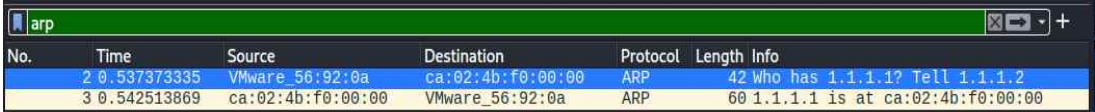
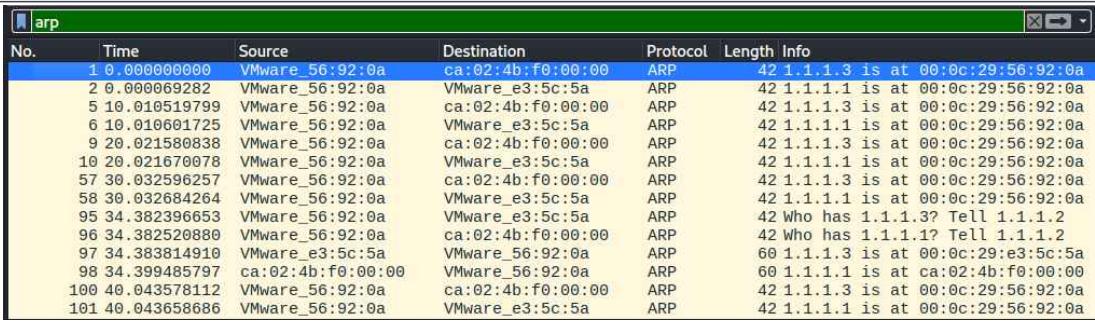
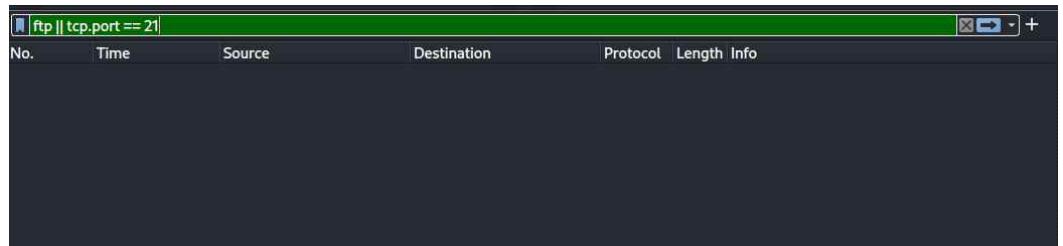
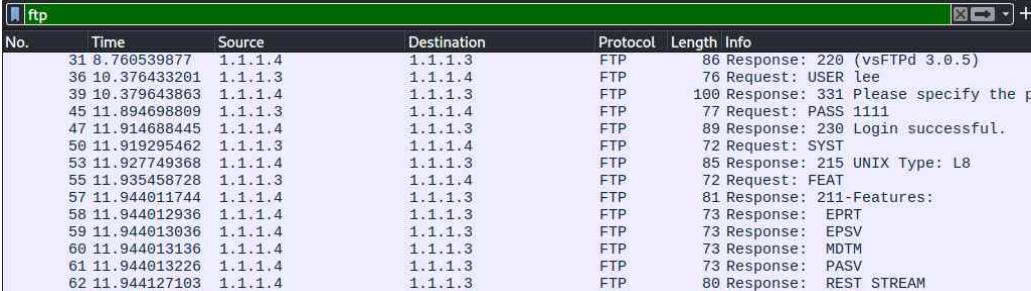
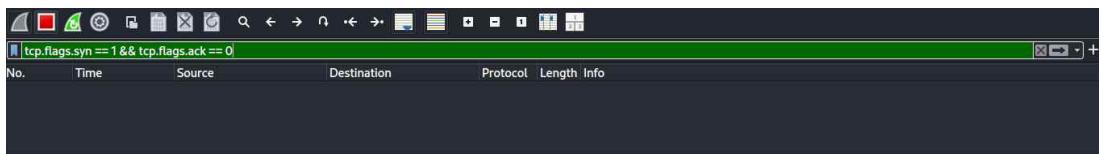


