

Alaskan Honeynet Project

Status Report: May 2007

DEPLOYMENTS

Current technologies deployed

The University of Alaska, Fairbanks has initially authorized only four external IP addresses to use for our honeynet, so this limits our ability to deploy a large variety of honeypots. We are currently re-configuring our honeypots for an experiment in the ability of software firewalls to repel attacks in unpatched Windows systems or Windows systems with outdated patches. We then will analyze the vulnerabilities that the attackers use to compromise the honeypots.

We are also investigating the possibility of expanding our deployment to other campuses in the University of Alaska (UA) system. The UA system has three main branches with more than a dozen community campuses. This allows us to expand our nodes and gather more information about the malicious activity across Alaska's large geographic area.

FINDINGS

Highlight any unique findings

As a precursor to our larger experiment, we placed an unpatched Windows XP machine with a software firewall set at maximum security on the internet. Within a day the machine was compromised, and had to be taken down to ensure that future attacks did not stem from that machine. We would like to investigate the validity of the software firewall's ability to evade attack and how our findings relate to the manufacturer's claims.

LESSONS LEARNED

What new positive things can you share with the community, so they can replicate your success?

None at this time.

What new mistakes can you share with the community, so they don't make the same mistakes?

None at this time.

Are there any research ideas you would like to see developed?

None at this time.

TECHNOLOGY

What tools or functionality are we lacking, what do we need to work on?

None identified at this time.

Would you like to integrate this with any other tools, or you looking for help or collaboration with others in testing or developing the tool?

We do have a honeynet-related technology research/development program in an early stage, but do not require assistance with testing or development at this time.

PAPERS AND PRESENTATIONS

Are you working any papers to be published, such as KYE or academic papers?

We have published a research paper on honeypots that describe our research results as well as the future direction that we will be investigating. In addition, we are working on a literature survey that documents some of the published research in Dynamic Honeypots that should provide excellent foundational information for researchers in this area.

Are you looking for any data or people to help with your papers?

We are looking for assistance in the literature review as much of the research in this area has not been published through traditional means. As a result, reviewers and information on where additional information can be found would be beneficial to the research community.

Where did you publish/present honeypot-related material?

Hecker, C, K. Nance and B. Hay. *Dynamic Honeypot Construction*. Proceedings of the 10th Colloquium for Information Systems Security Education. Adelphi, Maryland. June 2006

ORGANIZATIONAL

Changes in the structure of your organization

Since we are a new group, we are trying to raise awareness and recruit new students interested in participating in our research. We have had interest from several students, and expect increased involvement in the next academic year.

Your feedback on Alliance activities

The communication is impressive in this community. Since we are new members, we are trying to take in the atmosphere and the restructuring. With all of the good advice and technical knowledge of the Alliance, this will continue to be an organization with valuable input for the entire community.

Any suggestions for improving the Alliance?

Continuing from the Chicago's status report and the recent communications via email, building a list of the current members, their affiliations, and expertise would allow members to contact individuals with specific expertise to help them on their research.

GOALS

Which of your goals did you meet for the last six months?

We became a probationary member of the Honeynet alliance.

Which of your goals did you not meet for the last six months?

While we have increased awareness of the Honeynet Alliance within the university community, and identified several students who have an interest in becoming involved in our honeynet related projects, we were not able to get students heavily involved during this initial semester. We expect that this goal will be met during the next academic year.

Goals for the next six months

We would like to develop a working relationship with the University of Alaska Office of Information Technology security members. This will allow us to

increase participation in our chapter, possibly use information about malicious activity on the university's network, and/or find new places to deploy our honeynets. Our honeynet knowledge will also help them by alerting them to violators or vulnerabilities to which they were unaware. We plan to complete the literature survey and submit it for publication in a refereed journal.