janet

Janet CSIRT - Securing the Janet Network and Supporting Customers

Lee Harrigan

Overview

janet

- About CSIRT and our role
- An overview of the Incidents we see
- Some examples of incidents
- What can you do to help yourself
- Janet ESSIS
- If you have any questions please just interrupt me.

The Team

janet

1 Manager

- Wally Jackson

7 CSIRT Members

- James Davis
- James McLoughlin
- Lee Harrigan
- John Green
- Antoni Fertner
- Mark Siddle
- James Cleeter

What is a CSIRT?

janet

- CSIRT (Computer Security Incident Response Team)
- CERT© or CERT-CC (Computer Emergency Response Team / Coordination Centre)
- IRT (Incident Response Team)
- CIRT (Computer Incident Response Team)
- SERT (Security Emergency Response Team)

As you can see names can vary, but they all mean the same essentially.

Coordinate with our community and other CERTs, ISPs

Provide advice, and assistance in relation to security with confidentiality

What do we do?

janet

- Incident Response
  - Incident coordination
  - Vulnerability Reporting
  - Enforcing the AUP/Security Policy
  - Blocking Things
- Proactive Monitoring
  - Netflow based anomaly / malware detection
  - Post-incident analysis
  - Open source / social media intelligence gathering
  - Development of tools
- Advice and Expertise
  - Specialist systems knowledge
  - Advice and hands off assistance
  - Technical security leadership
  - Keeping up to date with security news

What we don't do!

janet

- We don't hack systems,
- We don't probe systems looking for vulnerabilities to advise the owners.
- We are not the internet Police
- We don't pass information onto the Government / CIA ..... But we do work with them.

How do we detect security incidents

janet

- Netflow Data
- Email's / Alerts from 3rd parties
- Website monitoring
- Telephone calls
- Keeping up to date with the security landscape / vulnerabilities
- Google Searches
- Post Incident analysis

Types of issues we deal with

janet

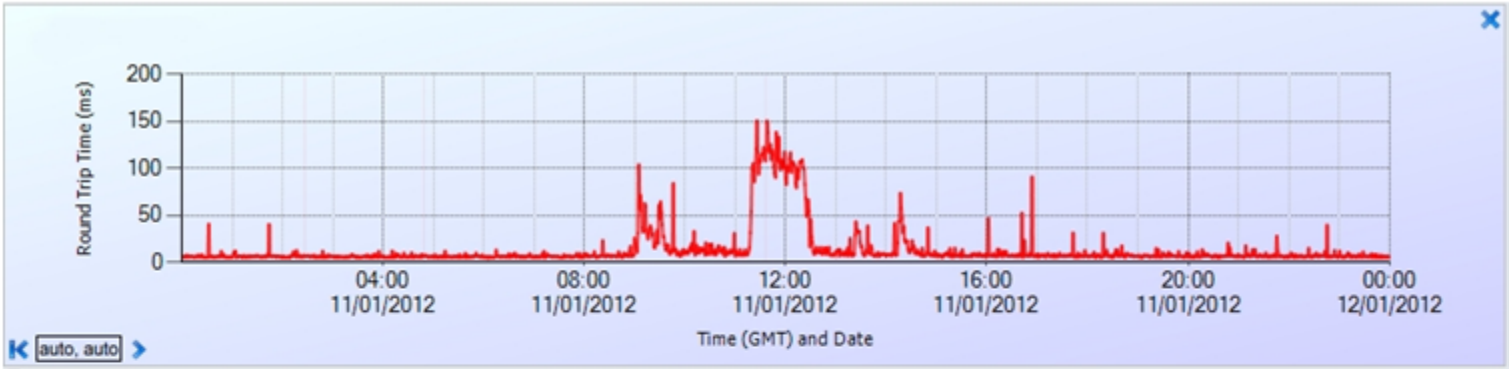
- Compromise
  - Data, usernames, passwords, personal information
  - Systems
- Copyright notices
- Denial of Service
- Queries
  - Law enforcement agencies requests for information (RIPA)
  - Legal / Policy advice
  - Networking / Security advice
- Malware
- Phishing
- Scanning
- Social Engineering
- Unauthorised Use
- Unsolicited Bulk Email (SPAM)

