

12월 21일 보안 세미나

장경배

공공기관 프린터 관리 시스템

ARP Spoofing 공격법

ARP(Adresss Resolution Protocol) : IP주소를 물리적주소(MAC 주소)로 대응 시켜주는 프로토콜

ARP Spoofing : 공격대상에게 잘못된 Mac주소를 보내 테이블을 조작하여 정보를 빼내는 해킹 기법

```
C:\Users\starj>arp -a

인터페이스: 192.168.56.1 --- 0x8
  인터넷 주소      물리적 주소      유형      형식
  192.168.56.255    ff-ff-ff-ff-ff-ff    유정적     정적
  224.0.0.22        01-00-5e-00-00-16    유동적     정적
  224.0.0.251       01-00-5e-00-00-fb    유동적     정적
  224.0.0.252       01-00-5e-00-00-fc    유동적     정적
  239.255.255.250   01-00-5e-7f-ff-fa    유동적     정적
  255.255.255.255   ff-ff-ff-ff-ff-ff    유정적     정적

인터페이스: 172.21.2.132 --- 0x11
  인터넷 주소      물리적 주소      유형      형식
  172.21.0.2        00-90-0b-1b-fb-63    유동적     정적
  172.21.0.3        00-90-fb-31-43-8f    유동적     정적
  172.21.1.150      60-f6-77-d1-e4-67    유동적     정적
  172.21.2.102      bc-a8-a6-c8-a6-1d    유동적     정적
  172.21.255.255    ff-ff-ff-ff-ff-ff    유정적     정적
  224.0.0.22        01-00-5e-00-00-16    유동적     정적
  224.0.0.251       01-00-5e-00-00-fb    유동적     정적
  224.0.0.252       01-00-5e-00-00-fc    유동적     정적
  239.255.255.250   01-00-5e-7f-ff-fa    유동적     정적
  255.255.255.255   ff-ff-ff-ff-ff-ff    유정적     정적
```

ARP table

공격 시나리오



Victim PC 의 ARP table

```
인터페이스: 223.194.129.14 --- 0xa
  인터넷 주소      물리적 주소      유형
223.194.128.236    00-26-c7-a7-08-ae    동적
223.194.128.247    88-53-2e-31-d9-a9    동적
223.194.128.254    2c-fa-a2-aa-9c-65    동적
223.194.135.255    ff-ff-ff-ff-ff-ff    정적
224.0.0.22         01-00-5e-00-00-16    정적
224.0.0.251        01-00-5e-00-00-fb    정적
224.0.0.252        01-00-5e-00-00-fc    정적
239.255.255.250    01-00-5e-7f-ff-fa    정적
255.255.255.255    ff-ff-ff-ff-ff-ff    정적

C: \Windows\system32>
```

