Project Description Form

MSc Information Security

TO BE COMPLETED BY THE PROJECT CANDIDATE

Name:

Contact email address:

Provisional Title of Project: An investigation into malicious activity on a small network.

1. Statement of Objectives

- Gain practical Information Security experience by building a virtual network to act as a honeypot
- Assess tools that can be used to monitor malicious activity on a honeypot
- Review of the techniques used by attackers to attack a small network
- Investigate a way to conduct an experiment to monitor malicious activity on a small network.
- Investigate whether the patching of operating systems affects malicious activity on networks
- If time permits, to attempt to draw conclusions from the timing of malicious activity. For example to see if it is possible to draw a link between malicious activity and leisure time.
b. **Why have you chosen the proposed project?**

I have chosen the proposed project as I wish to apply the knowledge that gained from the taught part of the course in a practical way.

Before joining the course I had a background in the design and development of websites. I wish to build upon this experience and observe first hand malicious activity on the internet.

I wish to further expand my understanding of potential threats networks face and to expand my analytical skills in the written section of the project.
2. **Methods to be used**

a. How do you intend to achieve the objectives listed above?

I intend to setup a virtual network at home to act as a honeypot to attract attackers and monitor their activities.

I will conduct a brief risk assessment on my current network to look at the potential threats that it could face. After reviewing the findings I will make a decision on the best way of conducting the experiment, for example should the current home network be physically isolated from the honeypot.

I am looking at dividing the project into two main stages:

1. Setup and monitoring of the network. This would come first so that the experiment can run long enough that it gives representative data to work with.
2. Conducting the research part of the project whilst the experiment is running.

**Network setup**

I propose building a virtual network on a single machine using Vmware. Then create a virtual network containing several operating systems patched to differing degrees. The idea being that a potential attacker would try to exploit vulnerabilities and the honeypot would monitor his activities.

After establishing the network I will look into ways of monitoring for malicious activity before it is connected to the internet. I am looking at the open source products Honeyd and HoneyWall to help in the monitoring of activity.

Once the monitoring system is in place I will attach the network to the Internet and then regularly monitor the system for malicious activity.

**Investigation into Patching and malicious network activity**

I intent to research current and historically malicious activity, see what effects patching has on attacks and look to review recommendations for when and why to patch. These are some of the sources of information I will use:

- Information released from Antivirus vendors
- University Library and the British Library
- Internet searches
- Guidelines from software vendors
- Previous research that has been conducted the effectiveness of patching

I will then use the information collected from my research and useful data from the honeypot to draw any possible conclusions for the project.
b. What is your strategy for getting started?

Setup network

I have decided to physically isolate the experiment from the rest of my home network by installing a second ADSL line. Firstly I will design the network with several virtual machines, running different operating systems and patched to different levels. The network will include several services, for example a HTTP and FTP server. I will introduce some “dummy” information into the network, which will include some several websites that I have previously designed and built.

The machine that I will be using initially is a Pentium 4 with 512Mb of RAM which I am planning to upgrade depending on the performance of the network.

Monitoring tools

I have discovered that honeypots are divided into two main categories low and high interaction. After researching ways to monitor these classes of honeypot I have discovered they following tools:

An example of a low interaction honeypot

As a low interaction honeypot this solution is designed to emulate services that an attacker can interact with for example HTTP. The benefits of this class of honeypot is that they are designed to be straight forward to setup and have the ability to limit the scope of an attack, by only providing certain services for the attacker to interact with. The drawback is that as it emulates services it is limited to monitoring known vulnerabilities.

Honeyynet [http://www.honeynet.org/index.html](http://www.honeynet.org/index.html)
An example of a high interaction honeypot

This class of honeypot is uses a “real” network that doesn’t restrict how the attacker can interact with it. The drawback is that there is a higher level of risk associated with it as the attacker may perform unexpected operations.

Review of techniques

I am currently collecting information on current trends in malicious activity from sources such as antivirus vendors and Information Security related websites.

I will continue this investigation with literature searches investigating threat trends to networks such as the one in the experiment.
Effect of patching

I will investigate the reasons for patching and the effects that patching has on malicious activity. I aim to look historically at when patches have been developed and the vulnerabilities they have addressed by looking at recommendations of software vendors and the types of malicious activity being reported at that time.

Further any useful data from the experiment will be used to see the effect that the patching had on the sample systems in the experiment.

Attack timing

In the course of developing this project plan I read an article that attempts to suggest the best times for the delivery of patches. If time permits I will endeavour to use this article as a starting point for investigating whether there is a relationship between the time of attacks and when patches are released.
Project Description Form

MSc Information Security

TO BE COMPLETED BY THE PROJECT CANDIDATE

Name:

Contact email address:

Provisional Title of Project: An investigation into malicious activity on a small network.