[시나리오 1] 패킷 식별 계획 - 내부망 침투 및 시스템 파괴

타겟 식별 및 초기 침투			
공격 시나리오	공격 기법	wireshark 필터	정상/비정상 식별 기준
네트워크 스캔 및 OS 분석	arp spoofing	arp	동일 IP에 MAC 주소 지속 변조
정상 패킷			
			
비정상 패킷			
			
공격 시나리오	공격 기법	필터	정상/비정상 식별 기준
네트워크 스캔 및 OS 분석	FTP 패킷 스니핑	ftp tcp.port == 21	Payload 내 계정 정보 노출 여부
정상 패킷			
			
비정상 패킷			
			

공격 시나리오	공격 기법	필터	정상/비정상 식별 기준
네트워크 스캔 및 OS 분석	nmap 스캔	tcp.flags.syn == 1	단시간 내 다수 포트 접속 시도

정상 패킷



비정상 패킷

No.	Time	Source	Destination	Protocol	Length	Info
2747	142.594667179	1.1.1.2	1.1.1.3	TCP	74	56494 - 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=40897
2751	142.599148586	1.1.1.2	1.1.1.3	TCP	74	56496 - 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=40897
2754	142.599655786	1.1.1.2	1.1.1.3	TCP	74	52194 - 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=40897
2766	142.651802699	1.1.1.2	1.1.1.3	TCP	74	52210 - 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=40897
2799	142.756193568	1.1.1.2	1.1.1.3	TCP	74	56502 - 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=40897
2805	142.759719370	1.1.1.2	1.1.1.3	TCP	74	47974 - 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=40897
2812	142.811683643	1.1.1.2	1.1.1.3	TCP	74	52212 - 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=40897
2824	142.864925430	1.1.1.2	1.1.1.3	TCP	74	52226 - 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=40897
2839	142.916252852	1.1.1.2	1.1.1.3	TCP	74	56508 - 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=40897
2866	142.921798689	1.1.1.2	1.1.1.3	TCP	74	52236 - 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=40897
2864	142.922939488	1.1.1.2	1.1.1.3	TCP	74	47978 - 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=40897
2870	143.073845764	1.1.1.2	1.1.1.3	TCP	74	56522 - 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=40897
2876	143.076919837	1.1.1.2	1.1.1.3	TCP	74	52240 - 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=40897
2906	143.234709155	1.1.1.2	1.1.1.3	TCP	74	56526 - 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=40897
2913	143.286676678	1.1.1.2	1.1.1.3	TCP	74	52244 - 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=40897
2935	143.394626452	1.1.1.2	1.1.1.3	TCP	74	47986 - 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=40897
2944	143.497884109	1.1.1.2	1.1.1.3	TCP	74	52254 - 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=40897
2961	143.652596219	1.1.1.2	1.1.1.3	TCP	74	47994 - 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=40897
2968	143.765375844	1.1.1.2	1.1.1.3	TCP	74	52264 - 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=40897
2987	143.913732729	1.1.1.2	1.1.1.3	TCP	74	48000 - 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=40897

