

Network Intrusion Detection Proposal

Erin Jamroz University of Puget Sound
1500 N. Alder St.
Tacoma, WA
ejamroz@ups.edu

Jacob Fuhrman University of Puget Sound
1500 N. Alder St.
Tacoma, WA
jfuhrman@ups.edu

ABSTRACT

Keywords

IDS: Intrusion Detection System

IPS: Intrusion Prevention System

1. INTRODUCTION

1.1 Host-Based Audit Systems

1.2 Network-Based Audit Systems

1.3 Application-Based Audit Systems

1.4 Signature Detection

1.5 Anomaly Detection

2. RELATED WORK

2.1 Probes

2.2 Privilege Escalation

Privilege Escalation attacks are described in two general categories in this paper: Remote to User Attacks and User to Root Attacks. In the broadest sense, Remote to User Attacks are when an attacker seeks to gain local user access to a machine that they have network access to. A User to Root Attack, as one may infer from its name, is when an attacker who already possesses local user access seeks to escalate their privileges to those of a root user, IE gain root user access. In the following sections, both types of attacks are explained in detail.

Remote to user attacks

User to root attacks

2.3 Denial of Service

3. METHODS

4. EVALUATION

5. DISCUSSION

6. CONCLUSIONS

7. REFERENCES