1. Statement of Objectives

- Gain practical Information Security experience by building a virtual network to act as a honeypot
- Assess tools that can be used to monitor malicious activity on a honeypot
- Review of the techniques used by attackers to attack a small network
- Investigate a way to conduct an experiment to monitor malicious activity on a small network.
- Investigate whether the patching of operating systems affects malicious activity on networks
- If time permits, to attempt to draw conclusions from the timing of malicious activity. For example to see if it is possible to draw a link between malicious activity and leisure time.
b. Why have you chosen the proposed project?

I have chosen the proposed project as I wish to apply the knowledge that gained from the taught part of the course in a practical way.

Before joining the course I had a background in the design and development of websites. I wish to build upon this experience and observe first hand malicious activity on the internet.

I wish to further expand my understanding of potential threats networks face and to expand my analytical skills in the written section of the project.
2. Methods to be used

a. How do you intend to achieve the objectives listed above?

I intend to setup a virtual network at home to act as a honeypot to attract attackers and monitor their activities.

I will conduct a brief risk assessment on my current network to look at the potential threats that it could face. After reviewing the findings I will make a decision on the best way of conducting the experiment, for example should the current home network be physically isolated from the honeypot.

I am looking at dividing the project into two main stages:

1. Setup and monitoring of the network. This would come first so that the experiment can run long enough that it gives representative data to work with.
2. Conducting the research part of the project whilst the experiment is running.

Network setup

I propose building a virtual network on a single machine using Vmware. Then create a virtual network containing several operating systems patched to differing degrees. The idea being that a potential attacker would try to exploit vulnerabilities and the honeypot would monitor his activities.

After establishing the network I will look into ways of monitoring for malicious activity before it is connected to the internet. I am looking at the open source products Honeyd and HoneyWall to help in the monitoring of activity.

Once the monitoring system is in place I will attach the network to the Internet and then regularly monitor the system for malicious activity.

Investigation into Patching and malicious network activity

I intent to research current and historically malicious activity, see what effects patching has on attacks and look to review recommendations for when and why to patch. These are some of the sources of information I will use:

- Information released from Antivirus vendors
- University Library and the British Library
- Internet searches
- Guidelines from software vendors
- Previous research that has been conducted the effectiveness of patching

I will then use the information collected from my research and useful data from the honeypot to draw any possible conclusions for the project.
b. What is your strategy for getting started?

Setup network

I have decided to physically isolate the experiment from the rest of my home network by installing a second ADSL line. Firstly I will design the network with several virtual machines, running different operating systems and patched to different levels. The network will include several services, for example a HTTP and FTP server. I will introduce some “dummy” information into the network, which will include some several websites that I have previously designed and built.

The machine that I will be using initially is a Pentium 4 with 512Mb of RAM which I am planning to upgrade depending on the performance of the network.

Monitoring tools

I have discovered that honeypots are divided into two main categories low and high interaction. After researching ways to monitor these classes of honeypot I have discovered they following tools:

Honeyd http://www.honeyd.org/
An example of a low interaction honeypot

As a low interaction honeypot this solution is designed to emulate services that an attacker can interact with for example HTTP. The benefits of this class of honeypot is that they are designed to be straight forward to setup and have the ability to limit the scope of an attack, by only providing certain services for the attacker to interact with. The drawback is that as it emulates services it is limited to monitoring known vulnerabilities.

Honeyynet http://www.honeynet.org/index.html
An example of a high interaction honeypot

This class of honeypot is uses a “real” network that doesn’t restrict how the attacker can interact with it. The drawback is that there is a higher level of risk associated with it as the attacker may perform unexpected operations.

Review of techniques

I am currently collecting information on current trends in malicious activity from sources such as antivirus vendors and Information Security related websites.

I will continue this investigation with literature searches investigating threat trends to networks such as the one in the experiment.
Effect of patching

I will investigate the reasons for patching and the effects that patching has on malicious activity. I aim to look historically at when patches have been developed and the vulnerabilities they have addressed by looking at recommendations of software vendors and the types of malicious activity being reported at that time.

Further any useful data from the experiment will be used to see the effect that the patching had on the sample systems in the experiment.

Attack timing

In the course of developing this project plan I read an article that attempts to suggest the best times for the delivery of patches. If time permits I will endeavour to use this article as a starting point for investigating whether there is a relationship between the time of attacks and when patches are released.
4. Additional comments

Use this section to make extra comments on the proposal on matters not covered above (use extra space if necessary). Include details of any involvement of external organizations.

Experiment results

I am unsure of the quality of the results that I may get from the experiment. From my current understanding the likelihood of observing malicious activity in the experiment is high. I am also aware that as the activity is malicious it could potentially destroy any useful data that I might otherwise have collected.

TO BE COMPLETED BY THE PROJECT SUPERVISOR

I approve the attached project plan.

Signed:

Name:

Date: