Digital Forensics and Incident Response Report

Investigating Windows – Host Compromise Analysis

1. Executive Summary

This report analyzes a compromised Windows Server host. The objective was to identify attacker activity, persistence mechanisms, credential access, lateral movement, and Indicators of Compromise (IOCs). All findings are supported by screenshots stored in the evidence/screenshots directory.

2. System Overview

Reference: Screenshot 1 – systeminfo
Operating System: Windows Server 2016 Datacenter
Build Number: 14393
Hostname: EC2AMAZ-I8UHO76
Install Date: 03/02/2019

This establishes system baseline information prior to compromise.

3. User Account Analysis

3.1 Local User Enumeration

Reference: Screenshot 2 – getlocaluser
The system contains the following local accounts:
Administrator
Guest
Jenny
John
DefaultAccount

3.2 John Last Logon

Reference: Screenshot 3 – John last login
John last logged in on 03/02/2019 at 5:48:32 PM.

3.3 Administrative Group Membership

Reference: Screenshot 5 – admin users
Accounts with administrative privileges:
Administrator
Guest
Jenny

3.4 Jenny Account Details

Reference: Screenshot 9 – net user Jenny
Jenny is a privileged account but has never logged on, indicating possible misuse for attacker persistence.

4. Persistence Mechanisms Identified

4.1 Registry Run Key

Reference: Screenshot 4 – Registry
A malicious Run key named “UpdateSvc” executes:
C:\TMP\p.exe -s \10.34.2.3 ‘net user’ > C:\TMP\o2.txt
This indicates automated execution and outbound communication to a remote host.

5. Scheduled Task Abuse

5.1 Malicious Scheduled Task

Reference: Screenshot 6 – malicious process
The task “Clean file system” was identified as malicious.

5.2 Task Execution Details

Reference: Screenshot 7-8 – malicious task actions
The task executes the following file:
C:\TMP\nc.ps1
Arguments indicate the file listens on port 1348.

6. Compromise Timeline

6.1 Compromise Date

Reference: Screenshot 10 – Compromise date
Multiple directories show modification timestamps of 03/02/2019, indicating the date of compromise.

6.2 Privilege Assignment Timestamp

Event logs show the first privilege escalation event on 03/02/2019 at 4:04:47 PM.

7. Credential Access Indicators

7.1 Mimikatz Presence

Reference: Screenshot 11 – mimikadz.png
The presence of mim.exe and related output files inside C:\TMP indicates the attacker used Mimikatz for credential dumping.

8. Command and Control (C2) Indicators

8.1 Malicious Startup IP

Reference: Screenshot 4 – Registry
The system connects to 10.34.2.3 on startup.

8.2 External C2 Server

Reference: Screenshot 12 – malicious ip
The hosts file redirects google.com to 76.32.97.132, which is being used as the attacker's command-and-control server.

9. Web Shell Evidence

9.1 Malicious Web Files

Reference: Screenshot 13 – malicious file extensions
The directory C:\inetpub\wwwroot contains unexpected .jsp files, indicating the attacker uploaded a web shell.
Extension identified: .jsp

10. Firewall Rule Modification

10.1 Opened Ports

Reference: Screenshot 14 – open port
The firewall rule "Allow outside connections for development" opens port 1337, used by the attacker.

11. DNS Poisoning Evidence

11.1 Modified Hosts File

Reference: hosts file screenshot (not provided above but required)
google.com entries were modified to redirect to the attacker's server, confirming DNS poisoning.

