PROCESSO SELETIVO GRIS 2020.1
TAG ENGENHARIA SOCIAL - FRANKLIN MARTINS

Nome: Yuri Medeiros da Silva

Enunciado: *Você foi contratado por uma empresa para testar a sua segurança física. Para isso, você pode usar de vários artifícios para obter sucesso em suas atividades. Digamos que você obteve. E para isso você explorou as falhas humanas (e usou algumas das técnicas do Mitnick) e também fez uso de tecnologia nesse processo. Agora que você terminou, eu quero que você me mande um relatório explicando tudo que você fez (digamos que eu seja o dono da empresa).*

Da motivação:

A JRFU há alguns anos já é considerada um polo tecnológico. Isso significa que empresas não apenas constroem sua PD, como também desenvolvem suas vantagens competitivas ali, que, em mãos errada, pode gerar grandes perdas financeiras, ou de vantagens estratégicas. A empresa X que desenvolve uma nova solução para tratamento dos dados dos seus clientes para ampliar suas vendas e o endereçamento de produtos, disponibiliza dados sensíveis de seus clientes e da empresa para seu núcleo de desenvolvimento na faculdade, laboratório esse localizado no ECN com parceria com alunos e professores do CCD.

Dado o medo de perder sua vantagem sobre as concorrentes, fui contratado pela empresa X para ver se seus dados e planos estavam de fácil acesso para qualquer espião ou pessoa má intencionada de outra possivel empresa.

Detalhes:

ETAPA 1: Do reconhecimento digital

A primeira etapa consiste em coletar dados possivelmente úteis e disponíveis na web. Basicamente, procuramos extrair informações dos sites principais.

Com o simples acesso e busca ao site do ECN já consigo extrair nome, telefone e email dos principais indivíduos envolvidos no projeto da EMPRESA X, além de algumas informações acadêmicas. Próximo passo é traçar ainda mais o perfil dos elementos, procurando informações em redes sociais, linkedin..., qualquer informação pode ser útil nessa fase - o grande ponto chave é saber as rotinas e padrões mais comuns das pessoas, até mesmo locais que costumam frequentar. Também consigo extrair dados da estrutura hierárquica do ambiente (diretores, vice-chefes, …) o que pode fazer com que certos nomes me ajudem a abrir portas.

Na hora de capturar o footprinting virtual de cada pessoa alvo podemos utilizar sites como *checkusernames.com* e *knowem.com* para descobrir as redes sociais que eles participam. Ainda, com os dados de telefone encontrados no site do ECN podemos tentar algumas ferramentas OSINT de geolocalização como o *geocreepy e o PhoneInfoga*

Para acessarmos o ECN precisamos passar por uma catraca, normalmente isso pode não ser tão simples e impedir algumas técnicas de tailgating. Cruzando os dados encontrados nos sites do ECN e do departamento mais próximo o CCD, pudemos notar que

alguns professores atuam nos dois. Acessar o CCD, pode ser uma das formas mais fáceis de ter acesso ao ECN. Acessando apenas os sites conseguimos traçar o perfil hierárquico do CCD e vemos que uma instalação onde os alunos servem pode ter privilégio suficiente para nos ajudar a chegar ao objetivo, o ICL. Continuamos nossa busca, agora pelo linkedin, descobrimos quem trabalha no ICL, o que cada um faz e como são divididas as equipes

Para finalizar o reconhecimento digital, procuramos por possíveis códigos dos alunos do laboratório em sites abertos, como github, utilizando o *searchcode.com*. Um dos alunos do laboratório, deixou senhas padrões em texto plano em códigos diferentes, isso pode não significar nada, mas é uma boa tentativa de senha padrão.

ETAPA 2: Do reconhecimento físico

A sede de pesquisa se localiza no ECN bem próximo ao CCD, acessar o ECN e conseguir dados que precisamos não é a coisa mais fácil do mundo. Eles possuem alguns mecanismos como catraca, algumas vezes pude notar pessoas entrando com cartão, e quando acontecia alguma indisponibilidade no sistema os seguranças permitiam qualquer pessoa entrar. (Alguns desses dados puderam ser coletados vias reclamações no twitter. Não conseguimos muitas informações do ambiente via instagram, ou em possíveis fotos postadas na internet).

Catraca e cartão são métodos mais complicados, o cartão ainda poderia ser explorado roubando os dados de algum aluno - de fácil acesso, basta pesquisar o nome com dork de pdf no google e conseguimos seus dados em planilhas de materiais unificadas - e fazendo o cadastro de um cartão fake, já que ninguém supervisiona diretamente o cadastro de cartões. Não seria difícil fazer um site fake (*phishing*) com o site que lê qrcode da catraca e roubar algumas contas, a rede costuma ser instável, criar um hotspot fake claramente funcionária, entretanto, essas formas não nos foram permitidas pela empresa e configurariam crime .

Ainda durante o período de observação e pesquisa pude notar que os alunos que trabalham no ICL possuem certos privilégios, os vi pegando chaves sem muita dificuldades - contanto que a chave já estivesse no balcão - e também conseguindo acesso a maioria dos locais sem nenhum verificação (apenas utilizando a mesma forma deles de se apresentar) , eles só se identificavam como membros do ICL e todo privilégio lhes é dado. Pude também mapear a secretaria onde o responsável expõe todos os seus dados em redes sociais, não seria muito difícil infectá-lo com algum email (*spearphishing*) mas procuramos algo ainda mais simples.

Pra finalizar essa etapa, notei que a maioria dos alunos do ICL saem antes das 17h - com exceção de um ou outro - e a troca de turno dos guardas costuma acontecer às 18h horas, como esses guardas possuem pouco contato com os membros do ICL seria mais fácil se passar por um deles e conseguir acesso ao nosso objetivo. Com a chave do ICL conseguiríamos acesso a quase toda a rede.

