Abertay University

Evaluating and Identifying the Most Effective Detection Methods for Purple Team Engagements Against RDP Honeypots

Christopher Di-Nozzi

BSc (Hons) Ethical Hacking

Supervised by Jamie O'Hare

Introduction

The Remote Desktop Protocol (RDP) is popular with cybercriminals due to the level of access it provides. RDP has seen many security vulnerabilities, including the infamous remote code execution vulnerability, BlueKeep.

Honeypots can be used to learn about current attacks and trends, but a honeypot is effective if it cannot be distinguished from the service it is mimicking. Knowing how to effectively fingerprint honeypots can improve the honeypot itself and the work of those participating in ethical offensive engagements, for instance, purple teams.

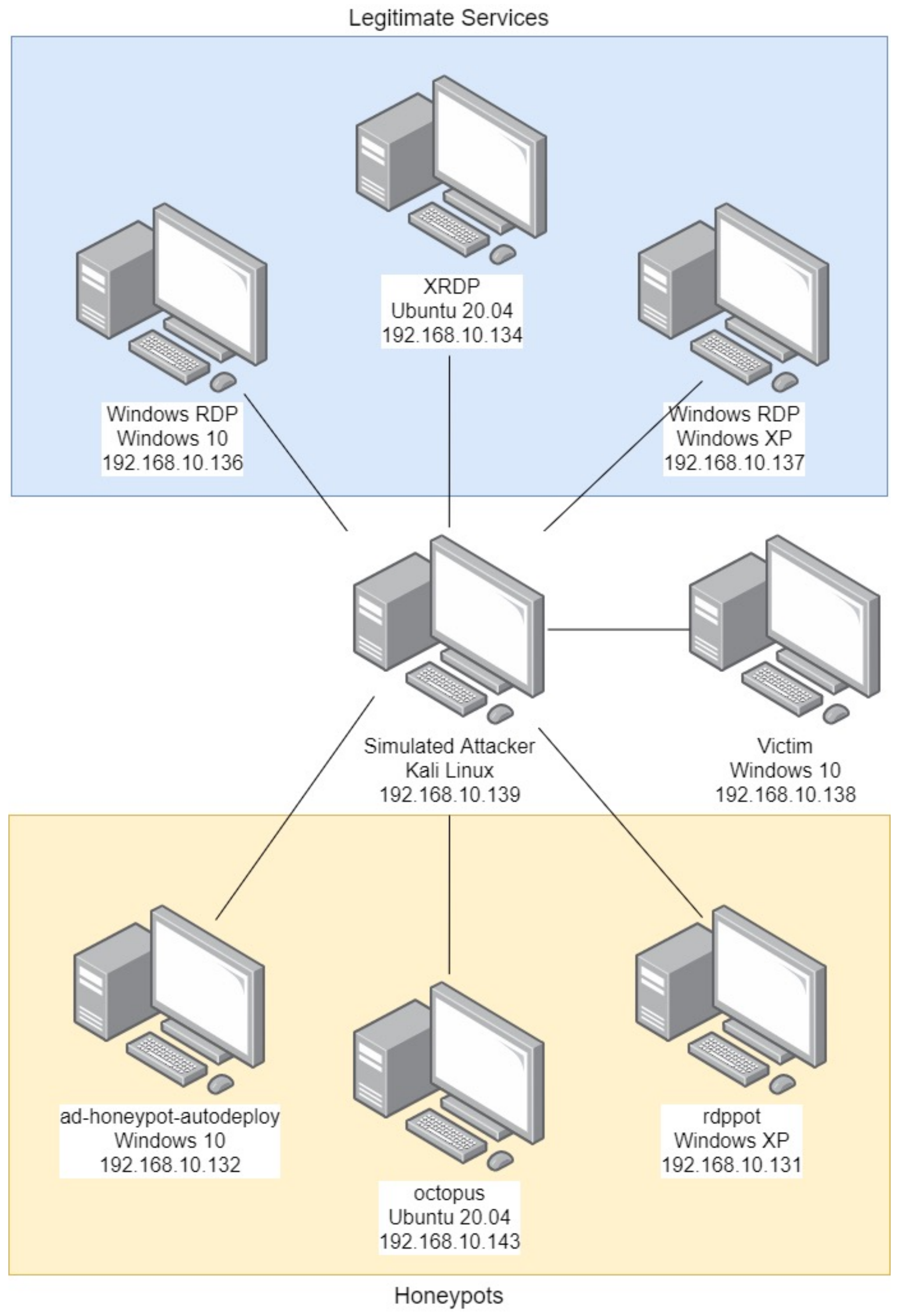
Aim

This project aims to identify and evaluate the most effective detection methods for purple team engagements against contemporary RDP honeypots. This aim can be broken down into three different research questions:

1. What are the existing honeypot detection methods, and how do they compare?
2. Which detection technique is most effective in a purple team engagement?
3. How can these detection methods, honeypots, and the broader network be refined to improve effectiveness?

Methodology

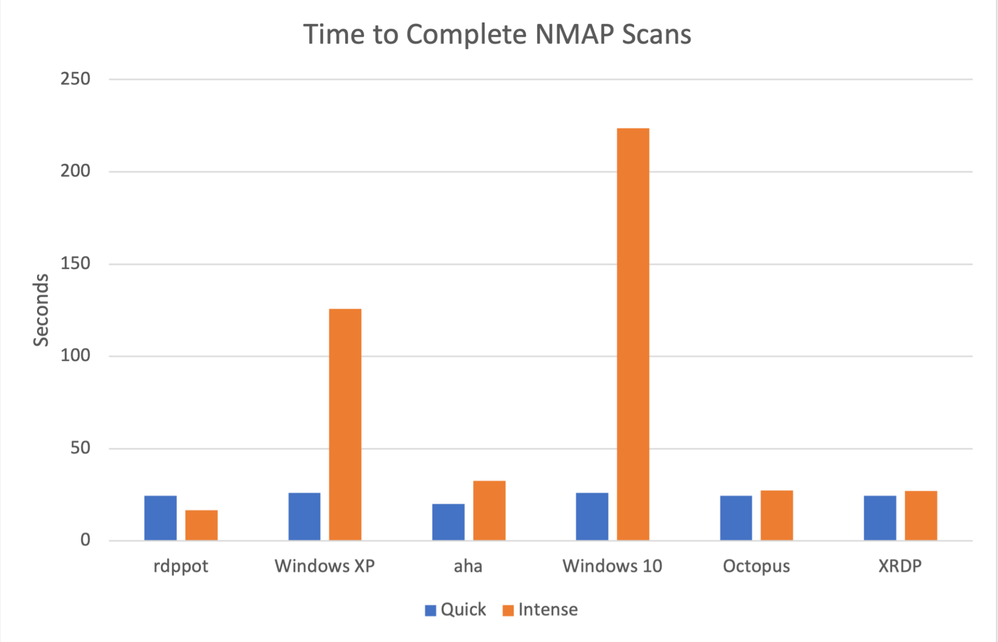
A virtual network was created that hosted three RDP honeypots and three legitimate RDP services. Three types of tests were performed against the services including network fingerprinting (NMAP and Xprobe2), latency testing (ICMP and TCP), and behavioral analysis (file persistence and further attacks).



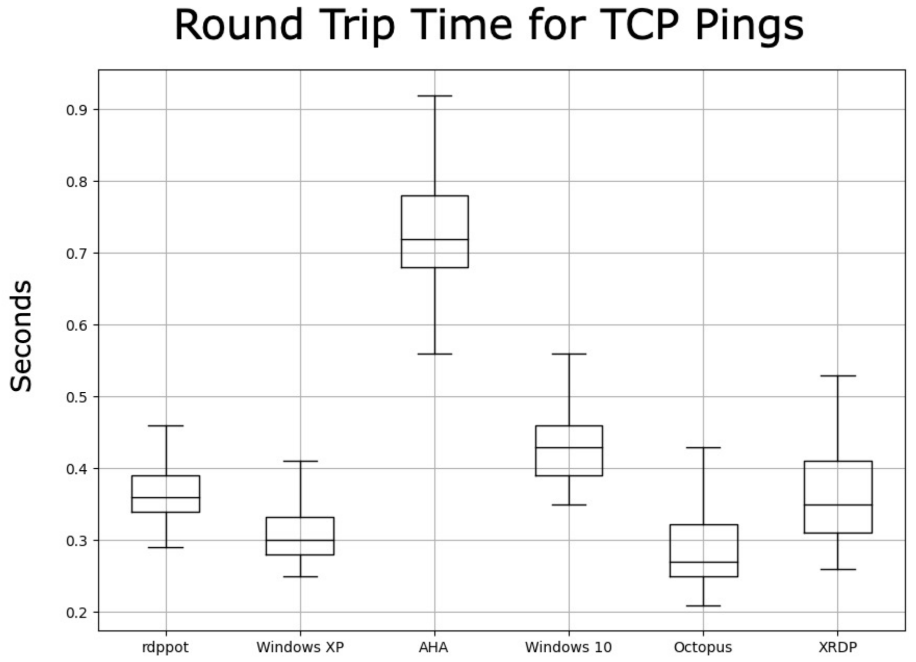
A diagram of the virtual network used for testing, with all eight virtual machines labelled with their role, operating system, and local IP address.

Results

The results found many of the tested techniques to be able to effectively identify honeypots from real services. The first figure shows a much longer time to complete NMAP scans against the legitimate Windows system than their honeypot counterparts. TCP round trip times were also longer for the Windows honeypots, as shown in the box plot.



Time to complete the quick and intense NMAP scan against each service



The stander deviation of the round trip times of TCP pings against each service

Discussion

This research has successfully identified methods for effectively detecting honeypots in a purple team engagement. Techniques like fingerprinting and latency were identified from the literature and were tested in a simulated environment.

Xprobe2 fingerprinting is the most effective in a purple team engagement. The time to complete of intense NMAP scans also proved reliable. These techniques could be further improved by automating them.

RDP honeypots need to have improved operating system spoofing or fuzzing capabilities as this is currently their biggest fault.

References

Boddy, M., Jones, B. & Stockley, M., 2019. RDP Exposed - The Threat That's Already at Your Door, s.l.: Sophos.

Srinivasa, S., Pedersen, J. M. & Vasilomanolakis, E., 2021. Gotta catch 'em all: a Multistage Framework for honeypot fingerprinting. ArTix, Volume 7, pp. 1-26.

Uitto, J., Rauti, S., Lauren, S. & Leppanen, V., 2017. A Survey on Anti-honeypot and Anti-introspection Methods Joni. A Survey on Anti-honeypot and Anti-introspection Methods Joni, Volume 570, pp. 125-134.

Holz, T. & Raynal, F., 2005. Detecting Honeypots and other suspicious enviroments. IEEE, pp. 29-36