BNE LLC
BREAKING N ENTERING LLC
PENETRATION TEST
GUIDANCE REPORT

VERSION 1.0

AUGUST 21, 2021

AARON ALBINO | PHILLIP CHOE | L.A. HARRIS

BNE LLC

BREAKING N ENTERING LLC

Contents

BNE LLC

BREAKING N ENTERING LLC

1.A Introduction

This penetration test report contains all agreed upon methods and efforts to conduct both a physical and network driven penetration test in order to override the security measures. This report will reflect all the threats and vulnerabilities found, grading these by severity as well as providing technical knowledge and solutions to enhance safety measures and protocol.

1.B Objective

The objective of this assessment is to perform a physical and network penetration test against the Paradisus Cancun Hotel Resort. BNE LLC will be tasked with using skills that include but are not limited to social engineering tactics, physical breach strategies, and network exploitation. This test will simulate an actual penetration test and how you would start from beginning to end, including a scenario-based assessment report.

1.C Synopsis

Frank Abagnale was recently appointed CEO and majority stakes owner of Paradisus Cancun Resort along with it's nationally recognized chain of hotels. Following this recent acquisition, Juan Rivera, the CISO or Chief Information Security Officer, has contracted BNE LLC to perform a security penetration test at Paradisus Cancun Resort during Labor Day Weekend (September 3 - 5, 2021). This is when the company will hold it's first media press conference announcing the newly appointed CEO. A security penetration test is an agreed upon dedicated attack against both the physical and network security systems. The objective of this test is to perform attacks, similar to those of a hacker that is attempting to gain access to the resort's sensitive data information which includes but is not limited to those of past, current, and future hotel guests, new business meetings, conference calls, vendor & client information, and it's books & financials. BNE LLC's overall objective is to gain access to the resort's network via Abagnale's privileges or alternatively with the resort's Manager, Maria Rosa's privileges. BNE LLC is to identify the network's systems, exploit it's flaws, and report the findings back to Rivera and his security team.

2.A Parties Involved

This acknowledges who both the client and the security penetration test teams are.

Client

Paradisus Cancun Resort
Boulevard Kukulcan, KM 16.5
Cancún, 77500

2.B Scope of Work

This clause runs through the obligations of both parties involved including both the security penetration test team and the client.

The security penetration test team, BNE LLC, is responsible for:

- Conducting a thorough security test to the best of their abilities, with the methodologies that are agreed upon within this contract.
- Following up with a comprehensive test report detailing the vulnerabilities, solutions, and preventative measures.
- Providing recommendations for the systems that are found to be vulnerable to security breaches.
- Securely delivering the analysis as well as properly disposing any and all data that is taken as evidence thereafter.

The client, Paradisus Cancun Resort LLC, is responsible for:

- Giving proof of authorized consent for the security penetration test to take place in the form of signed documentation.

- Conducting backup drives for all data prior to the agreed upon security penetration test during Labor Day Weekend.
- Keeping the knowledge of this test strictly between authorized personnel of the CEO, CISO, and Resort Manager.
- Procurement of payment

2.C Rules of Engagement

- The security penetration test team will be allowed accessed stay to a room as if they were a normal guest as a real-world hacker may have the same privileges.
- The attack methods used can include use of uniforms/disguises such as that of hotel staff as a real-world hacker may exploit the same vulnerability.
- Methods such as lock-picking and brute force tools can be used only if no physical damages may occur to physical property of the resort as a real-world hacker may exploit the same vulnerability.
- If rooms prove to be vulnerable, the security penetration test team will only be allowed to physically access rooms that are not resort guest’s rooms.

- If network access proves to be exploitable, the security penetration test team will not be allowed to remove or edit existing files as to not jeopardize the current flow of daily operation.
- If network access proves to be exploitable, the security penetration test team will only be allowed to procure proof of performance via copies or screengrabs of documentation.
- If at any point the security penetration test team is caught or jeopardized, they are to procure documentation that provides proof
- of agreement as well as contacting the agreeing parties of this security assessment.

3.A Social Engineering

- Pretexting: this is a type of social engineering tactic where the attacker creates a scenario where the victim feels compelled to comply under false pretenses. Typically, the attacker will impersonate someone with a position of power to persuade the victim to follow their orders with a sense of urgency.
    - Impersonate a member of the CEO's personal security team doing a patrol of the resort's facilities. Interact with hotel cleaning staff, attempting to clone their access cards which will gives access to all the rooms in the resort.

