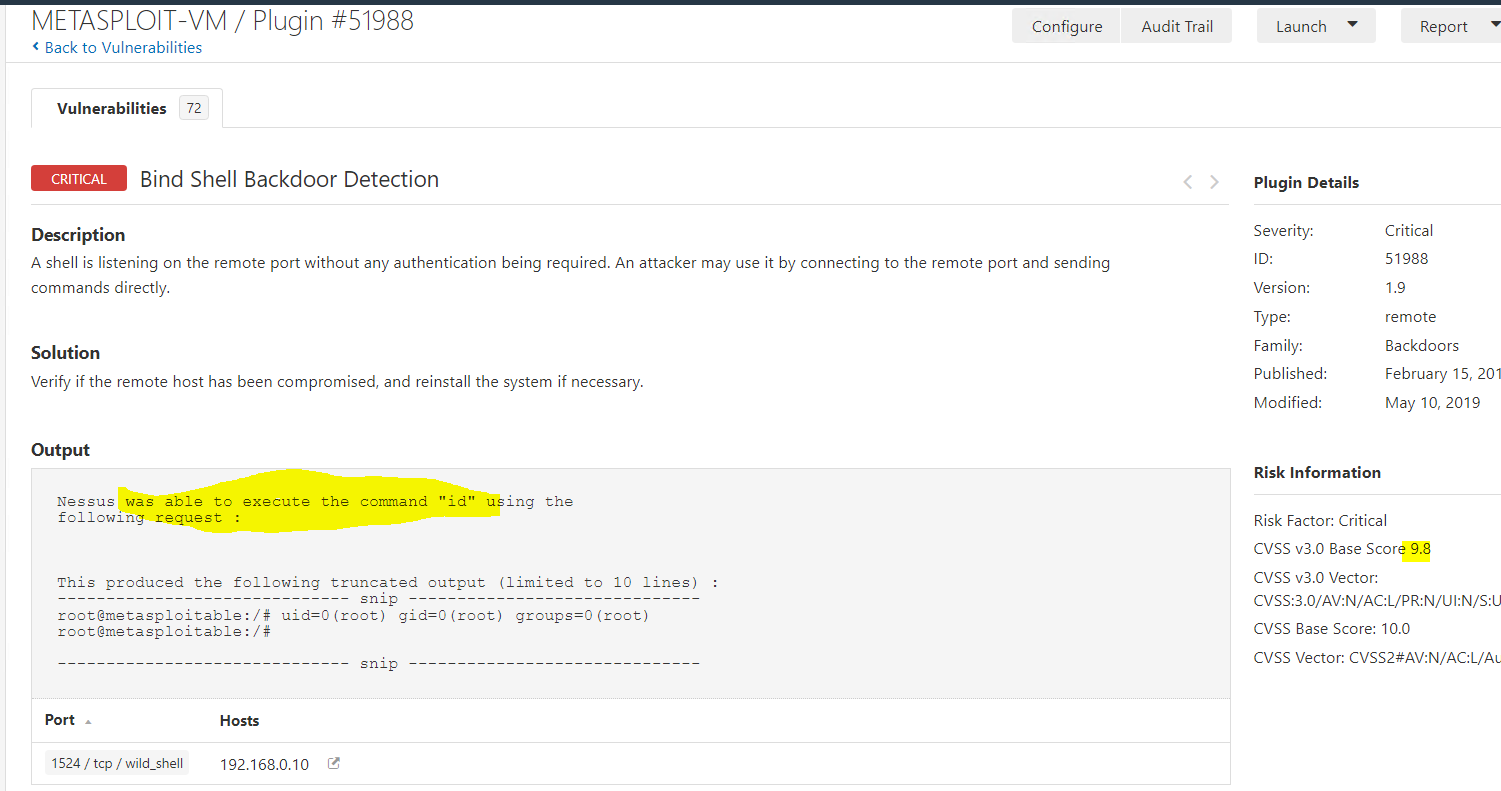


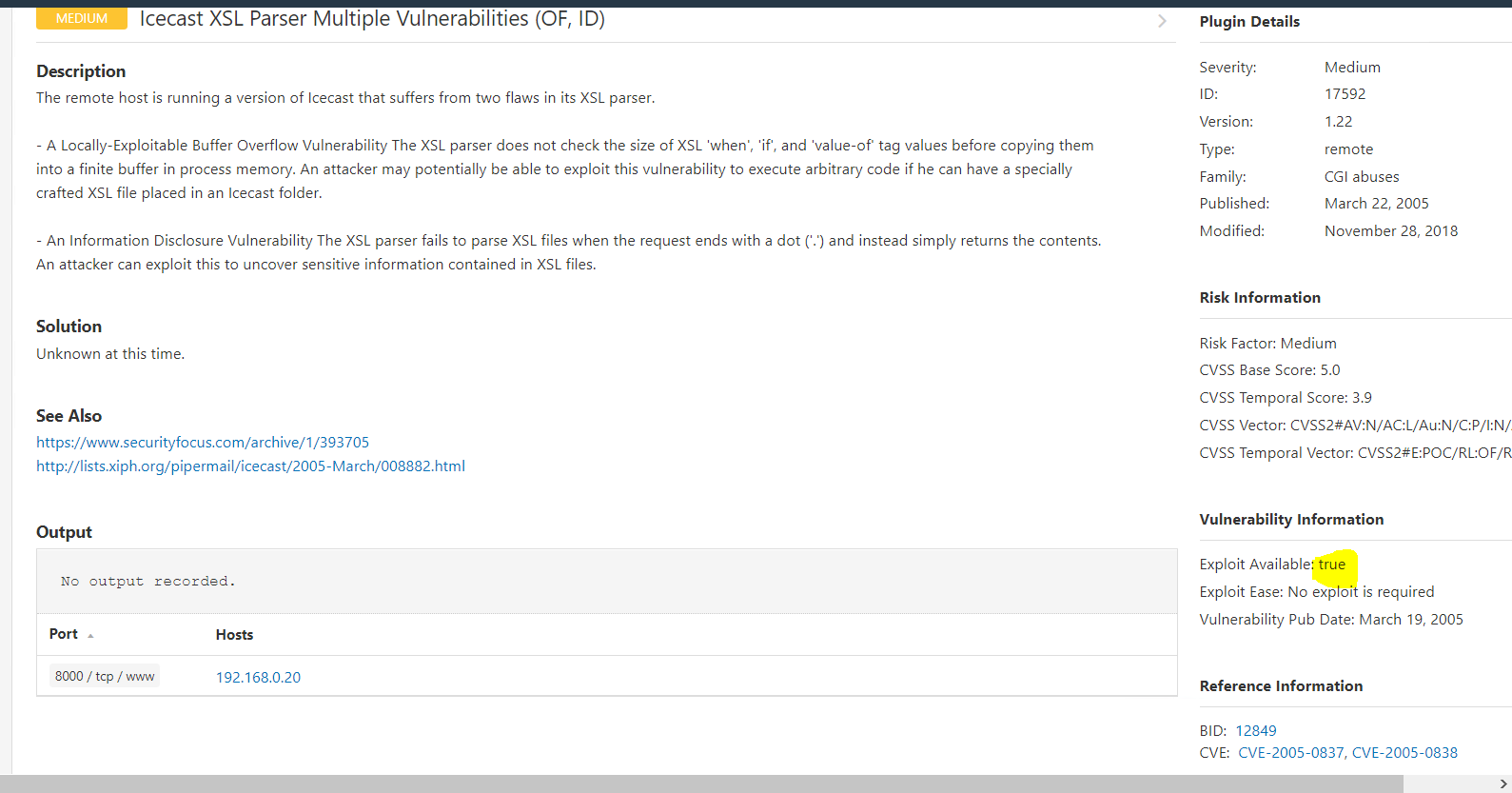
**There should be a separate finding for each vulnerability found!**

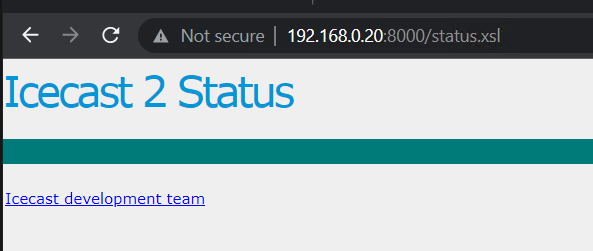
**\*Nessus Vulnerability Scanner:**



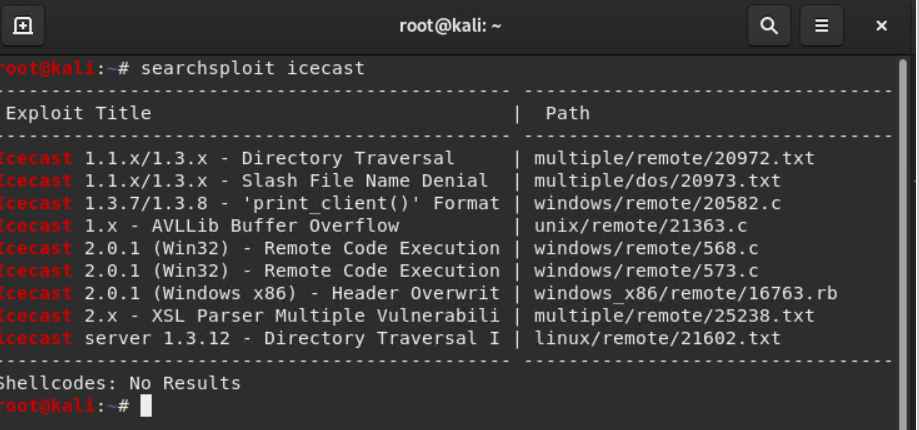








**\*Searchsploit, exploit scanner:**





# Recommendations

What recommendations would you give to GoodCorp?

-First include this server to the weekly patching group and the server IceCast2: 192.168.0.20 should be patched with the latest Icecast Current Release (2.4.4) via: <https://icecast.org/download/>

-Install a HIPS Host Intrusion Prevention System on Target to prevent malicious activities on the server like the installation of Meterpreter on the target. (HPIS windows solution example: <https://support.eset.com/en/enable-host-based-intrusion-prevention-system-hips-in-eset-windows-home-products> )

-Install XDR agent on Target in order to block any kind of abnormal activities and get report on it so we can take action. (XDR windows solution example: <https://www.trendmicro.com/en_ca/business/products/detection-response/xdr.html> )

-Install a IPS on the network / subnets where the Target resides to alert and block unusual activities.

(IPS solutions example: <https://suricata.readthedocs.io/en/latest/what-is-suricata.html> )

-Install a SOAR solution in order for the SOC analysts to track events, be alert and make recommendations to allow and disallow traffic. (SOAR solutions example: <https://www.splunk.com/en_us/software/splunk-security-orchestration-and-automation.html> )