공격 시나리오	공격 기법	필터	정상/비정상 식별 기준
SSH 크래킹 (hydra)	SSH Force	Brute	tcp.port == 22

정상 패킷

No.	Time	Source	Destination	Protocol	Length	Info
90	142.854961749	1.1.1.3	1.1.1.2	SSHv2	118	Server: Encrypted packet (len=44)
91	142.856289773	1.1.1.2	1.1.1.3	SSHv2	126	Client: Encrypted packet (len=60)
92	142.856694547	1.1.1.3	1.1.1.2	SSHv2	339	Server: Encrypted packet (len=264)
93	142.905949169	1.1.1.2	1.1.1.3	TCP	66	45344 - 22 [ACK] Seq=3922 Ack=3998 Win=76288 Len=0 TSval=409344726 TSe...
94	143.222691248	1.1.1.2	1.1.1.3	SSHv2	158	Client: Encrypted packet (len=84)
95	143.2340600418	1.1.1.3	1.1.1.2	SSHv2	94	Server: Encrypted packet (len=28)
96	143.2340955956	1.1.1.2	1.1.1.3	TCP	66	45344 - 22 [ACK] Seq=3106 Ack=3126 Win=76288 Len=0 TSval=409347054 TSe...
97	143.243694285	1.1.1.2	1.1.1.3	SSHv2	178	Client: Encrypted packet (len=112)
98	143.285591174	1.1.1.3	1.1.1.2	TCP	66	22 - 45344 [ACK] Seq=3126 Ack=3218 Win=71040 Len=0 TSval=4050564854 Ts...
99	143.3109219812	1.1.1.3	1.1.1.2	SSHv2	694	Server: Encrypted packet (len=628)
100	143.3151711399	1.1.1.2	1.1.1.3	TCP	66	45344 - 22 [ACK] Seq=3218 Ack=3154 Win=79360 Len=0 TSval=409347977 TSe...
101	143.3158096736	1.1.1.3	1.1.1.2	SSHv2	118	Server: Encrypted packet (len=44)
102	143.3158058916	1.1.1.2	1.1.1.3	TCP	66	45344 - 22 [ACK] Seq=3218 Ack=3198 Win=79360 Len=0 TSval=409347978 TSe...
103	143.3158255801	1.1.1.2	1.1.1.3	SSHv2	594	Client: Encrypted packet (len=528)
104	143.3158766211	1.1.1.3	1.1.1.2	TCP	66	22 - 45344 [ACK] Seq=3198 Ack=3179 Win=73856 Len=0 TSval=3050565727 TS...
105	143.3162456398	1.1.1.3	1.1.1.2	SSHv2	174	Server: Encrypted packet (len=108)
106	143.3162456398	1.1.1.3	1.1.1.2	SSHv2	1126	Server: Encrypted packet (len=668)
107	143.3163672391	1.1.1.2	1.1.1.3	TCP	66	45344 - 22 [ACK] Seq=3746 Ack=4966 Win=82432 Len=0 TSval=409347984 TSe...
109	143.3124562477	1.1.1.3	1.1.1.2	SSHv2	198	Server: Encrypted packet (len=132)
110	143.32989186155	1.1.1.2	1.1.1.3	TCP	66	45344 - 22 [ACK] Seq=3746 Ack=5098 Win=84992 Len=0 TSval=409348109 TSe...

비정상 패킷

No.	Time	Source	Destination	Protocol	Length	Info
277	142.850535588	1.1.1.2	1.1.1.3	TCP	66	46938 - 22 [FIN, ACK] Seq=1244 Ack=1826 Win=69120 Len=0 TSval=40966579...
278	142.852397951	1.1.1.3	1.1.1.2	TCP	66	22 - 40838 [ACK] Seq=1245 Ack=1245 Win=64256 Len=0 TSval=305083593 TSe...
279	142.857455888	1.1.1.3	1.1.1.2	TCP	66	22 - 40838 [FIN, ACK] Seq=1246 Ack=1245 Win=64256 Len=0 TSval=30508848...
280	142.867569669	1.1.1.2	1.1.1.3	TCP	66	46938 - 22 [ACK] Seq=1245 Ack=1827 Win=69120 Len=0 TSval=40966322 TSe...
281	143.807318973	1.1.1.3	1.1.1.2	SSHv2	118	Server: Encrypted packet (len=52)
282	143.812145936	1.1.1.2	1.1.1.3	TCP	66	49796 - 22 [FIN, ACK] Seq=1252 Ack=1850 Win=69120 Len=0 TSval=409667448...
283	143.815263776	1.1.1.3	1.1.1.2	TCP	66	22 - 40796 [ACK] Seq=1253 Win=64256 Len=0 TSval=30508852...
284	143.815309951	1.1.1.2	1.1.1.3	TCP	66	469796 - 22 [ACK] Seq=1253 Ack=1851 Win=69120 Len=0 TSval=409667490 TSe...
285	143.8340576719	1.1.1.3	1.1.1.2	SSHv2	118	Server: Encrypted packet (len=52)
286	143.837529583	1.1.1.2	1.1.1.3	TCP	66	469812 - 22 [FIN, ACK] Seq=1244 Ack=1850 Win=69120 Len=0 TSval=40966751...
287	143.841436372	1.1.1.3	1.1.1.2	TCP	66	22 - 40812 [FIN, ACK] Seq=1245 Ack=1245 Win=64256 Len=0 TSval=30508852...
288	143.8414846397	1.1.1.2	1.1.1.3	TCP	66	469812 - 22 [ACK] Seq=1245 Ack=1851 Win=69120 Len=0 TSval=409667516 TSe...
289	143.854269695	1.1.1.3	1.1.1.2	SSHv2	118	Server: Encrypted packet (len=52)
290	143.855103667	1.1.1.2	1.1.1.3	TCP	66	469816 - 22 [FIN, ACK] Seq=1245 Ack=1850 Win=69120 Len=0 TSval=40966753...
291	143.859510367	1.1.1.3	1.1.1.2	TCP	66	22 - 40848 [ACK] Seq=1245 Ack=1851 Win=64256 Len=0 TSval=30508852...
292	143.859558659	1.1.1.2	1.1.1.3	TCP	66	469848 - 22 [ACK] Seq=1245 Ack=1851 Win=64256 Len=0 TSval=409667534 TSe...
293	143.864629727	1.1.1.3	1.1.1.2	SSHv2	118	Server: Encrypted packet (len=52)
294	143.8653341617	1.1.1.2	1.1.1.3	TCP	66	469822 - 22 [FIN, ACK] Seq=1244 Ack=1850 Win=69120 Len=0 TSval=40966754...
295	143.872255537	1.1.1.3	1.1.1.2	TCP	66	22 - 40822 [FIN, ACK] Seq=1245 Ack=1245 Win=64256 Len=0 TSval=30508853...
296	143.872275652	1.1.1.2	1.1.1.3	TCP	66	469822 - 22 [ACK] Seq=1245 Ack=1851 Win=69120 Len=0 TSval=409667547 TSe...