ARP Spoofing 공격을 당한 후

인터페이스: 223.194.129.14 --- 0xa

인터넷 주소

물리적 주소

223.194.128.236

00-26-c7-a7-08-ae

223.194.128.247

88-53-2e-31-d9-a9

223.194.128.254

f8-63-3f-3b-6f-e1

223.194.134.216

f8-63-3f-3b-6f-e1

223.194.135.255

ff-ff-ff-ff-ff-ff

224.0.0.22

01-00-5e-00-00-16

224.0.0.251

01-00-5e-00-00-fb

224.0.0.252

01-00-5e-00-00-fc

239.255.255.250

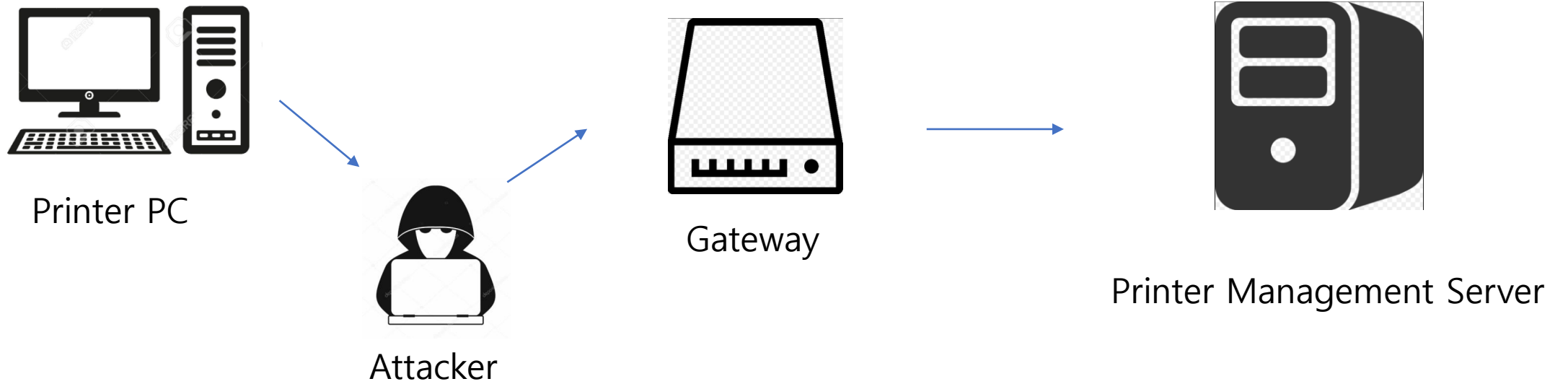
01-00-5e-7f-ff-fa

255.255.255.255

ff-ff-ff-ff-ff-ff

[illegible]

공격 성공 후 통신 모습



Spoofing 과정

Lain												
File View Configure Tools Help												
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query												
IP address	MAC address	OUI fingerprint	Host name	B...	B...	B8	Gr	M0	M1	M3		
223.194.128.8	F4D9FBE26D4B	Samsung Electronics CO., L...						*	*	*		
223.194.128.9	F4D9FBE26DAD	Samsung Electronics CO., L...						*	*	*		
223.194.128.17	00C2C6A4AE98	Intel Corporate		*	*	*	*	*	*	*		
223.194.128.23	6C8DC175A4...			*	*	*	*	*	*	*		
223.194.128.34	4C7C5F496F36											
223.194.128.40	E4FAED2DE013			*	*	*	*	*	*	*		
223.194.128.57	BC5451729A36			*	*	*	*	*	*	*		
223.194.128.65	3CF7A40236C1			*	*	*	*	*	*	*		
223.194.128.64	58404E6F57E1			*	*	*	*	*	*	*		
223.194.128.48	F8E61AB6F8E7			*	*	*	*	*	*	*		
223.194.128.82	D02820ADCA...			*		*						
223.194.128.62	948BC17755AC											
223.194.128.98	BC5451FC4660			*	*	*	*	*	*	*		
223.194.128.102	08AED6610EDB			*	*	*	*	*	*	*		
223.194.128.135	C4D98769695F	Intel Corporate		*	*	*	*	*	*	*		
223.194.128.121	C49880AF9582				*	*	*		*			
223.194.128.130	B0702D35739D			*	*	*	*	*	*	*		
223.194.128.148	A48431EC5CF0			*	*		*		*			
223.194.128.186	D02820A467B4			*	*	*	*	*	*	*		
223.194.128.125	507A55828FC5			*	*	*	*	*	*	*		
223.194.128.210	40D3AE02C6FC			*	*	*	*	*	*	*		
223.194.128.199	A0D795802307			*	*	*	*	*	*	*		
223.194.128.218	88365FB3C76E			*	*	*	*	*	*	*		
223.194.128.230	B8EE65FF2515			*	*	*	*	*	*	*		
223.194.128.195	08AED611271D			*	*	*	*	*	*	*		
223.194.128.231	E470B83DD263			*	*	*	*	*	*	*		
223.194.128.236	0026C7A708AE	Intel Corporate		*	*	*	*	*	*	*		
223.194.128.144	70700D7A5FE3					*						
223.194.128.233	702C1F267A95	Wisol		*	*	*	*	*	*	*		
223.194.128.247	88532E31D9A9	Intel Corporate		*	*	*	*	*	*	*		
223.194.128.254	2CFAA2AA9C...			*	*	*	*	*	*	*		
223.194.128.219	54996364E561			*	*	*	*	*	*	*		
223.194.129.14	6C299584A328	Intel Corporate		*	*	*	*	*	*	*		
223.194.129.11	9800C62CAFA4			*	*	*	*	*	*	*		
223.194.129.37	CC25EF9DE546			*	*	*	*	*	*	*		

네트워크 대역의

ip주소와

Mac 주소 검색

New ARP Poison Routing



WARNING !!!

APR enables you to hijack IP traffic between the selected host on the left list and all selected hosts on the right list in both directions. If a selected host has routing capabilities WAN traffic will be intercepted as well. Please note that since your machine has not the same performance of a router you could cause DoS if you set APR between your Default Gateway and all other hosts on your LAN.