Incident numbers for 2012 /13 /14

Incident Type	2012	2013	2014 To Date
Compromise	1487	1329	276
Copyright	2000	91 (1293)	19 (1909)
Denial of Service	43	127	293
General Query	59	82	89
LEA Query	46	29	20
Legal / Policy Query	7	9	4
Malware	3209	5148	2614
Net / Security Query	115	89	130
Other	114	196	594
Phishing	243	427	206
Scanning	578	380	58
Social Engineering	16	6	1
Unauthorised Use	39	42	16
Unsolicited Bulk Email	238	256	79
Total	**8194**	**8212 (9505)**	**4405 (6314)**

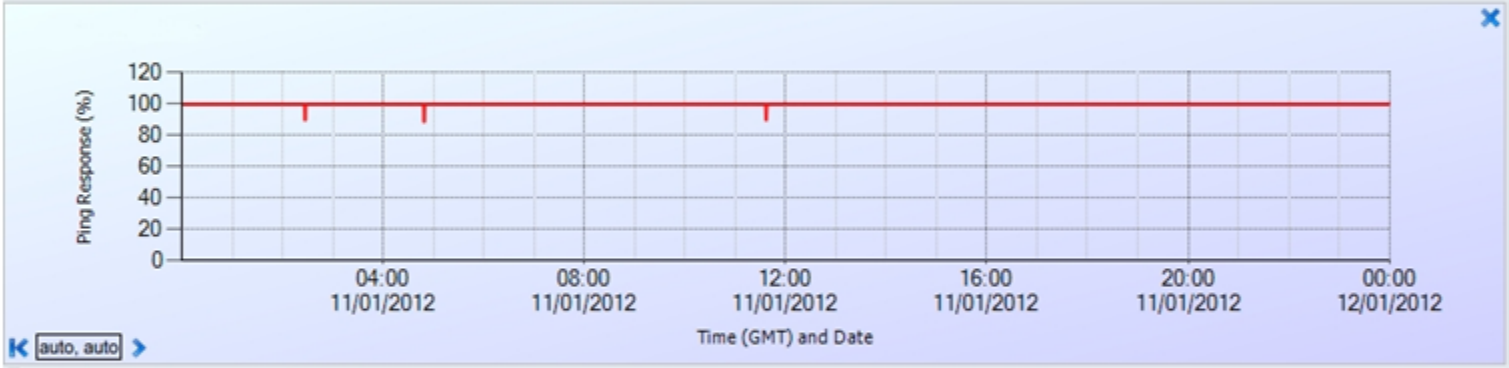
Denial of Service I

janet



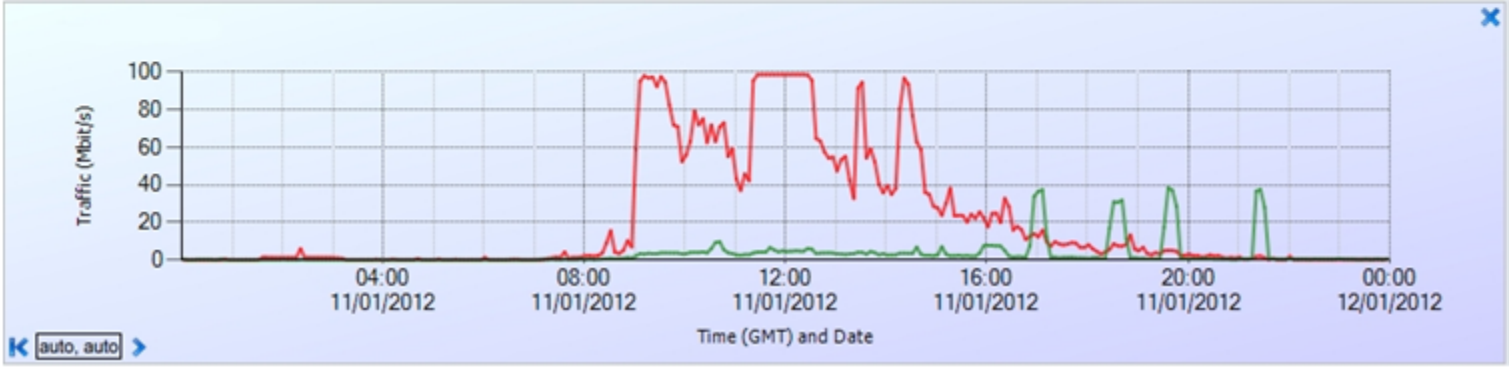
Round Trip Time

Mean	13.9ms
Max	151ms
Min	4.5ms
Last	5.9ms



Ping Response

Mean	100%
Max	100%
Min	88.9%
Last	100%

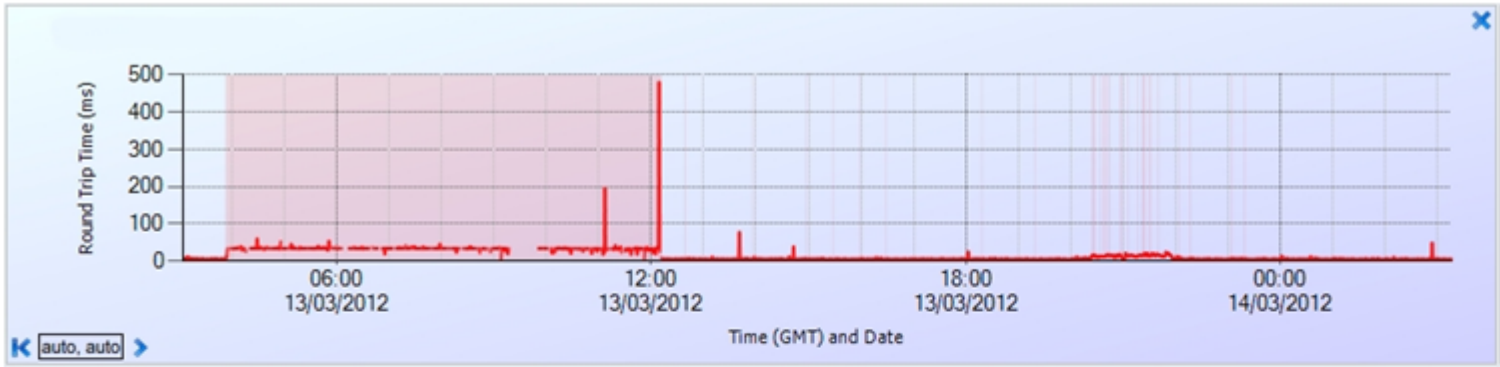


Bandwidth Throughput

	To Site	From Site
Mean	21Mbit/s	3.21Mbit/s
Max	98.6Mbit/s	38.4Mbit/s
Min	34.8Kbit/s	23.7Kbit/s
Last	290Kbit/s	485Kbit/s