ETAPA 3: Da estratégia à prática

Minha primeira tentativa para chegar foi tentando acesso a secretaria do CCD. Foi uma das etapas mais fáceis - porém arriscadas - apenas comuniquei ao responsável da secretaria que era do ICL e o professor X tinha pedido para eu verificar se a máquina da

secretaria estava infectada. Todos os dados e nomes utilizados nessa etapa foram de fácil acesso com alguns google dorks e pesquisas nas redes sociais.

Tive acesso a todos documentos importantes do CCD, como provas, relatórios de notas e afins, também fui capaz de identificar algumas vulnerabilidades nas máquinas com windows 7 antigas - facilmente conseguiria escalar e roubar dados sigilosos ou conseguir acesso a membro mais importante, o que não era meu objetivo. Minha próxima abordagem seria conseguir a chave da supervisão para ter acesso a rede - o que seria fácil, pois indo no funcionário certo ele apenas me entregaria a chave sem muitas perguntas (isso se a chave já estivesse em cima do balcão), contudo, descobri antes disso que a rede do CCD e do ECN estavam separadas.

Para entrar então precisaria de acesso pelas catracas. A estratégia pensada consistia em algumas ferramentas de osint de geolocalização https://n0where.net/creepy, e sms spoofing. Sms são poucos usados aqui no nosso país, entretanto a rede 3g/4g no prédio é péssima, então poderia ser justificável receber um sms do que uma mensagem no whatsapp. Combinei o horário em que o professor responsável da pesquisa estava em aula(dado facilmente encontrado no google), e, utilizando seu número de celular (encontrado no site) enviei uma mensagem me passando pelo professor responsável para um dos alunos que estava no laboratório informando que um supervisor da empresa iria no laboratório em instantes. Ao mesmo tempo, enviei um email falso ao professor coordenador do projeto informando que um supervisor iria ao local, como o professor estava em aula no momento ele muito raramente veria o email ou responderia a algum contato do aluno. Também estava de olho caso o *creepy* me mostrasse alguma movimentação brusca do professor em direção ao laboratório.

Passar na catraca foi um dos meus menores problemas, informei a secretária da guarita que era membro da supervisão do ICL (jargão utilizado pelos membros) e que precisava ir em um laboratório e meu celular estava descarregado pro app, assinei a pauta com os dados de algum membro real e não tive problemas. A moça não fez questão de verificar nada, apenas me deixou passar, o mesmo aconteceu na saída.

Nesse meio tempo consegui chegar ao laboratório, me encontrar com o aluno e fazer perguntas que comprometem o ambiente, inclusive pedi senhas de acesso e fiz testes localmente, por fim pedi uma cópia do sistema atual para meu pendrive.

⇒ Outro possível ataque seria executar um MITM com base no acesso físico ao switch do ECN, esse seria um pouco menos arriscado pois envolveria menos conversa humana e qualquer suspeita bastaria informar que eu estava fazendo um teste para o ICL. Chegando ao switch, faria um footprinting e “enumeração” da rede com o *Maltego* e desviaria o tráfego da rede desejada para obter as informações desejadas. Também poderia ter realizado um atauqe de *MacFlooding*, e conseguir acesso aos pacotes que estavam sendo transmitidos na rede, a parte complicada, talvez, seria distinguir a informação que desejamos do resto.

⇒ Para alguém mal intencionado, também não seria muito complicado clonar a página de acesso e roubar os dados de login de alguma pessoa. (SET).

⇒ Ainda, forçar o sistema de login para alguém mal intencionado seria algo fácil e depois, com a entrada liberada para todos, qualquer um poderia acessar.

ETAPA 4: Da conclusão

Para a mitigação das falhas exploradas será necessário instruir os seguranças presentes a verificarem a real identidade dos indivíduos devidamente, qualquer um que se passe por membro do ICL possui acesso fácil a boa parte das instalações.

Quanto aos possíveis ataques ao switch, o bloqueio de portas (*físicas)* que não estão em uso pode ser bem efetivo.

E, talvez o mais importante, informar aos contribuintes do projeto do laboratório do real estrago que essas informações em mãos erradas podem causar, para que eles estejam mais atentos e adicionem desenvolvam formas de verificarem os reais remetentes das mensagens.

Disclaimer: Tudo aqui relatado tem caráter exclusivamente educativo e fictício. Minha intenção é apenas compartilhar conhecimentos de modo a informar e prevenir. Não compactuo nem me responsabilizo pelo uso ilegal ou indevido de qualquer informação aqui incluída.

Algumas Fontes úteis:

www.social-engineer.org/framework/se-tools/computer-based/social-engineer-toolkit-set
iq.opengenus.org/mac-flooding-attack/
https://howdoesinternetwork.com/2011/mac-address-flooding
https://www.youtube.com/watch?v=hPIhItC-Vr8
https://docs.maltego.com/support/solutions/articles/15000011881-network-footprinting-with-maltego).
https://www.tracesecurity.com/uploads/Onsite-Social-Engineering-Sample-Report.pdf
https://digitalguardian.com/blog/social-engineering-attacks-common-techniques-how-prevent-attack
https://www.cisco.com/c/dam/en_us/training-events/le31/le46/cln/promo/share_the_wealth_contest/finalists/Hany_EL_Mokadem_Switch_Attacks_and_Countermeasures.pdf
https://www.first.org/resources/papers/tc-oct2002/d1-s2-kristoff-slides.pdf
https://www.redscan.com/news/ten-top-threats-to-vlan-security/
https://cybersecurity.att.com/blogs/security-essentials/vlan-hopping-and-mitigation
https://www.blackhat.com/presentations/bh-usa-02/bh-us-02-convery-switches.pdf