

CSIRT-MU

Jan Vykopal

Head of CSIRT-MU

Masaryk university

Brno, Czech Republic



TF-CSIRT meeting – 25/09/2009, National Library of Estonia, Tallinn

Our constituency: Masaryk University

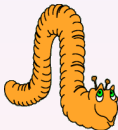
- tens of thousands of university students
- thousands of staff in 9 faculties and 3 institutes.

We are constituency of CESNET-CERTS (CSIRT of Czech NREN).

Who are we?

- Young team (< 1 year old).
- Manpower: 2 FTEs (including research projects).
- **Listed** by Trusted Introducer in June 2009.

- **Incident handling**
- **Intrusion detection**
- **Alerts & warnings**
- (Penetration testing)



Prevention is better than cure.

- Provided in business hours, best effort service.
- Communication with departments and faculties.
Need for a directive.
- Struggling with request trackers (OTRS, RT, RTIR...).
- Supported by **network flow monitoring** (several NetFlow probes in operation).

- About 10 incidents per week from outside.
- Majority of copyright issues.

Intrusion detection

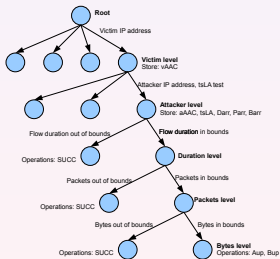
- Based on NetFlow monitoring: FlowMon probes + NfSen/nfdump.
- Specialized **scripts periodically process NetFlow** data.
- TCP port scanning probes detection, honeypot monitoring, spammers detection.

- Port scanning detection + Conficker spreading = 100 alerts in April and May 2009.
- New previously **unknown viruses found**.
- School term is just starting! :-)

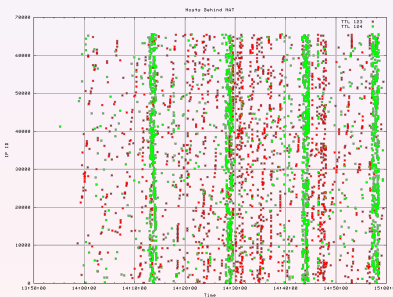
- Monthly issued **security bulletin** (summary + vulnerabilities).
- **Immediate announcements** of critical up-to-date updates and vulnerabilities.
- About 30 subscribers at Masaryk university.
- Short survey after first four bulletins:
I would recommend this bulletin to my colleague. (88 %)

Our research – for Czech Army

- Aimed at threats from inside the network.
- Development of detection methods for high-speed networks.
- SSH dictionary attack detection.
- Network Address Translation (NAT) detection.
- End host profiling.
- Cisco MARS and Enterasys DSCC testing.



Adaptive decision tree of SSH dictionary attack detection.



How many hosts are behind NAT?

Motivation

- Many heterogeneous data sources from NetFlow probes, honeypots, servers (syslog), blacklists. . .
- Manual event correlation is very demanding.

Implementation

- Maximal utilization of existing tools (not reinvent the wheel).
- Only one communication protocol: widely supported Syslog.
- Need to implement core (incl. anomaly detection module) and Syslog „adapters“ for existing tools.

Our TODO list

- Deployment of *the right one* request tracker + training.
- Improved searching in NetFlow data.
- Internal directive for administrators at university.
- NetFlow probes penetration.
- Extension of our detection scripts + NfSen plugins.

Thanks for your attention. Questions?



Jan Vykopal
vykopal@ics.muni.cz

Masaryk university

CSIRT-MU