IP address	MAC	Hostname
223.194.128.233	702C1F267A95	
223.194.128.247	88532E31D9A9	
223.194.128.254	2CFAA2AA9C65	
223.194.128.219	54996364E561	
223.194.129.14	6C299584A328	
223.194.129.11	9800C62CAFA4	
223.194.129.37	CC25EF9DE546	
223.194.129.25	041B6DC59F62	
223.194.129.35	8C1ABF6B646A	
223.194.129.27	0452F30E5EDB	

IP address	MAC	Hostname
223.194.129.35	8C1ABF6B646A	
223.194.129.25	041B6DC59F62	
223.194.129.37	CC25EF9DE546	
223.194.129.11	9800C62CAFA4	
223.194.128.219	54996364E561	
223.194.128.254	2CFAA2AA9C65	
223.194.128.247	88532E31D9A9	
223.194.128.233	702C1F267A95	
223.194.128.144	70700D7A5FE3	
223.194.128.236	0026C7A708AE	

OK

Cancel

Victim

Gateway

3928	180.637479	220.67.228.178	113.198.79.60	TCP	88 62703 → 8891 [PSH, ACK] Seq=1 Ack=1 Win=525568 Len=34
3930	180.667795	113.198.79.60	220.67.228.178	TCP	97 8891 → 62703 [PSH, ACK] Seq=1 Ack=35 Win=525568 Len=43
3931	180.667901	220.67.228.178	113.198.79.60	TCP	54 62703 → 8891 [FIN, ACK] Seq=35 Ack=44 Win=525312 Len=0
3932	180.668244	113.198.79.60	220.67.228.178	TCP	60 8891 → 62703 [ACK] Seq=44 Ack=36 Win=525568 Len=0
3933	180.668245	113.198.79.60	220.67.228.178	TCP	60 8891 → 62703 [FIN, ACK] Seq=44 Ack=36 Win=525568 Len=0
3934	180.668275	220.67.228.178	113.198.79.60	TCP	54 62703 → 8891 [ACK] Seq=36 Ack=45 Win=525312 Len=0

```

.... .... ...0 = Fin: Not set
[TCP Flags: .....AP...]
Window size value: 2053
[Calculated window size: 525568]
[Window size scaling factor: 256]
Checksum: 0x7524 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
▼ [SEQ/ACK analysis]
  [iRTT: 0.000545000 seconds]
  [Bytes in flight: 34]
  [Bytes sent since last PSH flag: 34]
▼ [Timestamps]
  [Time since first frame in this TCP stream: 0.000596000 seconds]
  [Time since previous frame in this TCP stream: 0.000051000 seconds]

```

Printer PC 의 통신패킷을 공격자의 PC에서
훔쳐볼 수 있게 된다.

```

0000 2c fa a2 90 86 ed 50 b7 c3 ac 99 f5 08 00 45 00 , .....P. ....E.
0010 00 4a 0c 50 40 00 80 06 6c 65 dc 43 e4 b2 71 c6 .J.P@... le.C..q.
0020 4f 3c f4 ef 22 bb 1e a7 90 9b 5f 01 0f 69 50 18 0<..."... ..iP.
0030 08 05 75 24 00 00 47 45 54 55 53 45 52 49 4e 46 ..u$.GE TUSERINF
0040 4f 33 0d 0a 30 0d 0a 31 33 39 34 30 37 30 0d 0a 03..0..1 394070..
0050 39 34 31 30 32 33 0d 0a 941023..

```

프린트스타 (JPA) - 인쇄

● 인쇄 작업 ● 인쇄 문서

로그인

사용자 ID : 1394070 비밀번호 : ***** 확인(O)

숫자와 영문자만 입력 가능합니다.

잔액 정보

출력 쪽수 : 1 현재 잔액 : 1,240원

출력 요금 : 20원 출력 후 잔액 : 1,220원

프린터 정보

프린터 종류 : M_흑백소형

프린터 위치 : 미래관

프린터 특성 : 흑백소형

출력 단가 :	A4	A3	B4	Letter
[흑백]	20원	x	x	x
[컬러]	x	x	x	x

프린트스타 JPA

인쇄(P) 취소(C)

