RSAConference2018
San Francisco | April 16–20 | Moscone Center

SESSION ID: TV-R04

BREAKING AND ENTERING: HOW AND WHY DHS CONDUCTS PENETRATION TESTS

Robert Karas

National Cybersecurity Assessments and Technical Services (NCATS)

Penetration Tests

- Act as Adversary
- Common Paths to Success
  - Phishing – Click rate 12%
  - Credentials
    - Default
    - Re-Used

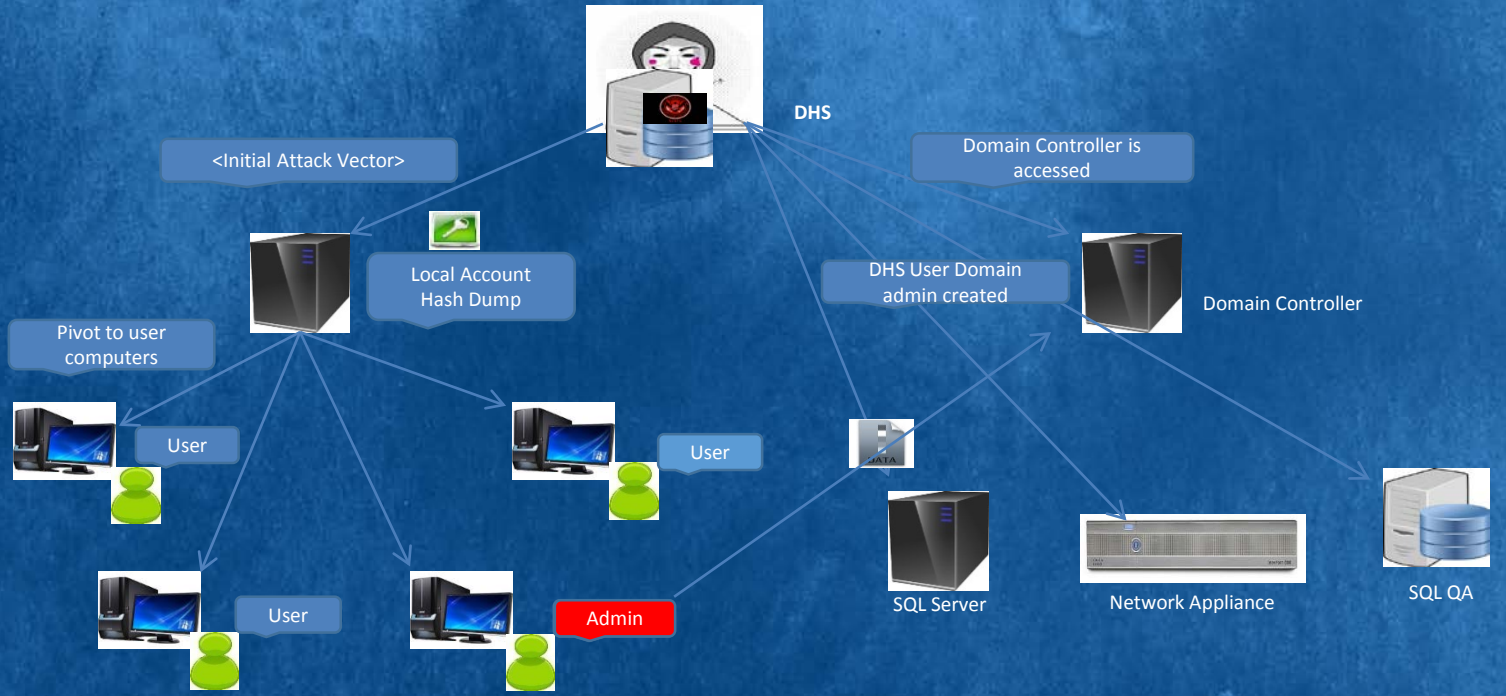
NCCIC | National Cybersecurity and Communications Integration Center

Issue	Impact	Mitigation
Stakeholder believed they had 800 hosts, scan revealed over	Flat network, person in region 1 can access all region 8	Segment network with router or firewall
Discovered over 200 security cameras accessible with default credentials	Physical security, theft, watching key strokes of users	Change default credentials and add network filters
SQL Injection- successfully crafted and input a data string enumerated web application usernames and passwords. credentials to log into web application and other devices	Unauthorized user access was achieved from the	Sanitize all input provided by an untrusted Implement server-side controls of white-listed character sets. Encrypt data stored on the
Discovered WAP buried underneath paper/trash/debris and into the Local Area Network	Security controls implemented to connected to the bypassed. Anyone at Starbucks next door could have	Monitor network for rogue devices, conduct walk-throughs to identify rogue devices
Phishing email sent to a limited number of employees. One forward to the entire agency	All machines were potentially compromised or had to cleaned. IT resources allocated to mitigation and clean	Train users to identify malicious email, technical controls.
Password reset function allowed the reset password to be any email address	Anyone could reset an account and log into the This logic flaw impacted Confidentiality, Availability Integrity	Ensure passwords can only be reset by the account owner and sent to the email address record for the account owner

Examples

NCCIC | National Cybersecurity and Communications Integration Center

What Happens Next?



NCCIC | National Cybersecurity and Communications Integration Center

Why DHS offers these services

- Make informed, risk-based decisions
- Eliminate remote attack paths
- Promote data-driven decisions

NCCIC | National Cybersecurity and Communications Integration Center

How DHS is helping

CYBER.DHS.GOV

15-01 Critical Vulnerability Mitigation

16-01- Security High Value Assets

16-01 - Threat to Network Infrastructure Devices

16-03 – 2016 Agency Cybersecurity Reporting Requirements

17-01 – Removal of Kaspersky Products

18-01 – Enhance Email and Web Security

SERVICES

Vulnerability Scanning

Incident Response

Automated Indicator Sharing

Architecture Review

Hunt

Self Assessments

Risk and Vulnerability Assessments

Questions?

NCATS_INFO@HQ.DHS.GOV

NCCIC