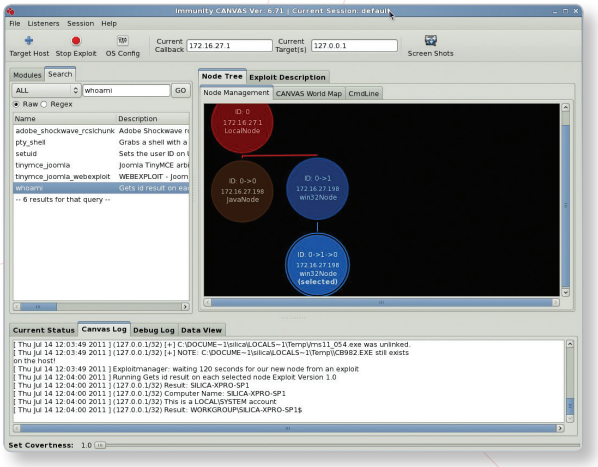
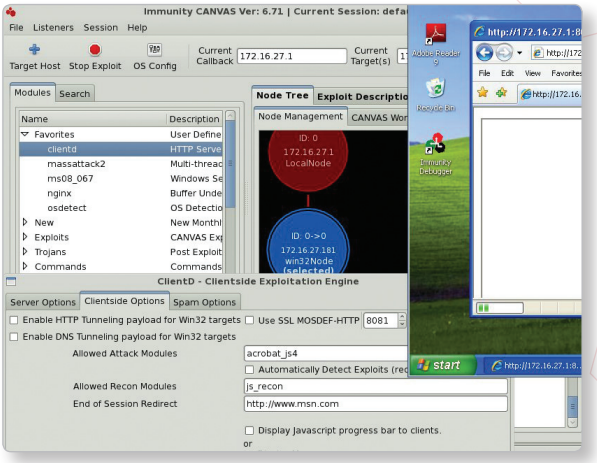
CANVAS

CANVAS is a trusted security assessment tool that allows penetration testing and hostile attack simulations by security professionals. Our multitude of customers currently take advantage of **CANVAS** to properly understand exposure and manage risk. Recognized as a best of breed attack framework, **CANVAS** takes managed computer and network exploitation to the next level. After using **CANVAS** to successfully compromise systems, users can grab screenshots, download password credentials, manipulate the target file system, and elevate privileges. More advanced users can stealthily bounce between target systems and target whole geographic regions.





- **CANVAS** offers a level of exploit quality, availability and real-world use unparalleled by any of our competitors. As such, more **CANVAS** exploits are viewed in the wild than those any of other penetration testing product in today's market.
- Our standard single-installation **CANVAS** package offers:
  - Over 500 current and functional exploits to allow our customers a heightened advantage when seeking out vulnerabilities.
  - Kernel Rootkit for longterm access to your target machine for maximized results.
  - Thunderbird and other advanced backdoors that begin to illustrate the variety that we account for when offering **CANVAS** as a solution.
  - As a small business, Immunity's **CANVAS** development team continues to remain accessible to our customers. The development team is always available to answer questions or provide demos that illustrate the newest features and functionalities that **CANVAS** has to offer.
- In addition to the 500+ exploits available with the basic **CANVAS** platform, our customers have the option of purchasing any or all of the following specialized 3rd party exploit packs:
  - DSquare – D2
  - Enable – VoIPPack
  - Gleg – Agora
  - Gleg – SCADA+
  - IntevyDis – VulnDisco
  - White Phosphorus
- Immunity's recently added Virtual **CANVAS** Training class is a convenient way for our customers to ensure that they are getting the most out of their **CANVAS** usage without having to leave their home or office. The two-day online class is held monthly with flexible scheduling and is taught by the experts themselves – the **CANVAS** research team.
- **CANVAS** Early Updates is another update option that was designed for our customers who need cutting-edge research. With Early Updates, the user is allowed access to up-to-the-minute vulnerabilities and research as it is produced.

CONSULTING SERVICES

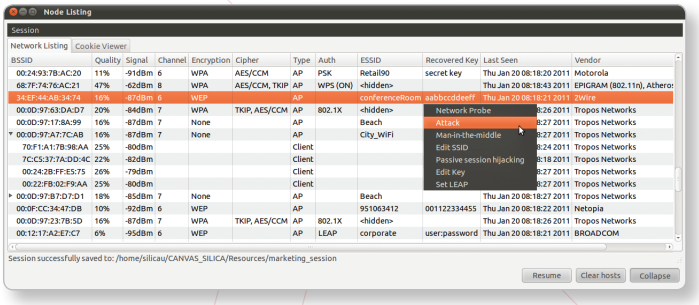
Immunity's team always employs the perspective and philosophy of an attacker. This provides the client with a realistic picture of their level of exposure and an ability to adequately measure the risk associated with technology deployments.

IMMUNITY DEBUGGER

- Immunity offers several high-level specialized attack and assessment services including:
  - Penetration Testing
  - Application Assessments
  - Vulnerability Analysis
  - Reverse Engineering
  - Architecture Review
  - Source Code Review
- Our consultants are world-renowned researchers in the field of Information Security and are highly respected among their peers.
- We specialize in real exploitation in order to fully illustrate true risks to our customers.
- Our wide-range of customers include global enterprise, educational institutions and major financial institutions.

SILICA

SILICA defines the state of the art in wireless attack and security assessment. These portable units allow security professionals to perform wireless network security penetration tests while behaving innocuously.



- Recover WEP, WPA1, 2 and LEAP keys.
- Passively hijack web application sessions for e-mail, social networking and Intranet sites.
- Map a wireless network and identify its relationships with associated clients and other access points.
- Identify vendors, hidden SSIDs and equipment passively.
- Scan and break into hosts on the network using integrated **CANVAS** exploit modules and commands to recover screenshots, password hashes and other sensitive information.
- Perform man in the middle attacks to find valuable information exchanged between hosts.
- It is shipped as VMWare ready VM and USB Wireless and is OSX, Linux and Windows supported.