

T1562.004 - Disable or Modify System Firewall

Description from ATT&CK

Adversaries may disable or modify system firewalls in order to bypass controls limiting network usage. Changes could be disabling the entire mechanism as well as adding, deleting, or modifying particular rules. This can be done numerous ways depending on the operating system, including via command-line, editing Windows Registry keys, and Windows Control Panel.

Modifying or disabling a system firewall may enable adversary C2 communications, lateral movement, and/or data exfiltration that would otherwise not be allowed.

Atomic Tests

- Atomic Test #1 Disable Microsoft Defender Firewall
- Atomic Test #2 Disable Microsoft Defender Firewall via Registry
- Atomic Test #3 Allow SMB and RDP on Microsoft Defender Firewall
- Atomic Test #4 Opening ports for proxy HARDRAIN
- Atomic Test #5 Open a local port through Windows Firewall to any profile
- Atomic Test #6 Allow Executable Through Firewall Located in Non-Standard Location
- Atomic Test #7 Stop/Start UFW firewall
- Atomic Test #8 Stop/Start UFW firewall systemctl
- Atomic Test #9 Turn off UFW logging
- Atomic Test #10 Add and delete UFW firewall rules
- Atomic Test #11 Edit UFW firewall user.rules file
- Atomic Test #12 Edit UFW firewall ufw.conf file

Preview Code Blame 665 lines (354 loc) · 14.2 KB

Raw ☐ <u></u> :=

↑ Top

• Atomic Test #15 - Tail the UFW firewall log file

7 torrie lest # 15 lan the of W in ewan log in

☐ Files

☐ Files

☐ Go to file

☐ June 1 June 2 Ju

Atomic Test #1 - Disable Microsoft Defender Firewall

Indexes T1003.001 T1003.002 T1003.003 T1003.004 T1003.005 T1003.006 T1003.007 T1003.008 T1003 T1006 T1007 T1010 T1012 T1014 T1016 T1018 T1020 T1021.001 T1021.002 T1021.003 T1021.006 T1027.001 T1027.002 T1027.004 T1027 T1030 T1033 T1036.003 T1036.004 T1036.005 T1036.006 T1036 > T1037.001 T1037.002 T1037.004 T1037.005

T1039

T1040

Disables the Microsoft Defender Firewall for the current profile. Caution if you access remotely the host where the test runs! Especially with the cleanup command which will reenable firewall for the current profile...

Supported Platforms: Windows

auto_generated_guid: 88d05800-a5e4-407e-9b53-ece4174f197f

Attack Commands: Run with command_prompt!

```
netsh advfirewall set currentprofile state off □
```

Cleanup Commands:

```
netsh advfirewall set currentprofile state on >nul 2>&1
```

Atomic Test #2 - Disable Microsoft Defender Firewall via Registry

Disables the Microsoft Defender Firewall for the public profile via registry Caution if you access remotely the host where the test runs! Especially with the cleanup command which will re-enable firewall for the current profile...

Supported Platforms: Windows

auto_generated_guid: afedc8c4-038c-4d82-b3e5-623a95f8a612

Attack Commands: Run with command_prompt!

```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAcce
```

Cleanup Commands:

```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAcce ☐
```

Atomic Test #3 - Allow SMB and RDP on Microsoft Defender Firewall

Allow all SMB and RDP rules on the Microsoft Defender Firewall for all profiles. Caution if you access remotely the host where the test runs! Especially with the cleanup command which will reset the firewall and risk disabling those services...