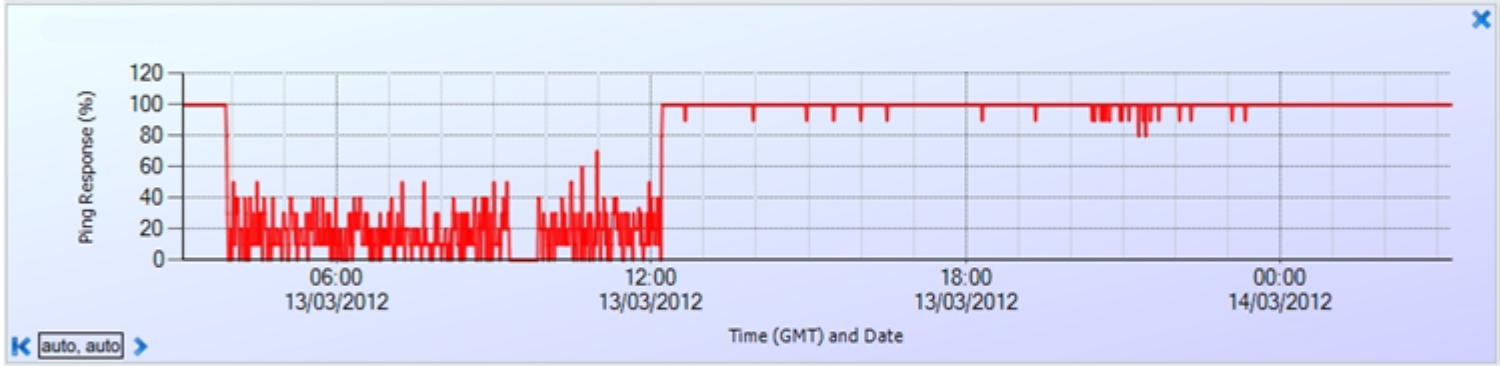
Denial of Service 2

janet



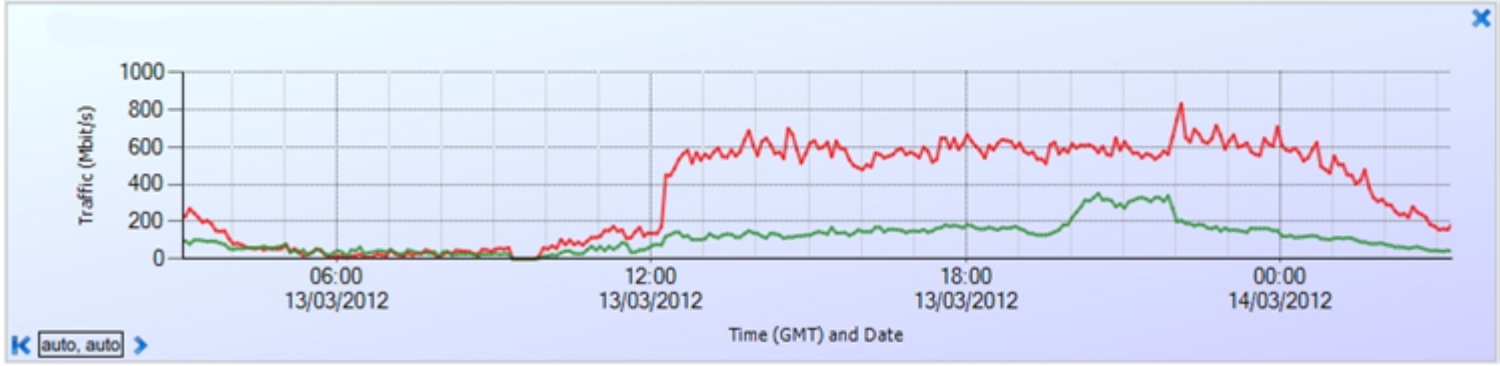
Round Trip Time

Mean	15ms
Max	480ms
Min	4.6ms
Last	6ms



Ping Response

Mean	71.1%
Max	100%
Min	0%
Last	100%

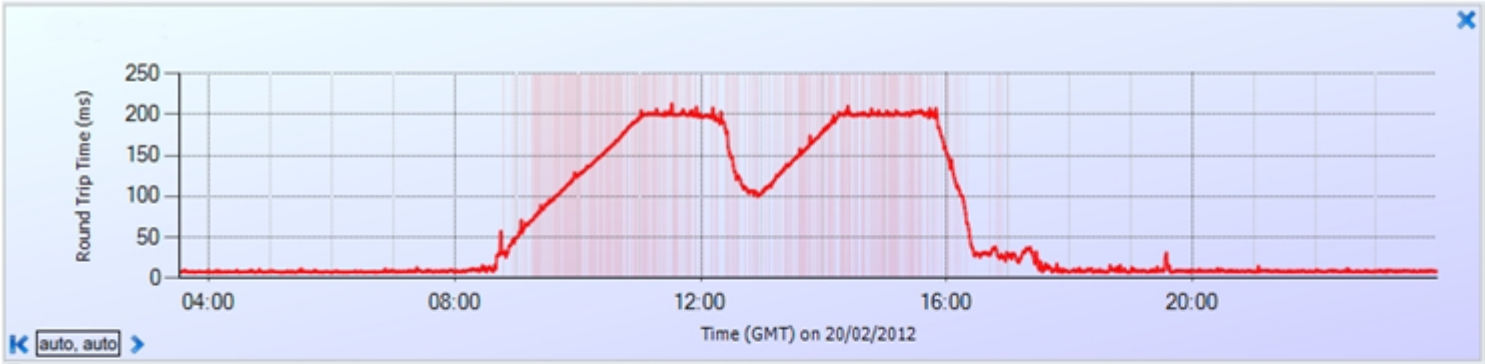


Bandwidth Throughput

	To Site	From Site
Mean	366Mbit/s	114Mbit/s
Max	834Mbit/s	352Mbit/s
Min	240bit/s	0bit/s
Last	158Mbit/s	46.3Mbit/s