미래관 프린터실 로그인

*이더넷
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 113.198.79.60

No.	Time	Source	Destination	Protocol	Length	Info
112	5.138802	113.198.79.60	220.67.228.178	TCP	64	8891 → 62696 [PSH, ACK] Seq=1 Ack=37 Win=525568 Len=10
113	5.139745	113.198.79.60	220.67.228.178	TCP	60	8891 → 62696 [FIN, ACK] Seq=11 Ack=37 Win=525568 Len=0
114	5.139772	220.67.228.178	113.198.79.60	TCP	54	62696 → 8891 [ACK] Seq=37 Ack=12 Win=525568 Len=0
115	5.141784	220.67.228.178	113.198.79.60	TCP	54	62696 → 8891 [FIN, ACK] Seq=37 Ack=12 Win=525568 Len=0
116	5.142041	113.198.79.60	220.67.228.178	TCP	60	8891 → 62696 [ACK] Seq=12 Ack=38 Win=525568 Len=0
3925	180.636883	220.67.228.178	113.198.79.60	TCP	66	62703 → 8891 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
3926	180.637375	113.198.79.60	220.67.228.178	TCP	66	8891 → 62703 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
3927	180.637428	220.67.228.178	113.198.79.60	TCP	54	62703 → 8891 [ACK] Seq=1 Ack=1 Win=525568 Len=0
3928	180.637479	220.67.228.178	113.198.79.60	TCP	88	62703 → 8891 [PSH, ACK] Seq=1 Ack=1 Win=525568 Len=34
3930	180.667795	113.198.79.60	220.67.228.178	TCP	97	8891 → 62703 [PSH, ACK] Seq=1 Ack=35 Win=525568 Len=43
3931	180.667901	220.67.228.178	113.198.79.60	TCP	54	62703 → 8891 [FIN, ACK] Seq=35 Ack=44 Win=525312 Len=0
3932	180.668244	113.198.79.60	220.67.228.178	TCP	60	8891 → 62703 [ACK] Seq=44 Ack=36 Win=525568 Len=0
3933	180.668245	113.198.79.60	220.67.228.178	TCP	60	8891 → 62703 [FIN, ACK] Seq=44 Ack=36 Win=525568 Len=0
3934	180.668275	220.67.228.178	113.198.79.60	TCP	54	62703 → 8891 [ACK] Seq=36 Ack=45 Win=525312 Len=0

[Checksum Status: Unverified]
Urgent pointer: 0
▼ [SEQ/ACK analysis]
 [This is an ACK to the segment in frame: 3928]
 [The RTT to ACK the segment was: 0.030316000 seconds]
 [iRTT: 0.000545000 seconds]
 [Bytes in flight: 43]
 [Bytes sent since last PSH flag: 43]
▼ [Timestamps]
 [Time since first frame in this TCP stream: 0.030912000 seconds]
 [Time since previous frame in this TCP stream: 0.030316000 seconds]
TCP payload (43 bytes)
▼ Data (43 bytes)
 Data: 4f4b3a303030d0a313339343037300d0a3934313032330d...
 [Length: 43]

0000	50 b7 c3 ac 99 f5 2c fa a2 90 86 ed 08 00 45 00	P.....,.....E-
0010	00 53 78 f9 40 00 7f 06 00 b3 71 c6 4f 3c dc 43	-Sx-@...-q-O<-C
0020	e4 b2 22 bb f4 ef 5f 01 0f 69 1e a7 90 bd 50 18	.."....-i...P-
0030	08 05 73 59 00 00 4f 4b 3a 30 30 30 0d 0a 31 33	..sY..OK:000-13
0040	39 34 30 37 30 0d 0a 39 34 31 30 32 33 0d 0a 31	94070-9 41023-1
0050	32 34 30 0d 0a c0 e5 b0 e6 b9 e8 0d 0a 0d 0a 0d	240.....
0060	0a	

사용자의 ID , PW 및
 사용요금까지 훔쳐봄



공공기관 프린터 관리 시스템의 취약점 분석

Vulnerability Analysis of Printer Management System in Public Institutions

저자 (Authors)	지우중, 이경문, 이병천 Woojoong Ji, Kyungmoon Lee, Byoungcheon Lee
출처 (Source)	정보보호학회논문지 28(3) , 2018.6, 655-663 (9 pages) Journal of the Korea Institute of Information Security & Cryptology 28(3) , 2018.6, 655-663 (9 pages)
발행처 (Publisher)	한국정보보호학회 Korea Institute Of Information Security And Cryptology
URL	http://www.dbpia.co.kr/Article/NODE07478917
APA Style	지우중, 이경문, 이병천 (2018). 공공기관 프린터 관리 시스템의 취약점 분석. 정보보호학회논문지, 28(3), 655-663.
이용정보 (Accessed)	한성대학교 113.198.80.*** 2018/10/17 21:20 (KST)



Cain & Abel



Wireshark

End