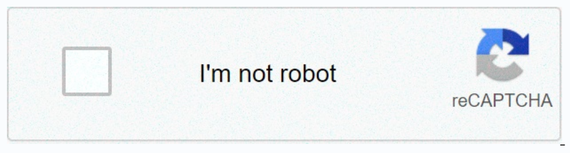


Continue

# Bypass meaning in information security

Nathan House is the founder and CEO of X Station a cyber education and consulting firm. Social Engineering uses influence and persuasion to deceive, persuade or manipulate. As a result, the social engineer is able to take advantage of people to obtain information with or without the use of technology. The following is an example of previous work I performed for a customer. It shows what seemed to be insignificant information that can build trust with people and endanger a company. This has been provided as further reading for an interview I did on penetration testing and social engineering for PC Extreme magazine. Social Engineering ToolsTo explain how I could go about using a combination of social engineering and technology I first need to explain the tools I use. We have many tools that we have developed for the purposes of penetration tests. In this example of social engineering, you should use a package or executable wrapper, a rootkit, and the RAT (Remote Access Tool). Simply put, the wrapper can create executable programs that seem to do one thing but, in fact, perform other tasks as well. Our wrapper also encrypts and compresses content to help deflect virus scans and computer criminology. RAT is a remote access tool that, when running on a computer, searches for connections outside the Internet network by using proxy servers and other devices, if required. RAT uses outgoing connections from the destination computer to obtain its commands to completely bypass any security from a firewall or NAT. Communication traffic is also sent as legitimate HTTP/HTTPS traffic, so even if the destination proxy server or firewall is filtered at the application level, the control commands will appear as normal HTTP traffic because, in fact, they are. This means that we can communicate with targets deep within the company's networks and defeat firewalls/proxies/DMZ, etc. RootKit is a program that hides the actions of hackers from the operating system and anyone who examines the machine. Our Rootkit hides processes, handles, modules, files and folders, registry keys and values, services, TCP/UDP Slots, and Systray Icons.What does this mean that the task manager, netstat, regedit, file explorer, etc. The hacker's actions and programs will be completely invisible. There are some less sophisticated versions of these types of tools available on the Internet, but there are two good reasons why a professional He won't use them. One is that they do not provide the required functionality, and the other reason is that many viruse controllers will get their signatures and stop them. That's the difference between the kiddie script and the professional hacker. Social Engineering call #1Call the organization's main switchboard from my mobile phone. Hey, I have a problem with my office phone. You can put me in someone who might be able to. Position. Can I make that clear to me? Reception: Connects you. Phone services: Hi.Nathan: Hi, I'm having a problem with my office phone. Sorry, I'm new here. Is there any way I can find out who's calling me when they call my office phone? Is there a caller ID? Because users typically use their mobile phones, the caller ID is not often associated with a name. Is that a problem for you? No, he's fine now. I understand. Thanks. Bye.I now know that the company uses hot desks and that phone caller ID is not always expected. Therefore, it is not a question of whether I call from outside the company. If it was to be expected, then I could skip it anyway. Social Engineering #2Call to the organization's main distribution table. Hey, can you put me in the building security? Reception: All right. Building security: Hello, how can I help you? Nathan: Hi, I do not know if you will be interested, but I found an access card outside the building that I think someone must have dropped. Building security: Just return it to us. We're in building 3.Nathan: Okay, no problem. May I ask who I'm talking to? Building security: My name is Eric Wood. If I'm not here, give it to Neal. I'm going to do it. Are you the head of building safety? Building security: It's really called Security Facilities and the head is Peter Reed.Nathan: OK, thanks a lot. Bye.This told me the name of a number of people in security, the correct name of the department, the head of security, and that they are the ones dealing with physical access cards. Social Engineering #3Call to the organization's main distribution table. Hello, I'm calling from the Agency Team and I'm wondering if you could help me. I had a meeting about a month ago with some of your HR people, but unfortunately, my computer crashed and I completely lost their names. Reception: Sure, no problem. Let me search the station. Do you have any idea their names? I know one of them was the head of the T.A.D. There were a number of people at the meeting though. Slot:..... OK, here we are. The head of the D.A.D. is Mary Kilmister. 0207 xxxxxXNathan: Yes, this rings a bell. What are the other names in the D.A.D.? Reception: At HR, Jane Ross, Emma Jones..... yes, I'm sure Jane and Emma. Can I have their numbers, please? Reception: Sure. Jane Ross is xxxxxxx and Emma Jones is xxxxxxx. You want me to put you in one of them? Yes. Can you send me to Emma, please? Now I know the names of the three people in the D.A.D., including the head. Social Engineering call #4HR: Hi, Emma here. Hello, Emma. This is Eric from Facilities in Building 3. I wonder if you can help me. We had a problem here with the access card database computer. It crashed last night and some of the data on the new starters is gone. Do you know who would have been able to tell who the new starters were over the last 2 weeks as their access cards would have stopped working? We need to contact them and let them go. Let. Asap. I can help you with that. I'll go through the names and email them to you, if you don't mind? In the last two weeks, you say? For the last two weeks, yes. That's great, thanks, but it would be possible to fax it as we share a computer for email and that was affected by the computer crash, too. yes, that's all right. What's your fax number? And what's your name? The sign for Eric's attention. I'm going to have to find the fax number for you and call you back. Ok. Do you know how long it's going to take to get the information? It won't take me more than 