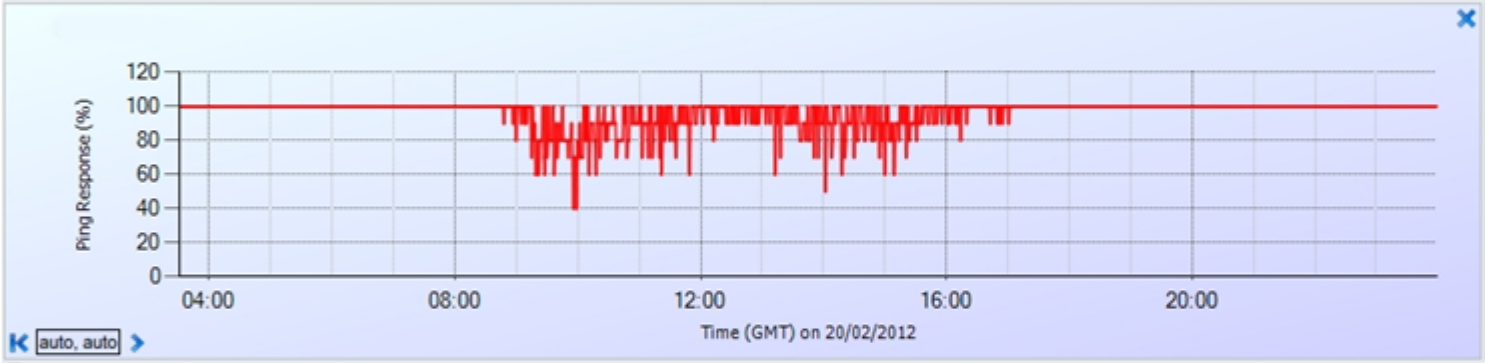
Denial of Service 3

janet



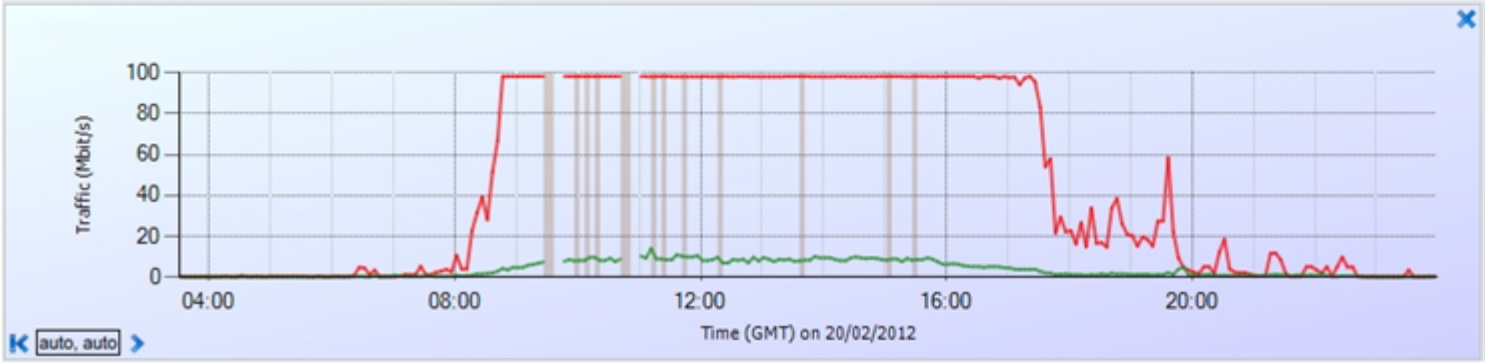
Round Trip Time

Mean	64.8ms
Max	213ms
Min	6.8ms
Last	8.3ms



Ping Response

Mean	96.4%
Max	100%
Min	40%
Last	100%



Bandwidth Throughput

	To Site	From Site
Mean	45.7Mbit/s	3.66Mbit/s
Max	98.4Mbit/s	14.1Mbit/s
Min	123Kbit/s	81.2Kbit/s
Last	201Kbit/s	202Kbit/s

RIPA Notifications

NOTICE UNDER SECTION 22(4) OF THE REGULATION OF INVESTIGATORY POWERS ACT 2000

Where it appears to the designated person that a CSP is or may be in possession of, or be capable of obtaining, any communications data, the designated person may, by notice require the CSP -
(a) if the CSP is not already in possession of the data, to obtain the data; and
(b) in any case, to disclose all of the data in his possession or subsequently obtained by him.
S. 22(6) - It is the duty of the CSP to comply with any notice given to him under subsection (4).

Unique reference number of Notice	[redacted]
CSP	JA.NET - JANET or JANET(UK)
CSP address	JANET Service Desk, JANET(UK), Lumen House, Library Avenue, Harwell Science and Innovation Campus, Didcot, Oxfordshire, OX11 0SG,
CSP contact	
Legislation	This data is necessary for one or more of the following purposes as specified in 'The Regulation of Investigatory Powers Act 2000': • For the prevention and detection of crime or preventing disorder S22 (2)(b)
DCG grade	3
Designated person and date and time of issue	[redacted]
Telephone number/other communication to which this Notice relates	[redacted]
Details of service/data required including dates	[redacted]
SPOC Office Contact Details and Address	[redacted]
Telephone No	[redacted]
Fax No	[redacted]
SPOC e-mail	[redacted]
SPOC Postal Address	[redacted]
SPOC Officer	[redacted]
SPOC Officer Telephone No	[redacted]
Date served	[redacted]