내부망 확장 및 관리자 권한 획득			
공격 시나리오	공격 기법	wireshark 필터	정상/비정상 식별 기준
DNS 정보 탈취	AXFR	tcp.port == 53	헤더 내 스캐너 명시
정상 패킷			
비정상 패킷			
공격 시나리오	공격 기법	wireshark 필터	정상/비정상 식별 기준
DNS 정보 탈취	WhatWeb	http	DNS 서버 설정 상태
정상 패킷			
비정상 패킷			

공격 시나리오	공격 기법	wireshark 필터	정상/비정상 식별 기준
SQL Injection	SQL Injection	http.request.uri	요청 데이터 내 DB 예약어 포함

정상 패킷

http.request.uri						
No.	Time	Source	Destination	Protocol	Length	Info
21	7.122531269	1.1.1.2	1.1.1.4	HTTP	691	POST /DVWA/login.php HTTP/1.1 (application/x-www-form-urlencoded)
23	7.125755625	1.1.1.4	1.1.1.2	HTTP	521	HTTP/1.1 302 Found
25	7.133825527	1.1.1.2	1.1.1.4	HTTP	513	GET /DVWA/index.php HTTP/1.1
26	7.136705171	1.1.1.4	1.1.1.2	HTTP	2888	HTTP/1.1 200 OK (text/html)

비정상 패킷

http.request.uri						
No.	Time	Source	Destination	Protocol	Length	Info
25	1.735779920	1.1.1.2	1.1.1.4	HTTP	525	GET /vulnerabilities/sqli/ HTTP/1.1
27	1.737934371	1.1.1.4	1.1.1.2	HTTP	1855	HTTP/1.1 200 OK (text/html)
41	11.420784629	1.1.1.2	1.1.1.4	HTTP	577	GET /vulnerabilities/sqli/?id=1%27+or+%271%27%3D%271&Submit=Submit HTTP/1.1
43	11.423874180	1.1.1.4	1.1.1.2	HTTP	1935	HTTP/1.1 200 OK (text/html)

시나리오1 차단 정책

시나리오 1은 서버 단에서 iptables로 차단할 예정

[시나리오 2]

공격 시나리오	공격 기법	wireshark 필터	정상/비정상 식별 기준
정상 패킷			
비정상 패킷			
공격 시나리오	공격 기법	wireshark 필터	정상/비정상 식별 기준
정상 패킷			
비정상 패킷			