Supported Platforms: Windows

auto_generated_guid: d9841bf8-f161-4c73-81e9-fd773a5ff8c1

Attack Commands: Run with command_prompt!

```
netsh advfirewall firewall set rule group="remote desktop" new enable=Ye netsh advfirewall firewall set rule group="file and printer sharing" new
```

Cleanup Commands:

```
netsh advfirewall reset >nul 2>&1
```

Atomic Test #4 - Opening ports for proxy - HARDRAIN

This test creates a listening interface on a victim device. This tactic was used by HARDRAIN for proxying.

reference: https://www.us-cert.gov/sites/default/files/publications/MAR-10135536-F.pdf

Supported Platforms: Windows

auto_generated_guid: 15e57006-79dd-46df-9bf9-31bc24fb5a80

Attack Commands: Run with command_prompt! Elevation Required (e.g. root or admin)

<code>netsh</code> advfirewall firewall add rule <code>name="atomic testing"</code> action=allow d \Box



Cleanup Commands:

<code>netsh</code> advfirewall firewall delete rule name="atomic testing" protocol=TC \Box

Atomic Test #5 - Open a local port through Windows Firewall to any profile

This test will attempt to open a local port defined by input arguments to any profile

Supported Platforms: Windows

auto_generated_guid: 9636dd6e-7599-40d2-8eee-ac16434f35ed

Inputs:

| Name | Description | Туре | Default Value |
|------------|---|---------|---------------|
| local_port | This is the local port you wish to test opening | Integer | 3389 |

Attack Commands: Run with powershell! Elevation Required (e.g. root or admin)

netsh advfirewall firewall add rule name="Open Port to Any" dir=in proto \Box



Cleanup Commands:

netsh advfirewall firewall delete rule name="Open Port to Any" | Out-Nul

Atomic Test #6 - Allow Executable Through Firewall **Located in Non-Standard Location**

This test will attempt to allow an executable through the system firewall located in the Users directory

Supported Platforms: Windows

auto_generated_guid: 6f5822d2-d38d-4f48-9bfc-916607ff6b8c

Inputs:

| Name | Description | Туре | Default Value |
|---------------|---------------------|------|--|
| exe_file_path | path to exe file | Path | PathToAtomicsFolder\T1562.004\bin\AtomicTest |

Attack Commands: Run with powershell! Elevation Required (e.g. root or admin)

```
Copy-Item #{exe_file_path} -Destination "C:\Users\$env:UserName" -Force netsh advfirewall firewall add rule name="Atomic Test" dir=in action=all
```

Cleanup Commands:

```
netsh advfirewall firewall delete rule name="Atomic Test" | Out-Null Remove-Item C:\Users\$env:UserName\AtomicTest.exe -ErrorAction Ignore
```

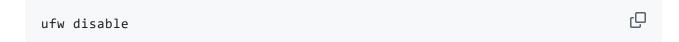
Atomic Test #7 - Stop/Start UFW firewall

Stop the Uncomplicated Firewall (UFW) if installed.

Supported Platforms: Linux

auto_generated_guid: fe135572-edcd-49a2-afe6-1d39521c5a9a

Attack Commands: Run with sh! Elevation Required (e.g. root or admin)



Cleanup Commands:

```
ufw enable
ufw status verbose
```

Dependencies: Run with sh!

Description: Check if ufw is installed on the machine.

Check Prereq Commands:

```
if [ ! -x "$(command -v ufw)" ]; then echo -e "\n**** ufw NOT installed
if echo "$(ufw status)" |grep -q "inactive"; then echo -e "\n**** ufw i
```

Get Prereq Commands:

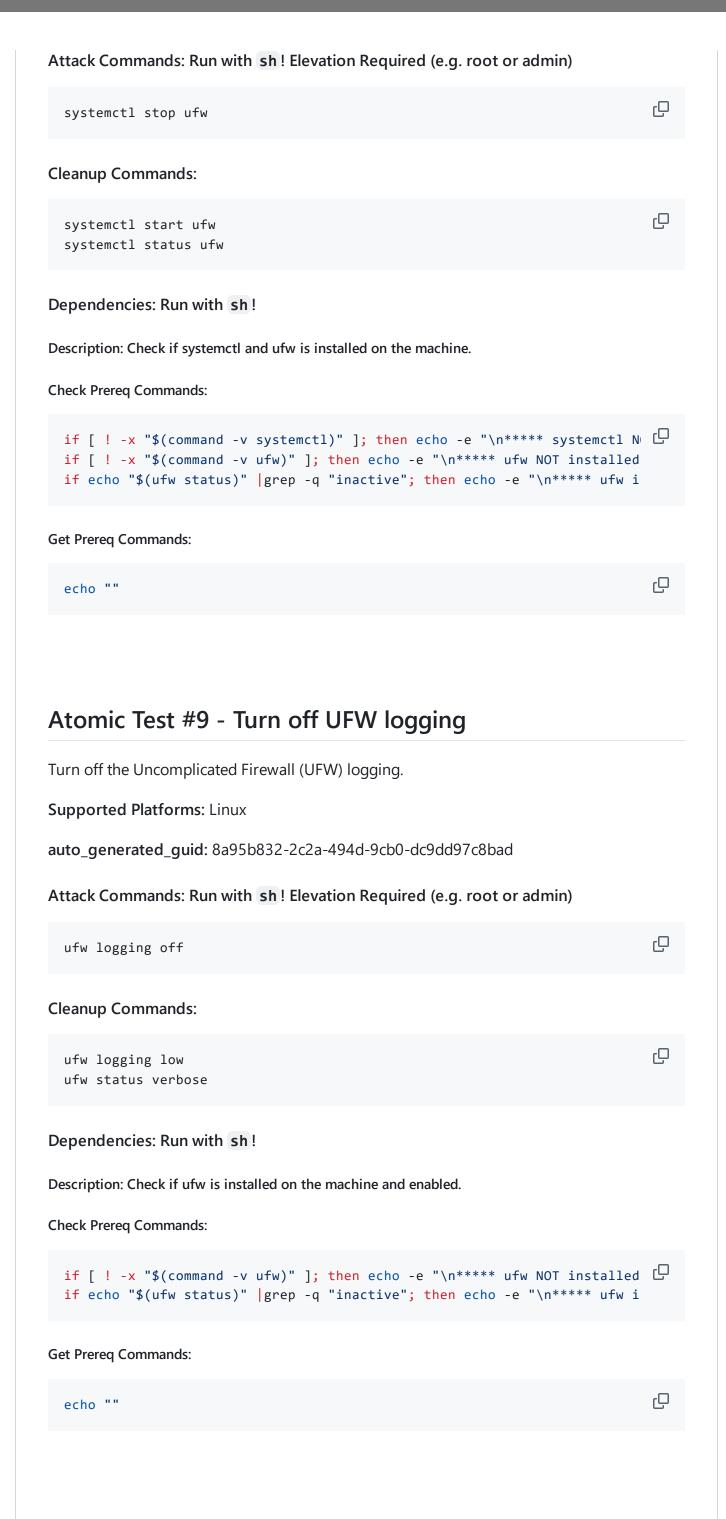
```
echo ""
```

Atomic Test #8 - Stop/Start UFW firewall systemctl

Stop the Uncomplicated Firewall (UFW) if installed, using systemctl.

Supported Platforms: Linux

auto_generated_guid: 9fd99609-1854-4f3c-b47b-97d9a5972bd1



Atomic Test #10 - Add and delete UFW firewall rules

Add and delete a rule on the Uncomplicated Firewall (UFW) if installed and enabled.

Supported Platforms: Linux

auto_generated_guid: b2563a4e-c4b8-429c-8d47-d5bcb227ba7a

Attack Commands: Run with sh! Elevation Required (e.g. root or admin)

```
ufw prepend deny from 1.2.3.4
ufw status numbered
```

Cleanup Commands:

```
{ echo y; echo response; } | ufw delete 1 ufw status numbered
```

Dependencies: Run with sh!

Description: Check if ufw is installed on the machine and enabled.

Check Prereq Commands:

Get Prereq Commands:

```
echo ""
```

Atomic Test #11 - Edit UFW firewall user.rules file

Edit the Uncomplicated Firewall (UFW) rules file /etc/ufw/user.rules.