CSPs must ensure the data is returned to a verified SPoC address, email or fax number. For information about how a CSP may verify the identity of a SPoC by use of the SPoC PIN list, contact commsdata@homeoffice.gsi.gov.uk

RESTRICTED

- Regulation of Investigatory Powers Act 2000
- Graded 1 (critical), 2, or 3
- Must originate from a SPoC
- CSIRT can verify a SPoC exists in Home Office database

Recent activities with the NCA

janet

Gameover Zeus (Zeus-p2p) & Cryptolocker

- Advanced warning of the botnet takedown.
- Worked with the NCA & FBI to establish the best course of action from a UK perspective.
- Distributed the list of known domains associated with the malware.
- Issued advice and guidance to affected customers on the global day of action.
- Taken positive action within our resolver service so that our customers are protected from this malware.

- More in the pipeline.....

Example of a Online website hacked

janet

- A small website online was vulnerable to a SQLi attack and contents were put onto pastebin.
- Details of usernames, passwords, and email addresses were dumped.
- Automated email received at 23:15.
- By 9:30 the following morning we had sent notifications to 42 different sites about the breach.
- We also alerted the site that was hacked, they were not aware and took the site offline and also notified all users in their database about the breach.

Example of a Moodle System Hack

janet

- Content of usernames and hashed passwords were put on pastebin approx 3500 unique hashes.
- Investigation started at 08:50 the following day
- A Janet connected organisation system was compromised due to running a old version of phpMyAdmin on a production Moodle server.
- 48% of the passwords were cracked using a small rainbow table (lowercase alpha numeric 1-8)
- Site advised of the very weak passwords.
- They rebuilt system with salted hashing, minimum password requirements and without phpMyAdmin.
- A student at the site was responsible

What can you do to keep yourself safe?

By following best practices you can keep yourself safe.

- Logging is the most important of these.
  - Firewall Logs
  - Proxy Logs
  - DHCP logs
  - Email logs
  - Web Server logs
- Use syslog to keep them in one easy location
- Keep systems up to date with latest patches and security updates.
- Maintain up to date security contacts with Janet CSIRT

Finally

- Contact us if you have any security related questions or queries.
- Effective Identification and Management of Security Incidents Course £200 + VAT for Primary connected Organisations
  13th August in Birmingham or 11th December in London

Janet ESISS

janet

- Recently we acquired ESISS to provide further security services under Janet
- Since the 1st of August 2013 Janet CSIRT acquired 1.5 members of staff from Loughborough University under the ESISS branch.
- It is accredited under TigerScheme which is the UK equlivant to CREST and all ESISS members are accredited under the scheme.
- ESISS has been designed to offer security services to the education sector and as such the services we provide are tailored to your needs.

Accredited Penetration Testing

janet

- Human testing at designated targets specified by you and can be either on-site or remote via a member of the accredited Janet ESISS Team.
- You can stipulate how the day is spent and how testing is conducted. Such as testing a single application or testing an entire range of services / address space.
- Daily rate of £650
- Basic test from £1300 over 2 days (2nd day writing of report)
- An automated Penetration Test / Scanner is also available

Automated Testing

janet

Automated Penetration Testing

- Online web based delivery with our fully accredited partner:
  - 1-3 URL's and upto 60 IP's £2500/year +VAT
  - 4-10 URL's and upto 200 IP's £3500/year +VAT
  - 11-20 URL's and upto 1,000 IP's £5000/year +VAT
  - 21-50 URL's and upto 5,000 IP's £7000/year +VAT
  - 51-1000 URL's and upto 10,000 IP's £8500/year +VAT
  - Unlimited URL's and Unlimited IP's £10000/year +VAT

+ 256 IPs	£300.00
+ 512 IPs	£500.00
+ 1024 IPs	£750.00
+ 2048 IPs	£1,000.00

You can run as many tests as you like against the URL's / IP's you stipulate. You can increase the number of IP's by the amounts above.

Consultancy

janet

- We also offer competitive consultancy rates where Janet staff can be requested alongside ESISS staff providing a greater range of experts on hand.

- For further information on Janet ESISS services contact info@esiss.ac.uk or contact your customer engagement manager.

janet

THANK YOU

Janet, Lumen House
Library Avenue, Harwell Oxford
Didcot, Oxfordshire
Telephone: 0300 999 2340
email: irt@csirt.ja.net
Twitter: @janetcsirt