서론

현재 게임은 단순히 시간을 보내기 위한 수단 그 이상의 가치를 가지고 규모와 질적인 측면에서 상당히 많은 성장을 보였습니다. 소규모의 자본과 인력으로도 충분히 성공을 거둘 수도 있는 산업의 특성상 다수의 게임회사들이 늘어났고, 그에 비해 보안에 대해서는 관심이 비교적 적었던 것이 사실입니다. 게임을 이용하기 위한 개인정보가 해킹으로 유출되거나, 계정을 탈취해서 게임 내 이득을 가로채는 것 뿐 만 아니라 게임 서버 자체를 공격하거나 게임 데이터를 해킹해서 조작을 하는 등 다양한 공격 사례가 있었습니다.

게임 내 데이터를 조작해서 게임을 원하는 대로 또는 편하게 변경하는 것도 게임을 개발한 개발자의 지적재산권을 침해하는 부당한 행위이지만, 게임을 제공하는 회사가 해킹 공격을 당한다면 단순히 게임 내에서 부당한 이득이 발생하는 것을 떠나서 회사와 게임 사용자에게도 피해가 될 수 있습니다. 게임 내에서 세금을 제때 내지 않아 발생한 전쟁으로 실제 현금 3억원 이상의 가치가 사라지고, 게임 아이템 하나가 억대에 거래가 되기도 하는 지금, 그 규모의 크고 작음을 떠나서 게임 컨텐츠 자체에 대한 투자 뿐 아니라 보안에 문제가 생기지 않도록 반드시 대비할 필요가 있습니다.

따라서 본 프로젝트는 현재 지속적인 성장을 보이고 있고, 새로운 게임을 출시할 예정에 있는 SmileGate사에 속한 계열사 SmileGate Entertainment를 가상 회사로 설정하여 현재 서비스 중인 게임 SoulWorker의 관리를 위해서 분리되었다는 상황을 가정하였습니다. 전체 프로젝트는 회사 내 PC 보안 점검과 모의 해킹 및 대응으로 이루어지고, 배웠던 내용이 특정 산업에 특수하게 적용되는 수준으로 보여질 수 있는 없겠지만, 시스템 보안, 웹 보안, DB 보안, 네트워크 보안으로 분류된 공격들을 통해서 게임회사에서 중요하게 다루어져야 할 계정 및 권한에 관한 공격과 웹 서버에 대한 공격 등 게임회사에서 빈번하게 발생할 수 있는 이슈에 대해서 점검하고 취약점을 보완하는 과정을 진행하였습니다.

결론

지금까지 본 프로젝트에서 가상회사인 SmileGate Entertainment를 대상으로 보안 점검 및 모의 해킹과 그에 따른 대응 조치 설정을 진행하였고, 계정 및 감사 정책 등 PC 보안 사항 점검과 시스템, 웹, DB, 네트워크로 구분된 모의 해킹을 통해 취약점을 점검하고 대응책을 제시하였습니다.

계정 정책에서는 계정 관리에서 중요한 비밀번호에 대한 설정과 기본 계정인 관리자 및 게스트 계정에 대한 설정, 용도에 따른 계정 분리 및 권한 부여에 대해서 확인했고, 감사 정책에서 필요한 로그를 기록하는 설정, 백업 일정에 대한 설정 등을 점검했습니다.

이후 모의 해킹에서는 시스템 보안에서 공격자가 회사 내부 네트워크에 접근이 가능해진 경우 내부 네트워크에서 동작 중인 PC의 IP를 확인하거나 서비스 중인 포트를 확인할 수 있다는 것을 확인했습니다.

웹 보안에서는 SSL 설정이 되어 있어서 웹 서버에 대한 접속이 암호화 되어 있더라도 XSS이나 SSL strip 공격에 의해서 세션 쿠키 값이 노출될 수 있고, 그 쿠키 값을 이용해 요청 패킷을 변조해서 탈취한 계정의 권한을 사용하는 것이 가능하다는 것과 Brute Forcing을 이용해서 계정 정보를 알아내는 공격을 확인했습니다.

웹 보안과 DB 보안과 관련해서는 웹 사이트에 값을 넘겨주는 과정에서 발생하는 취약점을 이용해서 서비스 이용자에게 공격을 하고 서비스 이용자가 자기도 모르게 자기 권한으로 공격자가 의도한 작업을 하게 하거나 DB 정보를 알아내는 등의 공격이 가능한 것을 확인했습니다.

마지막으로 네트워크 보안에서는 ARP Spoofing을 이용한 MITM 상태를 기반으로 IP Spoofing, DHCP Spoofing, DNS Spoofing등 다양한 Spoofing 공격이 가능했고, DHCP Starvation 같은 DOS 공격, SSL Strip 이나 VPN Snffing과 같이 패킷의 암호화 관련 취약점에 대해서 알아보았습니다.

프로젝트 과정에서 성공한 공격들에 대해서 방어에 필요한 PC 설정을 확인하고 사용 가능한 보안 장비를 이용해서 공격을 방어하는 방법과 직접 Secure Coding 등을 통해서 공격에 대응하는 방법을 확인했습니다.

의의 및 한계

수업을 통해 알게 된 내용으로 점검할 취약점 목록을 설정하고 방어 방법을 종합적으로 테스트 할 수 있었다는 점에서 프로젝트의 의의를 찾을 수 있다고 생각합니다. 다만 지식이 부족해 가상회사를 설정했음에도 특정 산업에 특징을 반영하여 점검이 이루어지지 못했다는 점, 배웠던 내용들도 전부 적용해서 프로젝트를 진행하지는 못한다는 점은 아쉽게 느껴집니다. 이후 다시 프로젝트를 기획한다면 가상으로 설정한 회사가 속한 산업에서 일반적으로 이루어지는 보안 설정들을 파악해서 해당 산업에 중요하게 다루어야 할 부분을 집중적으로 다루고, 오래 전부터 공격이 이루어져서 현재는 대부분 방어가 되어 있는 내용보다 최근에 많이 이루어지는 해킹 방법들을 알아보고 적용해보는 작업을 포함하는 것이 더 의미 있는 프로젝트가 될 것이라고 생각합니다.

프로젝트를 통해서 느낀 점

* 6개월 동안 수업 내용을 따라가고 시험 보기에 급급하다가 전체적으로 정리해볼 수 있는 시간이 된 것 같아서 좋았고, 프로젝트를 진행할수록 취약점 점검이나 대응에 있어서 배운 내용 외에는 아는 게 없는데 아는 것 만으로는 부족하다는 느낌이 많이 들어서 아쉬움이 남는다.