  - Impersonate a member of the media that is at the resort for the press conference. Can disguise a RFID card reader as a media recording device. Can use a camera for shoulder surfing at a distance.

- Tailgating: this is a type of social engineering tactic where the attacker gains physical access to an unauthorized location. Tailgating is achieved by closely following an authorized user. An attacker may tailgate another individual by quickly sticking their foot or another object into the door right before the door is completely shut and locked.
  - Can tailgate into rooms / offices that aren't accessible with key card access.

3.B Key Card Cloning

- RFID Card: this is a proximity card that's uses 125 kHz radio frequency fields to communicate with readers when in close proximity. Hotels use RFID cards to give guests access to their rooms and staff to their offices.

- Cards use a simple LC circuit. When a card is presented to the reader, the reader's electrical field excites a coil in the card. The coil charges a capacitor and in turn powers an integrated circuit. The integrated circuit outputs the card number to the coil which transmits it to the reader. The transmission of the card number happens in the clear, it is not encrypted.

- The RFID reader/writer tries to mimic the card reader and if successful, can access any data stored on the card. Once that data is stolen from the RFID card, the device can clone that data into a duplicate blank RFID card. This duplicated card can then be used to bypass any lock or security system the original card had access to. The device is also user friendly enough so that any amateur could leverage it to gain access to your organization's environment.

3.C Key Stroke Injection

- The objective of this is to quickly gain access to a network connected computer. One method is the insertion of a rubber ducky. A rubber ducky is a keystroke injection tool disguised as a generic flash drive. This rubber ducky will allow us to quickly inject a reverse bind shell onto the target network in a manner of seconds, setting up a

- listener so that when we get back to our attacking machine, we can implement our exploit to escalate privileges.

- A program will be downloaded into the rubber ducky to deliver a payload. This will allow the injection to disable the firewall system. A http server will need to be spun up so that we can send the network information there. The rubber ducky will continue to access the network details and will send it to the attacking machine that has been set up prior, providing information including ip addresses that will allow the utilization of GTFO bins to escalate privileges.

- With root access, we can navigate and grab screenshots to include in the report detailing vulnerabilities and the risk of information that can be stolen. If unsuccessful in gaining physical access to a system, we will attack the resort's guest wifi to see if it is separate from the network that contains sensitive data obtained from guests. Can grab whitelisted MAC addresses on the network by running Aircrack-ng. By spoofing MAC addresses, we can connect to their private network and runs scans for open ports and services to attack.

4.A Social Engineering Remediation

- Pretexting: the best way to prevent and manage pretexting attacks is to implement awareness training to your staff. Create a layered approach with a policy on how your organization should approach these attacks. Consider asking your employees to ask for verification of identity or proof of services. Is the person requesting access to your files who they say they are? Did you confirm with Verizon that they indeed sent a repair person to your home? In the digital space, be wary of who you open files from as they can be phishing attempts? Why is this person asking me to urgently open a hyperlink they sent? Always be wary!

- Tailgating: it's all about building a secure culture that challenges principle. You don't need security at every single door. Regular access control such as badges, smart cards, and turnstiles are all efficient, however empower your employees and staff to understand the risks of tailgating and to challenge unfamiliar faces that come along the way. Why did this person who I do not know follow me through this door? Do they have appropriate access or are they using my credentials to get in?

4.B Key Card Cloning Remediation

- Key cards can easily be misplaced or lost, risking the possibility of someone copying the card. One course of action is to add Two-Factor identification where additional to the card, an alternate password must be included in the form of a pin.

- Contactless Smart Card Technology utilizes 13.56-MHz rather than its 125 kHz counterpart. This ensures more security because of its more complex encryption. Smart cards have embedded integrated circuits which have the ability to either process of store data and also have the ability to communicate with a terminal using waves de radio.
- Mobile access with smartphones are starting to replace access cards because of their ability to designate, track, and remove access to individuals. They also do not have the ability to be taken to copy and then duplicate.
- RFID blocking wallets block signals by reducing the power of the readers signal which in turn would acquire your cards data.

4.C Key Stroke Injection Remediation

- Consider setting up a more detailed IPS/IDS (Intrusion Prevention System/Intrusion Detection System). Alerts should be set up whenever there are multiple ping sweeps. Keep track of logs as logs

- should be maintained and watched for any suspicious network device activity. Duckhunt is a simple yet very useful tool in fighting off rubber ducky attacks. It stops the rubber ducky from launching

- CMD or Powershell, but it also drops every 5th to 7th keystroke. The client side may think that the injection was fully delivered, however the target machine broke the injection code with this technique so it prevented the attack.