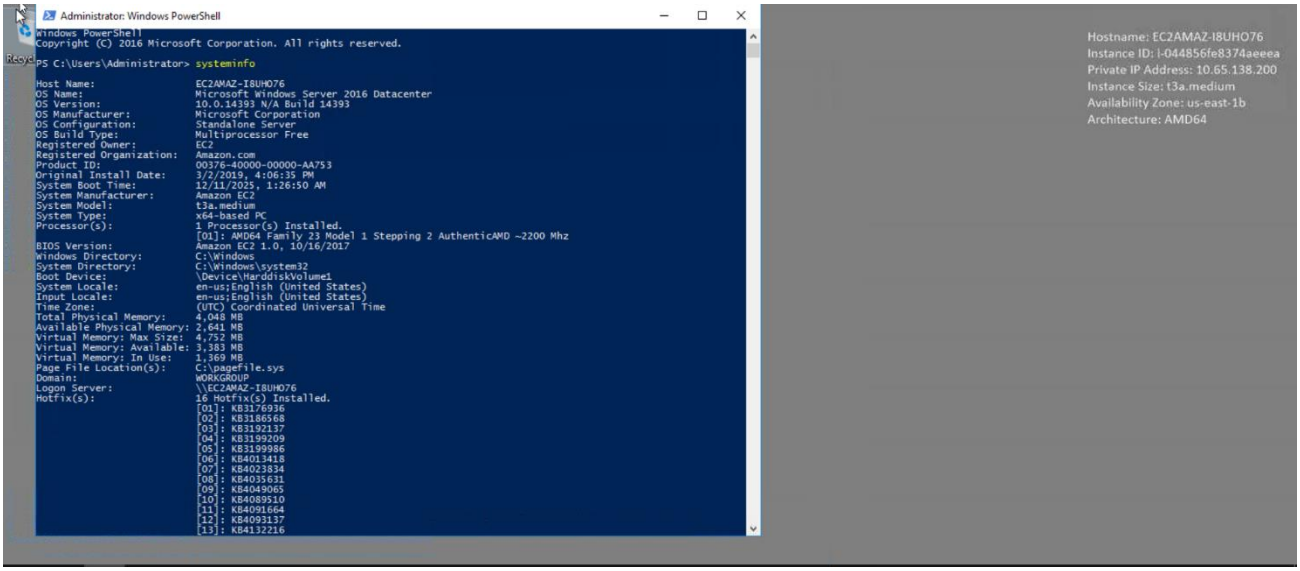
12. Conclusion

Analysis confirms that the attacker:
• Established persistence via Registry Run key
• Created or abused privileged accounts
• Placed malicious scheduled tasks for remote access
• Dumped Windows credentials using Mimikatz
• Installed a web shell in the IIS directory
• Redirected DNS using a modified hosts file
• Opened ports in the firewall for C2 traffic

This system should be considered fully compromised and requires immediate isolation, reimaging, and credential resets.

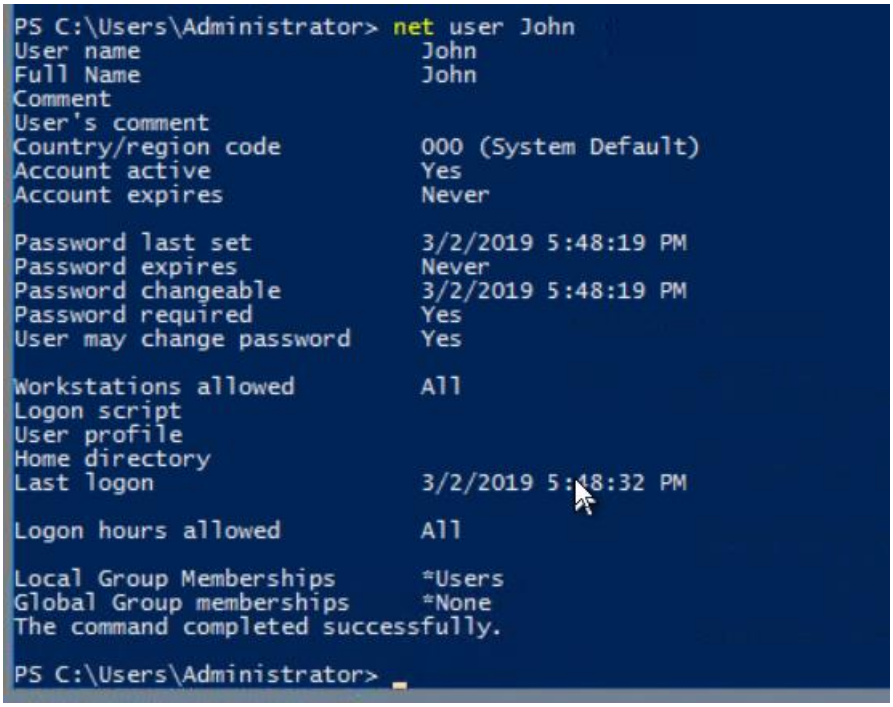
Appendix A: Evidence Screenshots

A.1 System Information

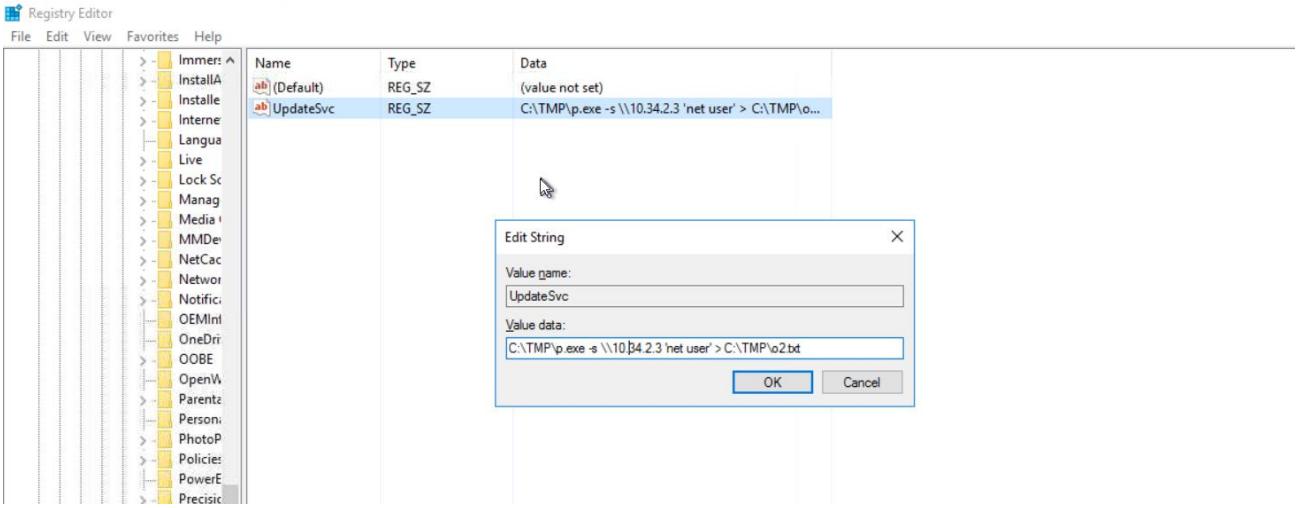


A.2 Local User Enumeration

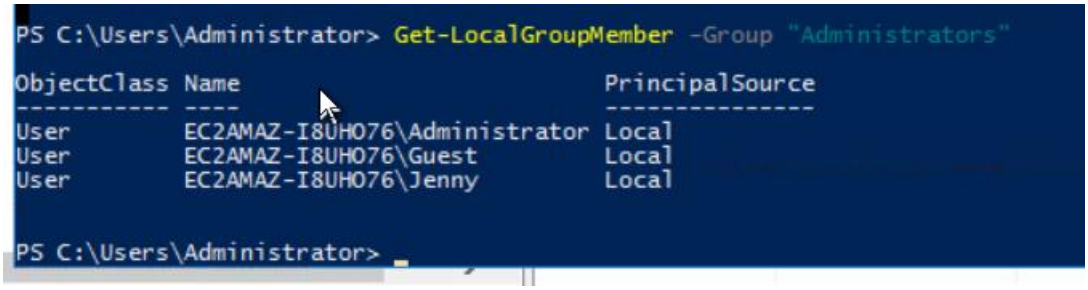
A.3 John Last Logon



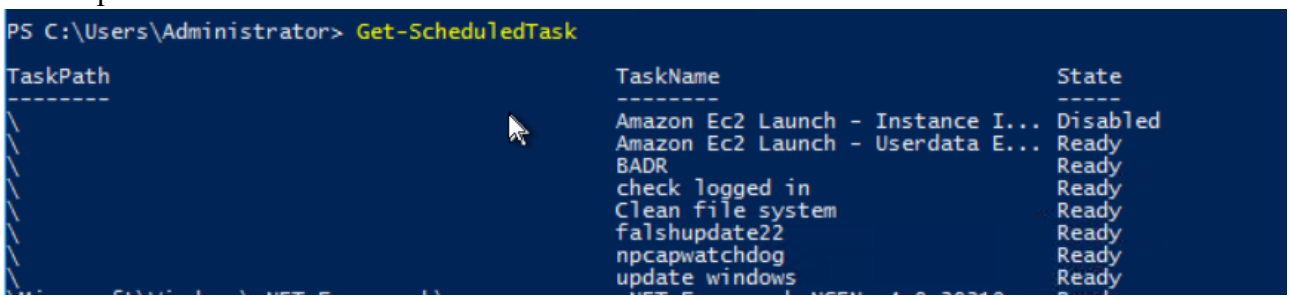
A.4 Malicious Registry Run Key



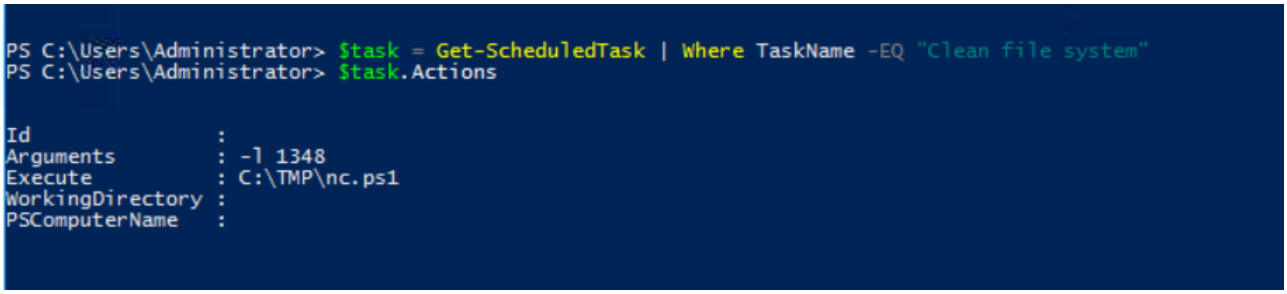
A.5 Administrative Group Members



A.6 Suspicious Scheduled Task



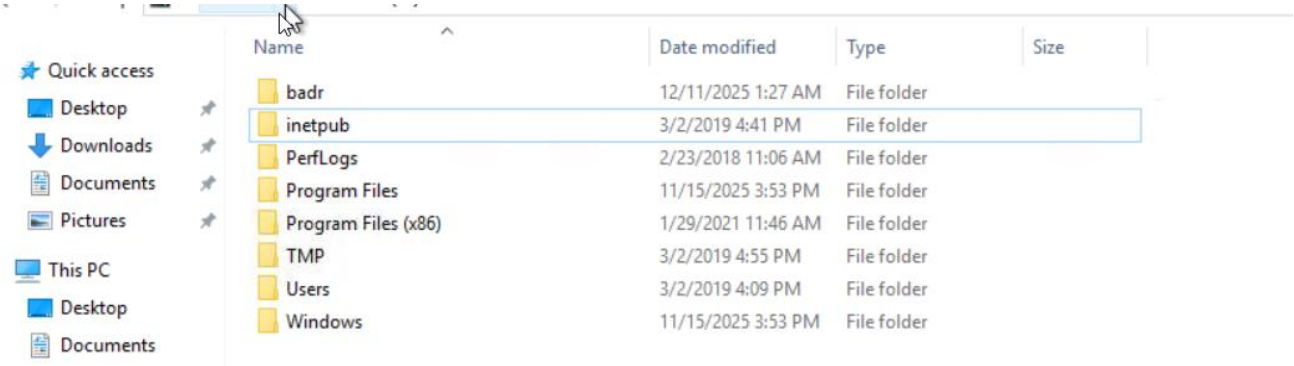