Supported Platforms: Linux

auto_generated_guid: beaf815a-c883-4194-97e9-fdbbb2bbdd7c

Attack Commands: Run with sh! Elevation Required (e.g. root or admin)

```
echo "# THIS IS A COMMENT" >> /etc/ufw/user.rules
grep "# THIS IS A COMMENT" /etc/ufw/user.rules
```

Cleanup Commands:

```
sed -i 's/# THIS IS A COMMENT//g' /etc/ufw/user.rules
```

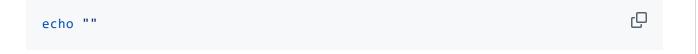
Dependencies: Run with sh!

Description: Check if /etc/ufw/user.rules exists.

Check Prereq Commands:

```
if [ ! -f "/etc/ufw/user.rules" ]; then echo -e "\n**** ufw NOT install [
```

Get Prereq Commands:



Atomic Test #12 - Edit UFW firewall ufw.conf file

Edit the Uncomplicated Firewall (UFW) configuration file /etc/ufw/ufw.conf which controls if the firewall starts on boot and its logging level.

Supported Platforms: Linux

auto_generated_guid: c1d8c4eb-88da-4927-ae97-c7c25893803b

Attack Commands: Run with sh! Elevation Required (e.g. root or admin)

```
echo "# THIS IS A COMMENT" >> /etc/ufw/ufw.conf
grep "# THIS IS A COMMENT" /etc/ufw/ufw.conf
```

Cleanup Commands:

```
sed -i 's/# THIS IS A COMMENT//g' /etc/ufw/ufw.conf cat /etc/ufw/ufw.conf
```

Dependencies: Run with sh!

Description: Check if /etc/ufw/ufw.conf exists.

Check Prereq Commands:

```
if [ ! -f "/etc/ufw/ufw.conf" ]; then echo -e "\n**** ufw NOT installed
```

Get Prereq Commands:

```
echo ""
```

Atomic Test #13 - Edit UFW firewall sysctl.conf file

Edit the Uncomplicated Firewall (UFW) configuration file for setting network variables /etc/ufw/sysctl.conf.

Supported Platforms: Linux

auto_generated_guid: c4ae0701-88d3-4cd8-8bce-4801ed9f97e4

Attack Commands: Run with sh! Elevation Required (e.g. root or admin)

```
echo "# THIS IS A COMMENT" >> /etc/ufw/sysctl.conf
grep "# THIS IS A COMMENT" /etc/ufw/sysctl.conf
```

Cleanup Commands:

```
sed -i 's/# THIS IS A COMMENT//g' /etc/ufw/sysctl.conf
cat /etc/ufw/sysctl.conf
```

Dependencies: Run with sh!

Description: Check if /etc/ufw/sysctl.conf exists.

Check Prereq Commands:

if [!-f"/etc/ufw/sysctl.conf"]; then echo -e "\n***** ufw NOT instal C

Get Prereq Commands:

echo ""

Atomic Test #14 - Edit UFW firewall main configuration file

Edit the Uncomplicated Firewall (UFW) main configuration file for setting default policies /etc/default/ufw.

Supported Platforms: Linux

auto_generated_guid: 7b697ece-8270-46b5-bbc7-6b9e27081831

Attack Commands: Run with sh! Elevation Required (e.g. root or admin)

```
echo "# THIS IS A COMMENT" >> /etc/default/ufw
grep "# THIS IS A COMMENT" /etc/default/ufw
```

Cleanup Commands:

```
sed -i 's/# THIS IS A COMMENT//g' /etc/default/ufw
```

Dependencies: Run with sh!

Description: Check if /etc/default/ufw exists.

Check Prereq Commands:

```
if [ ! -f "/etc/default/ufw" ]; then echo -e "\n**** ufw NOT installed
```

Get Prereq Commands:

```
echo ""
```

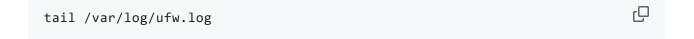
Atomic Test #15 - Tail the UFW firewall log file

Print the last 10 lines of the Uncomplicated Firewall (UFW) log file /var/log/ufw.log.

Supported Platforms: Linux

auto_generated_guid: 419cca0c-fa52-4572-b0d7-bc7c6f388a27

Attack Commands: Run with sh! Elevation Required (e.g. root or admin)



Cleanup Commands:

