The problem of mass unauthorized security scans/tests

Presenter: Rich Kulawiec, Fire on the Mountain (remote)

Contact: rsk@firemountain.net

Introduction:

An increasing number of operations are conducting mass security scanning/testing of as many systems as they can. This trips alarms, fills logs, consumes human time, is being done without permission, builds datasets that are highly useful to attackers who can't build their own, and won't scale.

Goal:

Discussion. Do we concur that this is a problem, and if so, do we think it's a problem we can/should address, and if so, then what can we do (RFC? BCP?) to address it? I suggest a temporary mailing list to ask/answer these questions.

The problem of mass unauthorized security scans/tests

Notes:

1. I estimate 30+ such operations so far but I'm probably undercounting. I've observed ~4000 (IPv4) originating addresses, also likely an undercount.

2. These aren't the preludes to attacks, they ARE attacks. These are active probes of services (e.g., SSH, IMAP), not passive data gathering.

3. Dealing with these attacks costs time/money/effort on the part of the targets. Note that identifying and blocking these is at best onerous, reactive, and only partially effective.

4. Some operations have gone to considerable lengths to obfuscate their identities and activities, e.g., frequently shifting origination points.

5. Aggregating this kind of data builds a valuable target. (Other) attackers will want it, and they'll get it. This makes the entire Internet *less* safe.

The problem of mass unauthorized security scans/tests

Notes, continued:

6. They're not (all) researchers. Consider:

- Have they fully identified themselves, the purpose of the research, its goals, its methods, its scope, etc.?
- Have they put their research proposal in front of an IRB?
- Did they get the informed consent of the subjects of their research before commencing?
- Did they provide the results of tests to the subjects?
- Have they published?

The problem of mass unauthorized security scans/tests

So, looping back to the beginning:

- Do we concur that this is a problem?
- If so, do we think it's a problem we can/should address?
- If so, then what can we do (RFC? BCP?) to address it?

I suggest a temporary mailing list to ask/answer these questions.

Thanks, and comments/questions/etc. to: Rich Kulawiec, rsk@firemountain.net.