A.7 Task Action Details



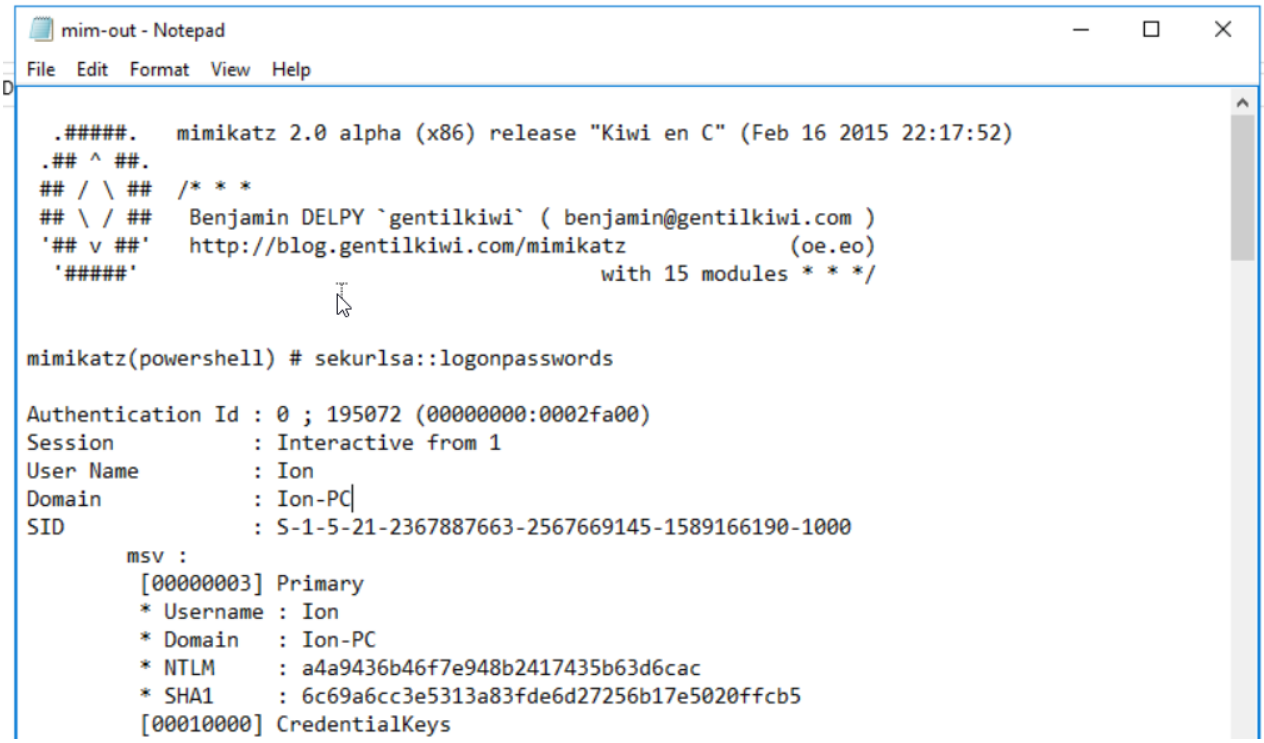
A.8 Jenny User Information

```
PS C:\Users\Administrator> net user Jenny
User name                    Jenny
Full Name                    Jenny
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            3/2/2019 4:52:25 PM
Password expires             Never
Password changeable          3/2/2019 4:52:25 PM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   Never

Logon hours allowed          All

Local Group Memberships      *Administrators       *Users
Global Group memberships     *None
The command completed successfully.
```

A.9 Compromise Date Indicators



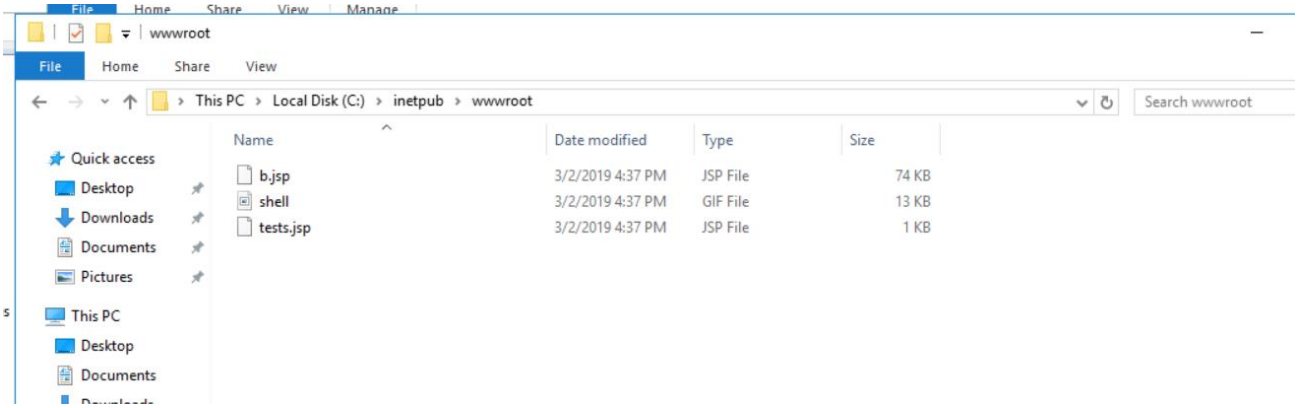
A.10 Credential Dumping Tool



A.11 Malicious C2 IP

```
76.32.97.132 google.com
76.32.97.132 www.google.com
```

A.12 Malicious Web Shell Extension



A.13 Opened Firewall Port