30 minutes. Nathan: You'll be able to start working on it right away, since it's quite urgent. I have a few things to do this morning, but I'm going to have to have the names this afternoon. That's great, Emma. Thanks. When you're done, will you be able to call me right away so I can start re-ing their cards? Oh, yes, of course. What's your number? I'll give you my cell phone number the way you're going to call me. 07970xxxxxx. I'll call you when I have the list. Excellent, thank you. I really appreciate that. Social Engineering invites SupportCall #5IT the organization's main switching table. Could you put me through IT support? Reception: Connects you... (Long wait in line.) IT Support: Hello, can I have your LS number or your case report? I have a quick question. Is that OK?IT support: What is it? Nathan: A guy from Reuters tries to send me a presentation and asks me what the maximum size is for attachments.IT support: It's 5MB, sir. That's great, thank you. And one more thing. He said it's a .exe file and sometimes, they get blocked or something.IT support: They won't be able to send an executable file as the viruses will stop it. Why should it be an exe file? I don't know. How can he send it to me then? Could the zipper or something?IT Support: Zip files allowed, sir. Okay, one more thing. I can't see my Norton Anti-virus icon on my system disk. The last place I worked, there was a little icon.IT support: We run McAfee here. It's just a different icon - the blue one. That explains it then. Thank you, bye. Now I know that to send an executable via email, it must be compressed first and less than 5 MB. I also know that they use McAfee anti-virus. Social Engineering call (6) A few hours later, call from Emma at Human Resources.Emma: Hey, is this Eric? Yes, hello. I have the new list for you. You want me to fax it? Yes, please. That would be great. How many are there? About 10 people. I'm not sure the fax works properly here. Can you read them to me? I think it'll be faster. Ok. Do you have a pen? Yes, go ahead. Jones, Sales. My manager is Roger Weak, ..... Okay, thank you. You've helped a lot. Goodbye I now have a list of new starters over the last 2 weeks. Weeks. they also have the departments to which they belong and the name of their director. New starters are many times more prone to social engineering than long-term workers. Social Mechanical Call (7)Invitation to the organization's main distribution table. Nathan: Hi, I'm trying to email Sarah Jones, but I'm not sure what the format of your email addresses is? Know? Reception: Yes, it would be sarah.jones@targetcompany.com.Nathan: Thanks.Social Engineering email #1Minutes later, a forged email is sent.from: itsecurity@targetcompany.comto: sarah.jones@targetcompany.comsubject: IT SecuritySarah, As a new starter for the company, you need to be informed about the company's IT policies and procedures and procedures and specifically, employees Acceptable Usage Policy. The purpose of this policy is to describe the acceptable use of computer equipment in the target company. These rules apply to the protection of the employee and the target company. Improper use exposes risks, including viruses attacks, breach of network systems and services and legal issues. This policy applies to employees, contractors, consultants, temporary and other employees of the target company, including all staff associated with third parties. This policy applies to all equipment owned or leased by the target company. Someone will contact you soon to discuss it with you. When it comes to calling #8A two hours later, call the organization's main switchboard. Hey, can you get me to Sarah Jones, please? Reception: Connects you. Hello, Pauli. How can I help you? Hello, Sarah. I call it Security to let you know about IT security best practices. You should have got an email about it. yes, I got an email about it today. Okay, great. It's just standard procedure for all new starters and only takes about 5 minutes. How do you find things here? Are you all helping? Oh, yes, thank you. It's been great. It's a little daunting starting somewhere new, though. yes, and it's always hard to remember everyone's name. Did Roger introduce you? (..... various small discussions about building rapport are inters with more confidence-building.) Nathan:... Emma Jones is very nice at HR if you need any help with this side of things. yes, Emma gave me a human resources interview for the job. Well, I'd better run to the security presentation with you. Do you have your email open? I'll send you the security presentation now and guide you. Okay, I see the e-mail. Nathan: OK, just double-click the Security Presentation.zip attachment. Sarah: It has come down to WinZip.Nathan: Just click on the quote and double-click on The Sarah Security Presentation: ..... The executable that ran is, in fact, a cleverly packaged set of scripts and tools created by our wrapper program, including within the rat, a rootkit, keyloggers, and anything else I might want to add. When the file clicks, the presentation starts immediately. Presentation. is just a series of PowerPoint slides telling her not to run executable files sent, etc ☺. A few seconds later, as this is taken through the presentation, scenarios within the package begin to try to disable McAfee and any other computer security that can be found that can help protect the user. The rootkit is then installed by hiding all future actions from the operating system or anyone conducting a forensic investigation. Then the RAT is hidden and installed. The RAT is made to start every time the machine restarts and these actions are all rootkitted and hidden. The RAT then searches for any proxy settings and other useful information and tries to get out of the network and on the Internet, ready to take its commands from its master. Obviously, all TCP processes and connections are hidden, and even running things like netstat and task manager won't reveal them. The rat is connected to the master. Now own computer and it's time to start looking around and really start hacking! Project. If you want to learn more about social engineering and hacking skills I recommend checking out my baby The StationX Cyber Security School. This article was originally published here. (Disclaimer: The author is the Founder and CEO at StationX) Join Hacker Noon Create your free account to unlock your customized reading experience. Experience.