UNIVERSITY OF PORTSMOUTH

ALERTS FROM UNUSUAL ACTIVITY

February 2016

Contents

Document title		
Normal text		
Document author and department		
Normal text		
Approving body		
Normal text		
Date of approval		
Normal text		
Review date		
Normal text		
Edition no.		
Normal text		
ID Code		
Normal text		
Date of effect		
Normal text		
EITHER For public access online (internet)? *Tick as appropriate*		**YES**
For public access on request copy to be mailed *Tick as appropriate*	**NO**	**YES**
OR For staff access only (intranet)? *Tick as appropriate*		**YES**
Password protected *Tick as appropriate*	**NO**	**YES**
External queries relating to the document to be referred in the first instance to the Corporate Governance team: email corporate-governance@port.ac.uk		

If you need this document in an alternative format, please email corporate.communications@port.ac.uk

The latest version of this document is always to be found at:

https://erecords.port.ac.uk/documents/qA43279

Summary

What is this document about?

Legitimate research can generate security alerts which indicate that “unusual network activity” is taking place. This advisory suggests a mechanism by which certain forms of cyber research activity can be performed with minimal interruption or concern to internal and external security groups.

Who is this for?

Both IS staff and researchers.

How does the University check this is followed?

Compliance is not required.

Who can you contact if you have any queries about this document?

Any questions about should be directed to servicedesk@port.ac.uk

1.0 Introduction

Security alerts and warnings often result from legitimate academic research which produces "unusual network activity". For example, research into malware or penetration testing may probe many sites on the Internet, and may trigger security alarm bells in certain circumstances and even breach legislation if not properly managed. The time and resources spent responding to legitimate but unusual activity could be more effectively spent elsewhere.

2.0 What activity might fall under 'Unusual Activity'?

The scope of what constitutes "unusual network activity" is difficult to define but could include one or more of the following :-

- Performing traditional network scanning - such as *nmap*.
- Performing abnormal application-specific probes against many targets - such as performing an SSL negotiation and then immediately quitting.
- Sending any application data that could be defined as non-standard
- Attempting to exceed application limits (such as filling in a web-based form with a name longer than 8Kbytes).

If in doubt whether your intended activity qualifies, please contact servicedesk@port.ac.uk for advice.

3.0 The Intention

This advisory describes the steps needed to give prior warning to Information Services, to inform them that the activity is research related and not intentionally malicious.

4.0 The Steps

The following steps are advised:-

1. Request IS configure a static network address for the workstation used to send the research probes. IS will need
    a. the MAC address of the workstation,
    b. a suggested name for the DNS registration which should be a helpful indication that research is taking place (e.g. *tor-research.static.port.ac.uk*), and
    c. a "Responsible Person" to contact in case of difficulties.
2. Set up a web page explaining what the research is.
3. Set up a web form allowing organisations to request that their network range is excluded (and of course implement an exclusion list!).
4. Request IS register a DNS TXT record containing the relevant web address.

5.0 Who to contact

If you have any questions or you are concerned that your research activity might trigger a security alert, please make contact with members of the IS Networks and Security Services group by calling the IS Service Desk on ext 7777.

University of Portsmouth
Department of Human Resources
University House
Winston Churchill Avenue
Portsmouth PO1 2UP
United Kingdom

T: +44 (0)23 9284 3141
F: +44 (0)23 9284 3122
E: university.secretary@port.ac.uk
W: www.port.ac.uk