Cadre
information security

INTRUSION PREVENTION

IPS, the what, why and how.

Tom Ellis
Senior Security Engineer
Cadre Information Security

INTRODUCTION

- Tom Ellis, Senior Security Engineer
- 4 years with Cadre Information Security
- 25 years of IT experience
- Systems Engineering
- Operations Management
- Project Management
- Security Engineering
- Cadre IPS Subject Matter Expert

WHAT IS IPS?

- Intrusion Prevention Systems are designed to detect and mitigate potential intrusion events in a given system.
- Hacking attacks
- Malware
- Protection from Common Vulnerabilities and Exposures (CVE)
- Provide active protection as opposed to Intrusion Detection Systems (IDS)

WHY USE IPS?

- Protect sensitive data
- PCI compliance
- HIPAA compliance
- Trade secrets
- Customer data
- Hackers are becoming increasingly sophisticated
- Sleep better at night

TYPES OF IPS

- NIPS – Network based IPS. These analyze protocol activity at the network level.
- NBA – Network Behavioral Analysis. These look for unusual traffic patterns and flows. Especially useful for detecting Distributed Denial of Service (DDOS) attacks and certain malware.
- HIPS – Host based IPS. Installed on a single host to monitor for suspicious activity through event analysis on the protected host.
- WIPS – Wireless IPS. Protects Wi-Fi networks.

METHODS USED BY IPS

- Signature based – Matches packets to pre-determined attack patterns, similar to how traditional Anti Virus packages work.
- Stateful Protocol Analysis – Looks for events compared to predetermined activity profiles to determine anomalous protocol activity.
- Statistical anomaly based – Looks at statistical baselines of ‘normal’ network activity on a given network. Generates alerts when significant deviations from normal behavior are detected.

IMPLEMENTING IPS

- Inline – In order to provide active protection, the solution needs to sit inline on important network segments.
- Fail open or fail close? – A choice must be made between failing in a state that leaves the connection open or one that shuts down traffic as a precaution should the device fail.
- Bypass switches – Bypass switches should be considered even with solutions that provide a fail open option. This provides an added layer of redundancy.

IMPLEMENTING IPS

- Examine the network to determine what segments need to be protected. This is often the core but can also include internal segments such as server farms.
- Determine the bandwidth needs. Our use of bandwidth is ever increasing. Proper sizing of an IPS solution helps ensure that the chosen solution will have longevity.
- Determine which product is the best fit. There is no one easy answer to this and due diligence is important.

TUNING IPS

- Many organizations do not properly tune their IPS solutions. Instead it is all too often just a ‘check box’ that they install then cross off the list.
- Tuning can be a very manual and time consuming process.
- Without tuning, false positives can cause legitimate applications to fail while allowing potential attacks to succeed.
- Out of the box settings generally only catch 80-85% of attack events. Tuning can increase that to over 97%.

MAINTAINING THE SYSTEM

- IPS software should be kept up to date.
- Signatures should be updated regularly.
- Logs should be reviewed on a regular basis by security staff. The use of a good SIEM can make this job a lot easier.
- Tuning should be revisited periodically to ensure that the system is providing maximum protection. Ideally this is an ongoing process as updates are applied.

CONCLUSION

- IPS is critical piece of any organization’s security infrastructure.
- A firewall alone is often no longer enough to protect the network and its resources.
- Proper planning and design is required to ensure the proper solution. There is no ‘one size fits all’ answer.
- Proper tuning and maintenance are required to get the most out of the solution.

QUESTIONS

- Any Questions?
- I can be reached at tom.ellis@cadre.net
- Contact your Cadre sales representative
  - Chris Loughner, Enterprise Security Consultant, chris.loughner@cadre.net
  - David Scott, SMB Security Consultant, david.scott@cadre.net